Manuale partecipanti TISAX

Come completare il processo di valutazione TISAX e condividere i risultati della valutazione con il proprio partner

Pubblicato da

ENX Association
un’associazione costituita ai sensi della legge francese del 1901,
iscritta con il numero w923004198 presso la Sous-préfecture of Boulogne-Billancourt, Francia

Indirizzi
20 rue Barthélémy Danjou, 92100 Boulogne-Billancourt, Francia
Bockenheimer Landstraße 97-99, 60325 Francoforte sul Meno, Germania

Autore

Florian Gleich

Contatti

tisax@enx.com
+49 69 9866927-77

Versione

Data:	06.03.2024
Versione:	2.7.1
Classificazione:	Public
ENX doc ID:	602-IT

Avviso sul copyright

Tutti i diritti riservati da ENX Association.
ENX, TISAX e i rispettivi loghi sono marchi registrati di ENX Association.
I marchi di terzi citati sono di proprietà dei rispettivi titolari.

Indice

1. Panoramica . . . 8
1.1. Scopo . . . 8
1.2. Ambito di applicazione . . . 8
1.3. Destinatari . . . 9
1.4. Struttura . . . 9
1.5. Come utilizzare questo documento . . . 9
1.6. Contatti . . . 10
1.7. Il Manuale per i partecipanti TISAX in altre lingue e altri formati . . . 10
1.7.1. Informazioni sulla traduzione in italiano . . . 13
1.7.2. Informazioni sul formato online . . . 13
1.7.3. Informazioni sul formato offline . . . 14
1.7.4. Informazioni sul formato PDF . . . 14
2. Introduzione . . . 15
2.1. Perché TISAX? . . . 15
2.2. Chi stabilisce cosa si intende con "sicurezza"? . . . 15
2.3. Il metodo del settore automotive . . . 16
2.4. Come si può dimostrare la sicurezza in modo efficace? . . . 16
3. Il processo TISAX . . . 18
3.1. Panoramica . . . 18
3.2. Registrazione . . . 19
3.3. Valutazione . . . 19
3.4. Scambio . . . 20
4. Registrazione (fase 1) . . . 21
4.1. Panoramica . . . 21
4.2. La vostra azienda è un partecipante TISAX . . . 21
4.3. Preparazione per la registrazione . . . 24
4.3.1. Le basi giuridiche . . . 24
4.3.2. L’ambito di valutazione TISAX . . . 25
4.3.2.1. Descrizione dell’ambito . . . 26
4.3.2.2. Ambito standard . . . 26
4.3.2.3. Definizione dell’ambito di applicazione . . . 27
4.3.2.4. Personalizzazione dell’ambito . . . 28
4.3.2.5. Sedi dell’ambito . . . 30
4.3.2.6. Nome dell’ambito . . . 33
4.3.2.7. Contatti . . . 34

4.3.2.8. Pubblicazione e condivisione . . . 35
4.3.3. Obiettivi di valutazione . . . 37
4.3.3.1. Elenco degli obiettivi di valutazione . . . 38
4.3.3.2. Obiettivi di valutazione e ISA . . . 41
4.3.3.3. Obiettivi di valutazione ed etichette TISAX . . . 41
4.3.3.4. Selezione degli obiettivi di valutazione . . . 42
4.3.3.5. Esigenze di protezione e livelli di valutazione . . . 46
4.3.3.6. Obiettivi di valutazione e fornitori della vostra azienda . . . 51
4.3.4. Tariffa . . . 52
4.4. Portale ENX . . . 54
4.5. Procedura di registrazione online . . . 54
4.5.1. Tempistiche . . . 55
4.5.2. Da dove iniziare . . . 55
4.5.3. Account sul portale . . . 55
4.5.4. Registrazione del partecipante . . . 56
4.5.5. Contatto del partecipante . . . 56
4.5.6. Condizioni generali . . . 57
4.5.7. Registrazione dell'ambito di valutazione . . . 57
4.5.8. E-mail di conferma . . . 60
4.5.8.1. Participant ID (🇮🇹 ID Partecipante) . . . 62
4.5.8.2. Scope ID (🇮🇹 ID Ambito) . . . 62
4.5.9. Informazioni sullo stato . . . 64
4.5.10. Modifiche alle informazioni di registrazione . . . 67
5. Valutazione (fase 2) . . . 68
5.1. Panoramica . . . 68
5.2. Autovalutazione basata sull'ISA . . . 68
5.2.1. Download del documento ISA . . . 69
5.2.2. Come interpretare il documento ISA . . . 69
5.2.2.1. Cataloghi di criteri . . . 69
5.2.2.2. Capitoli . . . 77
5.2.2.3. Domande di controllo . . . 77
5.2.2.4. Campi del modulo di autovalutazione . . . 78
5.2.2.5. Obiettivo . . . 79
5.2.2.6. Requisiti . . . 80
5.2.2.7. Livelli di maturità . . . 81
5.2.3. Esecuzione dell'autovalutazione . . . 82
5.2.4. Interpretazione del risultato dell'autovalutazione . . . 83

5.2.4.1. Analisi . . . 83
5.2.4.2. Il livello di maturità target (a livello di domanda) . . . 87
5.2.4.3. Il risultato della vostra azienda (a livello di domanda) . . . 87
5.2.4.4. Il valore target (a livello di punteggio) . . . 90
5.2.4.5. Il risultato della vostra azienda (a livello di punteggio) . . . 92
5.2.4.6. La vostra azienda è pronta? . . . 93
5.2.5. Gestione del risultato dell'autovalutazione . . . 95
5.3. Selezione del fornitore di audit . . . 96
5.3.1. Dati di contatto . . . 97
5.3.2. Copertura . . . 97
5.3.3. Richiesta di offerte . . . 97
5.3.4. Valutazione delle offerte . . . 98
5.4. Il processo di valutazione TISAX . . . 100
5.4.1. Panoramica . . . 100
5.4.2. Riunione iniziale . . . 100
5.4.3. Tipologie di valutazione TISAX . . . 101
5.4.4. Elementi delle valutazioni TISAX . . . 102
5.4.5. Informazioni sulla conformità . . . 102
5.4.6. La preparazione della vostra azienda per il processo di valutazione TISAX . . . 105
5.4.7. Valutazione iniziale . . . 105
5.4.7.1. La prima riunione formale di apertura . . . 106
5.4.7.2. Procedura di valutazione . . . 106
5.4.7.3. Riunione di chiusura . . . 106
5.4.7.4. Relazione della valutazione TISAX . . . 107
5.4.8. Preparazione del piano d'azione correttivo . . . 107
5.4.9. Valutazione del piano d'azione correttivo . . . 109
5.4.9.1. Motivazioni alla base di una valutazione del piano d'azione correttivo . . . 109
5.4.9.2. Combinazione con la valutazione iniziale . . . 109
5.4.9.3. Requisiti del piano d'azione correttivo . . . 109
5.4.9.4. Etichette TISAX temporanee . . . 110
5.4.10. Valutazione di follow-up . . . 111
5.4.10.1. Tempistiche . . . 111
5.4.10.2. Prerequisiti . . . 111
5.4.10.3. Scadenza delle etichette TISAX temporanee . . . 111
5.4.11. Grafico del processo di valutazione TISAX . . . 112
5.4.12. Assessment ID (🇮🇹 ID Valutazione) . . . 115
5.4.13. Relazione della valutazione TISAX . . . 116

5.4.14. Etichette TISAX . . . 117
5.4.14.1. Gerarchia delle etichette TISAX . . . 118
5.4.14.2. Periodo di validità delle etichette TISAX . . . 119
5.4.14.3. Rinnovo delle etichette TISAX . . . 119
6. Scambio (fase 3) . . . 121
6.1. Premessa . . . 121
6.2. La piattaforma di scambio . . . 121
6.3. Prerequisiti generali . . . 121
6.4. Permanenza dei risultati scambiati . . . 122
6.5. Livelli di condivisione . . . 122
6.6. Pubblicazione del risultato della valutazione sulla piattaforma di scambio . . . 123
6.7. Condivisione del risultato della valutazione con un partecipante specifico . . . 124
6.7.1. Prerequisiti . . . 125
6.7.2. Come creare un'autorizzazione di condivisione . . . 126
6.8. Condivisione del risultato della valutazione al di fuori di TISAX . . . 127
6.8.1. Motivi alla base della rigorosa regolamentazione del meccanismo di scambio . . . 127
6.8.2. Istruzioni su come pubblicare le informazioni sul processo TISAX . . . 127
6.8.3. Condivisione con un partner che non è ancora un partecipante TISAX . . . 128
6.8.4. Condivisione con i dipendenti del vostro partner che non hanno accesso diretto al portale ENX . . . 128
7. Allegati . . . 130
7.1. Allegato: Esempio di fattura . . . 130
7.2. Allegato: Esempio di e-mail di conferma . . . 131
7.3. Allegato: Esempio dell'Estratto dell'ambito TISAX . . . 132
7.4. Allegato: Participant status (Stato del partecipante) . . . 133
7.4.1. Panoramica: Participant status (Stato del partecipante) . . . 133
7.4.2. Participant status "Incomplete" (Stato del partecipante "Incompleto") . . . 135
7.4.3. Participant status "Awaiting approval" (Stato del partecipante "In attesa di approvazione") . . . 136
7.4.4. Participant status "Preliminary" (Stato del partecipante "Preliminare") . . . 136
7.4.5. Participant status "Registered" (Stato del partecipante "Registrato") . . . 138
7.4.6. Participant status "Expired" (Stato del partecipante "Scaduto") . . . 139
7.5. Allegato: Assessment scope status (Stato dell'ambito di valutazione) . . . 139
7.5.1. Panoramica: Assessment scope status (Stato dell'ambito di valutazione) . . . 139
7.5.2. Assessment scope status "Incomplete" (Stato dell'ambito di valutazione "Incompleto") . . . 141
7.5.3. Assessment scope status "Awaiting your order" (Stato dell'ambito di

valutazione “In attesa dell’ordine”) . . . 142
7.5.4. Assessment scope status “Awaiting ENX approval” (Stato dell’ambito di valutazione “In attesa dell’approvazione di ENX”) . . . 142
7.5.5. Assessment scope status “Awaiting your payment” (Stato dell’ambito di valutazione “In attesa del pagamento”) . . . 144
7.5.6. Assessment scope status “Registered” (Stato dell’ambito di valutazione “Registrato”) . . . 145
7.5.7. Assessment scope status “Active” (Stato dell’ambito di valutazione “Attivo”) . . . 145
7.5.8. Assessment scope status “Expired” (Stato dell’ambito di valutazione “Scaduto”) 146
7.6. Allegato: Assessment status (Stato della valutazione) . . . 147
7.6.1. Panoramica: Assessment status (Stato della valutazione) . . . 147
7.6.2. Assessment status “Initial assessment ordered” (Stato della valutazione “Valutazione iniziale richiesta”) . . . 149
7.6.3. Assessment status “Initial assessment ongoing” (Stato della valutazione “Valutazione iniziale in corso”) . . . 149
7.6.4. Assessment status “Waiting for corrective action plan assessment” (Stato della valutazione “In attesa della valutazione del piano d’azione correttivo) . . . 150
7.6.5. Assessment status “Waiting for follow-up” (Stato della valutazione “In attesa del follow-up”) . . . 151
7.6.6. Assessment status “Finished” (Stato della valutazione “Terminata”) . . . 151
7.7. Allegato: Motivazioni a sfavore delle “valutazioni preliminari” e delle “analisi dei divari” . . . 152
7.8. Allegato: Ambiti personalizzati . . . 153
7.8.1. Ambito personalizzato esteso . . . 153
7.8.2. Ambito personalizzato completo . . . 154
7.9. Allegato: Gestione del ciclo di vita dei dati del partecipante . . . 155
7.9.1. Perdita dell’accesso ai dati del partecipante (portale ENX) . . . 155
7.9.2. Gestione dei contatti . . . 155
7.9.2.1. Come aggiungere un nuovo contatto . . . 155
7.9.2.2. Come eliminare un contatto esistente . . . 156
7.9.2.3. Come aggiornare i dati di un contatto esistente . . . 156
7.9.3. Gestione delle sedi . . . 157
7.9.3.1. Come richiedere la modifica della denominazione della propria azienda . . . 157
7.9.3.2. Come richiedere la modifica di una sede . . . 158
7.9.3.3. Come richiedere la modifica del nome di una via . . . 159
7.9.3.4. Come aggiungere un’ulteriore sede . . . 160
7.10. Allegato: Valutazione di estensione dell’ambito . . . 160

7.11. Allegato: Gestione del ciclo di vita dell'ISA . . . 161
7.12. Allegato: Documenti utili . . . 161
7.13. Allegato: Gestione dei reclami . . . 162
7.13.1. Cause dei reclami . . . 162
7.13.1.1. Reclami relativi a ENX Association . . . 162
7.13.1.2. Reclami relativi ai fornitori di audit . . . 162
7.13.1.3. Requisiti per i reclami . . . 163
7.13.2. Contatto per i reclami . . . 164
8. Cronologia dei documenti . . . 165

1. Panoramica

1.1. Scopo

Vi diamo il benvenuto su TISAX, il Trusted Information Security Assessment Exchange.

Uno dei vostri partner vi ha chiesto di dimostrare che la gestione della sicurezza delle informazioni della vostra azienda è conforme a un determinato livello secondo i requisiti del documento "Information Security Assessment" (ISA). Ora volete quindi capire come soddisfare questa richiesta.

Lo scopo di questo manuale è quello di aiutarvi a soddisfare la richiesta del vostro partner o di portarvi avanti anticipandola prima che venga formulata.

Il presente manuale descrive le azioni da compiere per superare la valutazione TISAX e per condividere il relativo risultato con il vostro partner.

Definire e mantenere un sistema di gestione della sicurezza delle informazioni (information security management system, ISMS) è già di per sé un'operazione impegnativa. Dimostrare al vostro partner che la gestione della sicurezza delle informazioni della vostra azienda è adeguata la rende ulteriormente complessa. Il presente manuale non vi aiuterà a gestire la sicurezza delle informazioni: il suo scopo è invece quello di rendere il più semplice possibile dimostrare l'impegno della vostra azienda al partner in questione.

1.2. Ambito di applicazione

Il presente manuale si applica a tutti i processi TISAX in cui la vostra azienda può essere coinvolta.

Contiene tutto ciò che dovete sapere per completare il processo TISAX.

Il manuale offre alcuni consigli su come gestire i requisiti di sicurezza delle informazioni al

centro della valutazione. Il suo obiettivo, tuttavia, non è quello di fornirvi una preparazione generale su cosa è necessario fare per superare la valutazione della sicurezza delle informazioni.

1.3. Destinatari

Il presente manuale si rivolge principalmente alle aziende che devono o vogliono dimostrare di possedere un determinato livello di gestione della sicurezza delle informazioni secondo i requisiti dell'"Information Security Assessment" (ISA).

Non appena la vostra azienda sarà attivamente coinvolta nei processi TISAX, potrete beneficiare delle informazioni fornite in questo manuale.

Anche le aziende che richiedono ai propri fornitori di dimostrare di possedere determinati livelli di gestione della sicurezza delle informazioni ne trarranno vantaggio. Questo manuale permette a tali aziende di capire cosa devono fare i relativi fornitori per soddisfare la loro richiesta.

1.4. Struttura

Innanzitutto introdurremo brevemente TISAX, per passare subito dopo alle istruzioni su COME procedere. Troverete tutte le informazioni che vi servono per completare il processo nell'ordine più appropriato.

Il tempo di lettura stimato del documento è di 75-90 minuti.

1.5. Come utilizzare questo documento

È probabile che prima o poi avrete bisogno di familiarizzare con la maggior parte dei contenuti di questo documento. Per una preparazione adeguata, si consiglia di leggere l'intero manuale.

Il manuale è strutturato in base alle tre fasi principali del processo TISAX, in modo da poter passare alla sezione di cui avete bisogno e leggere il resto in un secondo momento.

Nel manuale sono contenute illustrazioni che facilitano la comprensione. I colori delle illustrazioni hanno spesso un significato aggiuntivo: si consiglia pertanto di leggere il documento da computer o su una copia cartacea a colori.

Il vostro feedback è molto apprezzato: se pensate che in questo manuale manchi qualcosa o che determinati contenuti non siano chiari, non esitate a comunicarcelo. Noi e tutti i futuri lettori del manuale vi saremo grati per il feedback fornito.

Se avete già utilizzato una versione precedente del Manuale per i partecipanti TISAX, troverete alcune note utili alla fine del documento in Sezione 8, "Cronologia dei documenti".

1.6. Contatti

Restiamo a disposizione per guidarvi attraverso il processo TISAX e per rispondere a tutte le vostre domande.

Potete inviarci un'e-mail all'indirizzo: tisax@enx.com

Oppure potete contattarci al numero: +49 69 9866927-77

Siamo raggiungibili durante il normale orario di lavoro in Germania (UTC+01:00).

Tutti i nostri dipendenti parlano inglese e tedesco. Un dipendente è madrelingua italiano.

Si prega di consultare la Sezione 7.13, "Allegato: Gestione dei reclami".

1.7. Il Manuale per i partecipanti TISAX in altre lingue e altri formati

Il Manuale per i partecipanti TISAX è disponibile nelle seguenti lingue e nei seguenti formati:

Lingua	Versione	Formato	Link
Inglese	2.7.1	Online	https://www.enx.com/handbook/tisax-participant-handbook.html
		Offline	https://www.enx.com/handbook/tisax-participant-handbook-offline.html
		PDF	https://www.enx.com/handbook/TISAX%20Participant%20Handbook.pdf

Lingua	Versione	Formato	Link
Tedesco	2.7.1	Online	https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html
		Offline	https://www.enx.com/handbook/tisax-teilnehmerhandbuch-offline.html
		PDF	https://www.enx.com/handbook/TISAX-Teilnehmerhandbuch.pdf
Francese	2.7	Online	https://www.enx.com/handbook/tph-fr.html
		Offline	https://www.enx.com/handbook/tph-fr-offline.html
		PDF	https://www.enx.com/handbook/tph-fr.pdf
Cinese	2.7	Online	https://www.enx.com/handbook/tph-cn.html
		Offline	https://www.enx.com/handbook/tph-cn-offline.html
		PDF	https://www.enx.com/handbook/tph-cn.pdf
Spagnolo	2.7	Online	https://www.enx.com/handbook/tph-es.html
		Offline	https://www.enx.com/handbook/tph-es-offline.html
		PDF	https://www.enx.com/handbook/tph-es.pdf
Giapponese	2.7	Online	https://www.enx.com/handbook/tph-jp.html
		Offline	https://www.enx.com/handbook/tph-jp-offline.html
		PDF	https://www.enx.com/handbook/tph-jp.pdf
Portoghese del Brasile	2.7	Online	https://www.enx.com/handbook/tph-pt.html
		Offline	https://www.enx.com/handbook/tph-pt-offline.html
		PDF	https://www.enx.com/handbook/tph-pt.pdf
Italiano	2.7.1	Online	https://www.enx.com/handbook/tph-it.html
		Offline	https://www.enx.com/handbook/tph-it-offline.html
		PDF	https://www.enx.com/handbook/tph-it.pdf

Lingua	Versione	Formato	Link
Coreano	2.7	Online	https://www.enx.com/handbook/tph-kr.html
		Offline	https://www.enx.com/handbook/tph-kr-offline.html
		PDF	https://www.enx.com/handbook/tph-kr.pdf
Ceco	2.7.1	Online	https://www.enx.com/handbook/tph-cz.html
		Offline	https://www.enx.com/handbook/tph-cz-offline.html
		PDF	https://www.enx.com/handbook/tph-cz.pdf
Polacco	2.7.1	Online	https://www.enx.com/handbook/tph-pl.html
		Offline	https://www.enx.com/handbook/tph-pl-offline.html
		PDF	https://www.enx.com/handbook/tph-pl.pdf

Nota importante:

La versione inglese è quella di riferimento.
Tutte le altre lingue sono traduzioni della versione inglese.
In caso di dubbi, fa fede la versione inglese.

1.7.1. Informazioni sulla traduzione in italiano

Il presente Manuale per i partecipanti TISAX è una traduzione della versione inglese.

Tutti i documenti alla base di TISAX sono stati creati in inglese (ad esempio, tutti i contratti e i requisiti per i fornitori dei servizi di audit di TISAX). Di conseguenza, il vostro partner o fornitore di audit potrebbe utilizzare alcuni termini specifici di TISAX in inglese.

Per aiutarvi a effettuare una corretta interpretazione, abbiamo mantenuto il termine originale TISAX inglese nella traduzione del Manuale per i partecipanti TISAX o lo abbiamo indicato tra parentesi direttamente dopo la relativa traduzione.

1.7.2. Informazioni sul formato online

Ciascuna sezione è provvista di un ID unico (formato: ID1234).
Un ID fa riferimento a una sezione specifica, indipendentemente dalla lingua.

Per accedere a una sezione specifica potete:

- fare clic con il tasto destro del mouse sul titolo della sezione e copiare il link, oppure
- fare clic sul titolo della sezione e copiare il link dalla barra degli indirizzi del browser.

La maggior parte delle figure è disponibile con dimensioni più grandi rispetto a quelle visualizzate per impostazione predefinita in questo documento. Fate clic sulla figura in questione per aprire la versione ingrandita.

1.7.3. Informazioni sul formato offline

Il formato offline mantiene la maggior parte delle caratteristiche del formato online. In particolare, le figure sono incorporate nel file HTML. Per utilizzare il formato offline occorre un solo file.

Rispetto al formato online, il formato offline non contiene:

- le immagini ingrandite
- i caratteri originali del formato online
  I caratteri sono definiti in base alle impostazioni predefinite del vostro browser.

1.7.4. Informazioni sul formato PDF

Se utilizzate il formato PDF da computer, potrete comunque fare clic su tutti i riferimenti. Se decidete invece di stampare la versione PDF, non avrete a disposizione i numeri di pagina e dovrete cercare i riferimenti autonomamente.

2. Introduzione

Le sezioni seguenti introducono il concetto di TISAX.

Se vi trovate in una situazione di urgenza, potete saltarle e passare subito alla Sezione 4.3, “Preparazione per la registrazione”.

2.1. Perché TISAX?

O per meglio dire: perché siete qui?

Per rispondere a questa domanda, cominceremo con alcune riflessioni sull’attività commerciale in generale e sulla protezione delle informazioni in particolare.

Mettetevi nei panni del vostro partner: possiede delle informazioni riservate e vuole condividerle con il suo fornitore, ossia la vostra azienda. La collaborazione tra voi e il vostro partner genera valore e le informazioni che il vostro partner condivide con voi sono una parte importante di questa creazione di valore. Per questo motivo vuole proteggerle in maniera adeguata. Vuole inoltre assicurarsi che voi gestiate le sue informazioni con la stessa cura.

Ma come può essere sicuro che le sue informazioni siano in buone mani? Non può semplicemente “fidarsi” di voi, deve averne la prova.

Le domande da porsi a questo punto sono due: chi stabilisce cosa si intende con gestione “sicura” delle informazioni? E come la si dimostra?

2.2. Chi stabilisce cosa si intende con "sicurezza"?

Voi e il vostro partner non siete gli unici a dover affrontare queste domande per la prima volta. Quasi tutti sono alla ricerca di una risposta e quasi tutte le risposte sono simili tra loro.

Invece di dover trovare ogni volta una soluzione individuale a un problema comune, l’adozione di un metodo standard elimina le difficoltà derivanti dal dover creare tutto da zero. Definire uno standard comporta uno sforzo enorme, ma è un’operazione che viene fatta una sola volta e chi lo segue ne trarrà vantaggio ogni volta.

Esistono sicuramente opinioni diverse su cosa sia giusto fare per proteggere le informazioni. Tuttavia, proprio per i vantaggi citati sopra, la maggior parte delle aziende decide di avvalersi di standard. Uno standard condensa dentro di sé tutte le best practice comprovate e testate nel tempo per una determinata sfida.

Nel vostro caso, standard come l’ISO/IEC 27001 (sui sistemi di gestione della sicurezza delle informazioni o ISMS) e la loro implementazione stabiliscono modalità avanzate per gestire in modo sicuro le informazioni riservate. Con uno standard come questo non dovrete perdere tempo ogni volta per inventare una soluzione che esiste già. Inoltre, gli standard forniscono una

base comune che due aziende possono utilizzare quando devono scambiarsi dati riservati.

2.3. Il metodo del settore automotive

Per loro natura, gli standard indipendenti da un settore specifico sono concepiti come soluzioni universali, anziché essere adattate alle particolari esigenze delle aziende del settore automobilistico.

Molto tempo fa, l'industria automobilistica ha formato delle associazioni che avevano come obiettivo, tra gli altri, quello di perfezionare e definire standard adatti alle specifiche necessità del settore. L'associazione "Verband der Automobilindustrie" (VDA) è una di queste. All'interno del gruppo di lavoro che si occupa di sicurezza delle informazioni, diversi membri dell'industria automobilistica sono giunti alla conclusione che le loro esigenze sono sufficientemente simili per adattare gli standard esistenti di gestione della sicurezza delle informazioni.

Il loro impegno congiunto ha portato alla realizzazione di un questionario relativo ai requisiti di sicurezza delle informazioni ampiamente accettati dal settore automobilistica, denominato "Information Security Assessment" (ISA, Valutazione della sicurezza delle informazioni).

Grazie all'ISA, ora abbiamo una risposta alla domanda "Chi stabilisce cosa si intende con sicurezza?". Attraverso la VDA, il settore automobilistico stesso offre questa risposta ai suoi membri.

2.4. Come si può dimostrare la sicurezza in modo efficace?

Mentre alcune aziende utilizzano l'ISA solo per finalità interne, altre lo usano per valutare la maturità della gestione della sicurezza delle informazioni dei loro fornitori. In alcuni casi, un'autovalutazione è sufficiente ai fini dei rapporti commerciali. Tuttavia, a volte, le aziende conducono una valutazione completa della gestione della sicurezza delle informazioni dei propri fornitori (compresi gli audit in loco).

Parallelamente alla crescente consapevolezza della necessità di gestire la sicurezza delle informazioni e alla diffusione dell'ISA come strumento di valutazione della sicurezza delle informazioni, un numero considerevole di fornitori si è trovato di fronte a richieste simili da partner diversi.

Tali partner applicavano comunque standard diversi e avevano opinioni differenti su come interpretarli. In sostanza i fornitori dovevano dimostrare le stesse cose, solo in modi diversi.

E più i partner chiedevano ai fornitori di dimostrare il proprio livello di gestione della sicurezza delle informazioni, più le proteste di questi ultimi aumentavano per il continuo lavoro che veniva loro richiesto. Mostrare a un auditor dopo l'altro le stesse misure di gestione della sicurezza delle informazioni è semplicemente un metodo inefficace.

Come rendere quindi questa operazione più efficace? Non sarebbe utile poter riutilizzare la relazione di uno stesso auditor per più partner?

Gli OEM e i fornitori del gruppo di lavoro di ENX responsabile della gestione dell'ISA hanno ascoltato le rimostranze dei propri fornitori. Oggi sono quindi in grado di offrire loro e a tutte le altre aziende del settore automobilistico una risposta alla domanda "Come si può dimostrare la sicurezza?".

Questa risposta è TISAX, acronimo di "Trusted Information Security Assessment Exchange" ("Scambio affidabile delle valutazioni sulla sicurezza delle informazioni").

3. Il processo TISAX

3.1. Panoramica

Il processo TISAX normalmente[1] inizia con la richiesta da parte di uno dei vostri partner di dimostrare un determinato livello di gestione della sicurezza delle informazioni in base ai requisiti dell'"Information Security Assessment" (ISA). Per soddisfare tale richiesta, dovete completare il processo TISAX in 3 fasi. In questa sezione troverete una panoramica delle fasi da completare.

Il processo TISAX è composto dalle seguenti 3 fasi:

Figura 1. Panoramica del processo TISAX

1. Fase 1
   Registrazione
2. Fase 2
   Valutazione
3. Fase 3
   Scambio

1. Registrazione
   Raccogliamo informazioni sulla vostra azienda e su quali elementi devono essere inclusi nella valutazione.
2. Valutazione
   La vostra azienda completa la valutazione (o le valutazioni) condotta da parte di uno dei nostri fornitori di audit TISAX.
3. Scambio
   La vostra azienda condivide il risultato della valutazione con il partner in questione.

Ciascuna fase è composta da sotto-fasi, delineate nelle tre sezioni seguenti e descritte in dettaglio nelle rispettive sezioni più avanti.

Attenzione:

Anche se ci piacerebbe potervi dire quanto tempo è necessario per ottenere il risultato della valutazione TISAX, ci teniamo a precisare che non è possibile per noi fare previsioni affidabili. La durata complessiva del processo TISAX dipende da troppi fattori. Le diverse dimensioni delle aziende, la varietà degli

> obiettivi di valutazione e il grado di sviluppo di ciascun sistema di gestione della sicurezza delle informazioni rendono questa previsione impossibile.

3.2. Registrazione

Il primo passo è la registrazione a TISAX.

Lo scopo principale della registrazione a TISAX è quello di raccogliere informazioni sulla vostra azienda. Utilizziamo una procedura di registrazione online attraverso la quale potete fornirci queste informazioni.

Si tratta di un prerequisito per tutte le fasi successive. e prevede il pagamento di una tariffa.

Durante la procedura di registrazione online:

- Vi chiediamo di fornirci i vostri dati di contatto e di fatturazione.
- Dovete accettare le nostre condizioni.
- Potete definire l'ambito della valutazione della sicurezza delle informazioni della vostra azienda.

Per un avvio diretto con questa azione, si veda Sezione 4, "Registrazione (fase 1)".

La procedura di registrazione online è descritta in dettaglio in Sezione 4.5, "Procedura di registrazione online". Se invece volete iniziare subito il processo, accedete a enx.com/en-US/TISAX/.

3.3. Valutazione

La seconda fase consiste nel completamento della valutazione della sicurezza delle informazioni.

Sono previste quattro sotto-fasi:

a. Preparazione della valutazione
   Dovete predisporre la valutazione. La portata di tale preparazione dipende dal livello di maturità corrente del sistema di gestione della sicurezza delle informazioni della vostra azienda. La vostra preparazione deve basarsi sul catalogo dell'ISA.
b. Selezione del fornitore di audit
   Dovete scegliere uno dei nostri fornitori di audit TISAX.
c. Valutazione/i della sicurezza delle informazioni
   Il vostro fornitore di audit condurrà la valutazione sulla base di un ambito di valutazione che corrisponde ai requisiti del vostro partner. Come minimo, il processo di valutazione consiste nell'audit iniziale.

Qualora la vostra azienda non superi subito la valutazione, il processo può richiedere ulteriori fasi.

d. Risultato della valutazione
Una volta che la vostra azienda ha superato la valutazione, il vostro fornitore di audit vi fornirà la relazione della valutazione TISAX ufficiale. Il risultato della valutazione sarà anche accompagnato dalle etichette TISAX[2].

Per maggiori informazioni su questa azione, si veda Sezione 5, “Valutazione (fase 2)”.

3.4. Scambio

La terza e ultima fase consiste nel condividere il risultato della valutazione con il vostro partner. Il contenuto della relazione della valutazione TISAX è strutturato in livelli. Potete decidere fino a quale livello concedere l’accesso al vostro partner.

Il risultato della valutazione ha una validità di tre anni. Se a quel punto sarete ancora un fornitore del partner in questione, dovrete ripetere le tre fasi del processo[3].

Per maggiori informazioni su questa azione, si veda Sezione 6, “Scambio (fase 3)”.

Ora che vi siete fatti un’idea di base del processo TISAX, nelle sezioni seguenti troverete le istruzioni su come completare ogni fase.

4. Registrazione (fase 1)

Il tempo di lettura stimato per la sezione relativa alla registrazione è di 30-40 minuti.

4.1. Panoramica

La registrazione a TISAX è il primo passo da compiere. Si tratta di un prerequisito per tutte le fasi successive.

Le sezioni che seguono vi guideranno durante la procedura di registrazione:

1. Cominceremo con lo spiegare un nuovo termine essenziale.
2. Vi forniremo poi consigli su come prepararvi per la procedura di registrazione online.
3. Infine vi guideremo durante la procedura di registrazione online.

4.2. La vostra azienda è un partecipante TISAX

Cominciamo con l'introdurre innanzitutto un nuovo termine indispensabile da comprendere. Finora la vostra azienda ha ricoperto il ruolo di "fornitore", chiamato a soddisfare una richiesta del suo "cliente". TISAX, tuttavia, non fa una vera e propria distinzione tra questi due ruoli. Per TISAX ogni soggetto che si registra è un "partecipante". La vostra azienda, così come il vostro partner, "partecipa" allo scambio dei risultati relativi alla valutazione della sicurezza delle informazioni.

Figura 2. Registrazione per diventare un partecipante TISAX

1. La vostra azienda
2. Registrazione a TISAX
3. Partecipante TISAX

Per distinguere i due ruoli fin dall'inizio, ci riferiremo alla vostra azienda, il fornitore, come "partecipante attivo", mentre il vostro partner verrà indicato come "partecipante passivo". In quanto "partecipante attivo", la vostra azienda verrà sottoposta alla valutazione TISAX e condividerà il risultato della valutazione con gli altri partecipanti. Il "partecipante passivo" è il soggetto che ha richiesto alla vostra azienda di sottoporsi alla valutazione TISAX e che riceve quindi il risultato della valutazione.

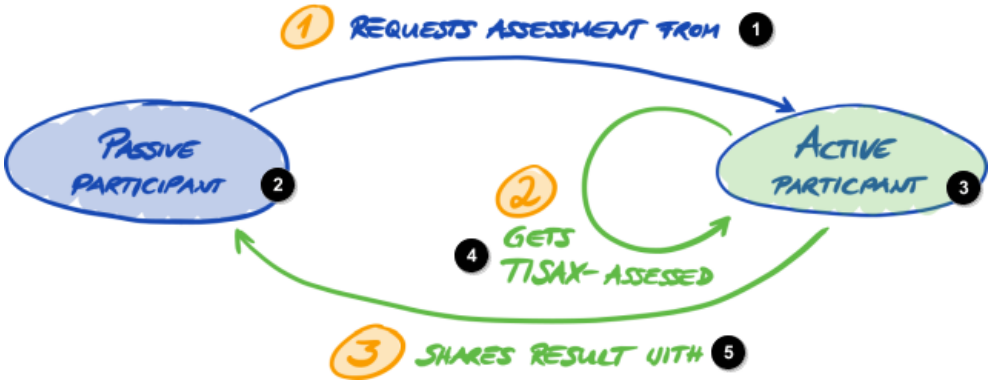


Figura 3. Partecipante passivo e partecipante attivo

1. 1 Richiede la valutazione a
2. Partecipante passivo
3. Partecipante attivo
4. 2 Si sottopone alla valutazione TISAX
5. 3 Condivide il risultato con

Tutte le aziende possono ricoprire entrambi i ruoli. Potete condividere il risultato di una valutazione con il vostro partner e chiedere al tempo stesso ai vostri fornitori di sottoporsi a una valutazione TISAX.

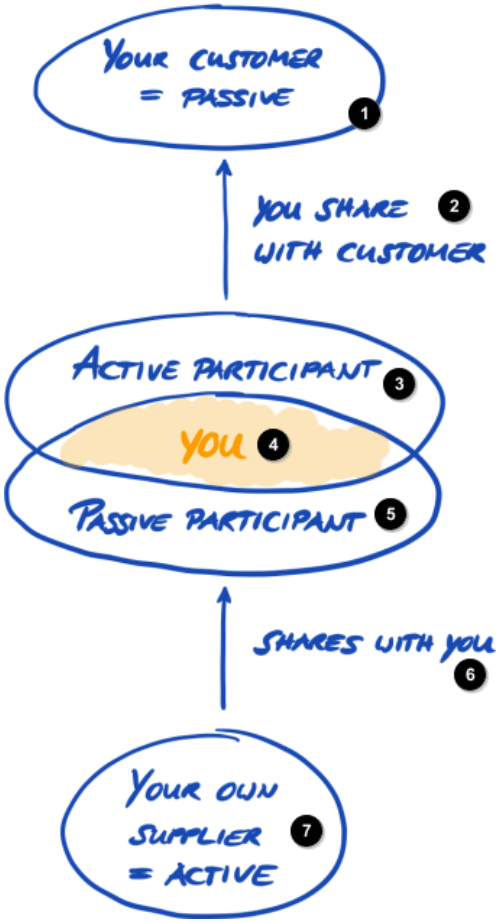


Figura 4. I partecipanti TISAX possono essere attivi e passivi al tempo stesso

1. Il vostro cliente
   = passivo
2. La vostra azienda condivide il risultato con il cliente
3. Partecipante attivo
4. La vostra azienda
5. Partecipante passivo
6. Condivide il risultato con la vostra azienda
7. Il vostro fornitore
   = attivo

Richiedere ai propri fornitori di sottoporsi alla valutazione TISAX può essere particolarmente opportuno se anche loro gestiscono le informazioni del vostro partner con esigenze di protezione.

4.3. Preparazione per la registrazione

Questa sezione contiene consigli su come *prepararsi* per la registrazione. La procedura di registrazione è descritta in dettaglio in Sezione 4.5, “Procedura di registrazione online”.

Prima di iniziare la procedura di registrazione online, vi consigliamo vivamente di:

- raccogliere le informazioni in anticipo
- e prendere alcune decisioni.

4.3.1. Le basi giuridiche

Normalmente è necessario firmare due contratti. Il primo contratto viene stipulato tra la vostra azienda ed ENX Association: le “Condizioni generali di partecipazione a TISAX” (CG di Partecipazione a TISAX). Il secondo contratto viene invece concluso tra la vostra azienda e uno dei nostri fornitori di audit TISAX. Ai fini della registrazione ci soffermeremo solo sul primo contratto.

Le CG di Partecipazione a TISAX regolano i rapporti tra noi e la vostra azienda e quelli tra la vostra azienda e gli altri partecipanti TISAX. In esse sono stabiliti i diritti e i doveri di tutti i soggetti coinvolti. Oltre alle clausole standard che si trovano nella maggior parte dei contratti, esse definiscono nel dettaglio come vengono trattate le informazioni scambiate e ottenute durante il processo TISAX. Un obiettivo fondamentale di queste regole è quello di mantenere riservati i risultati delle valutazioni TISAX. Poiché tutti i partecipanti TISAX sono soggetti alle stesse regole, potete aspettarvi un’adeguata protezione dei risultati della valutazione TISAX da parte del vostro partner (nel suo ruolo di partecipante passivo).

Già nella fase iniziale della procedura di registrazione online, vi chiederemo di accettare le CG di Partecipazione a TISAX. Trattandosi di un vero e proprio contratto, consigliamo di leggere le CG di Partecipazione a TISAX prima di iniziare la procedura di registrazione online. A seconda del vostro ruolo in azienda, infatti, potrebbe essere necessario ottenere l’autorizzazione da parte di un consulente legale interno o esterno.

Le “Condizioni generali di partecipazione a TISAX”[4] possono essere scaricate dal nostro sito web al seguente indirizzo:
enx.com/en-US/TISAX/downloads/

Download diretto del PDF:
enx.com/tisaxgtcen.pdf

Durante la procedura di registrazione online, vi chiederemo di selezionare due caselle obbligatorie:

- ☐ We accept the TISAX Participation General Terms and Conditions (Accettiamo le Condizioni generali di partecipazione a TISAX)

- We confirm knowledge of Applicant’s release of Audit Providers’ professional duties of secrecy acc. to Sec. IX.5. and X.3 of the TISAX Participation General Terms and Conditions; (Confermiamo di essere a conoscenza del fatto che il Richiedente esonera i Fornitori di Audit dai propri obblighi di segretezza professionale conformemente alle Sezioni IX.5. e X.3 delle Condizioni generali di partecipazione a TISAX;)

Abbiamo inserito la seconda casella perché alcuni dei nostri fornitori di audit TISAX sono revisori contabili certificati e devono quindi rispettare speciali requisiti in materia di segreto professionale. Di solito, i requisiti speciali in materia di segreto professionale vietano ai revisori contabili certificati che operano in qualità di nostri fornitori di audit di condividere informazioni con noi. In particolare, ciò ci impedirebbe di eseguire i controlli necessari per svolgere la nostra funzione di governance. Pertanto, abbiamo bisogno di questa liberatoria. Si consiglia di prestare particolare attenzione a queste clausole prima di selezionare la relativa casella.

Se generalmente la vostra azienda necessita di stipulare un accordo di riservatezza (NDA) con qualunque soggetto che gestisca informazioni riservate, vi invitiamo a consultare le rispettive sezioni delle nostre CG, dove dovreste trovare risposta a tutti i vostri dubbi. Inoltre, di solito non è previsto che ci forniate alcuna informazione riservata.

Per concludere la sezione legale, precisiamo che il nostro sistema si basa sull’accettazione delle stesse regole da parte di tutti. Per questo motivo non possiamo accettare condizioni generali aggiuntive[5].

4.3.2. L’ambito di valutazione TISAX

Durante la seconda fase del processo TISAX, uno dei nostri fornitori di audit TISAX condurrà la valutazione della sicurezza delle informazioni. Tale fornitore deve sapere da quale punto iniziare e quando fermarsi, ecco perché è necessario che definiate un “ambito di valutazione”.

L’“ambito di valutazione” descrive il perimetro della valutazione della sicurezza delle informazioni. In parole povere, ogni area della vostra azienda coinvolta nella gestione delle informazioni riservate del vostro partner rientra nell’ambito di valutazione. Si tratta di un elemento fondamentale nella descrizione dei compiti del fornitore di audit e stabilisce gli elementi che egli deve valutare.

L’ambito di valutazione è importante per due motivi:

a. Il risultato della valutazione soddisferà i requisiti del vostro partner solo se il relativo ambito di valutazione copre tutte le aree della vostra azienda coinvolte nella gestione delle informazioni di tale partner.
b. Un ambito di valutazione definito con precisione è un prerequisito essenziale per permettere ai nostri fornitori di audit TISAX di calcolare correttamente i costi.

Nota importante:

> ISO/IEC 27001 vs TISAX
>
> Dobbiamo innanzitutto distinguere tra due tipi di ambito:
> 1) l'ambito del sistema di gestione della sicurezza delle informazioni (ISMS) della vostra azienda e
> 2) l'ambito della valutazione.
> Questi due ambiti non sono necessariamente identici.
>
> Per la certificazione ISO/IEC 27001, potete definire l'ambito dell'ISMS della vostra azienda (nella "definizione dell'ambito") in completa libertà. Tuttavia, l'ambito della valutazione (noto anche come "ambito dell'audit") deve essere identico all'ambito dell'ISMS della vostra azienda.
>
> Anche nel caso di TISAX vi viene chiesto di definire l'ISMS della vostra azienda, ma l'ambito della valutazione può essere diverso.
>
> Per la certificazione ISO/IEC 27001, potete stabilire liberamente l'ambito della valutazione nello stesso modo in cui stabilite l'ambito dell'ISMS della vostra azienda.
>
> Nel caso di TISAX, invece, l'ambito della valutazione è predefinito. L'ambito della valutazione può essere inferiore rispetto all'ambito dell'ISMS della vostra azienda, ma deve rientrare in quest'ultimo.

4.3.2.1. Descrizione dell'ambito

La descrizione dell'ambito definisce l'ambito di valutazione. Per la descrizione dell'ambito, è necessario scegliere uno dei seguenti due tipi di ambito:

1. Standard scope (Ambito standard)
2. Custom scope (Ambito personalizzato)
    a. Custom extended scope (Ambito personalizzato esteso)
    b. Full custom scope (Ambito personalizzato completo)

Parleremo dell'ambito standard nella sezione seguente. L'ambito standard è la scelta giusta per oltre il 99% dei partecipanti. Pertanto, parleremo degli ambiti personalizzati solo in Sezione 7.8, "Allegato: Ambiti personalizzati".

4.3.2.2. Ambito standard

La descrizione dell'ambito standard è alla base della valutazione TISAX. Gli altri partecipanti TISAX accettano solo i risultati di valutazioni basati sulla descrizione dell'ambito standard.

La descrizione dell'ambito standard è predefinita e non può essere modificata.

Uno dei vantaggi principali dell'adottare un ambito standard è il fatto che non occorre elaborare una propria definizione.

Di seguito è riportata la descrizione dell'ambito standard (versione 2.0):

```
The TISAX assessment scope defines the
scope of the assessment. The
assessment includes all processes,
procedures and resources under
responsibility of the assessed
organization that are relevant to the
security of the protection objects and
their protection goals as defined in
the listed assessment objectives at
the listed locations.
The assessment is conducted at least
in the highest assessment level listed
in any of the listed assessment
objectives. All assessment criteria
listed in the listed assessment
objectives are subject to the
assessment.
```

```
L□ambito di valutazione TISAX
definisce il perimetro della
valutazione. La valutazione include
tutti i processi, le procedure e le
risorse di cui l□organizzazione
soggetta a valutazione è responsabile
e che sono rilevanti per la sicurezza
degli elementi oggetto di protezione e
i relativi obiettivi di protezione,
definiti negli obiettivi di
valutazione indicati, nelle sedi
indicate.
La valutazione viene condotta almeno
al livello di valutazione più alto tra
quelli elencati negli obiettivi di
valutazione indicati. Tutti i criteri
di valutazione elencati negli
obiettivi di valutazione indicati sono
soggetti a valutazione.
```

Consigliamo vivamente di scegliere l'ambito standard. Tutti i partecipanti TISAX accettano i risultati della valutazione della sicurezza delle informazioni basati sull'ambito standard.

4.3.2.3. Definizione dell'ambito di applicazione

Dopo aver definito il tipo di ambito, dovete decidere quali sedi rientrano nell'ambito di valutazione.

Se la vostra azienda è di piccole dimensioni (una sola sede), si tratta di un'operazione facile. Dovrete semplicemente aggiungere la vostra sede all'ambito di valutazione.

Se si tratta invece di un'azienda di grandi dimensioni, potete valutare se registrare più di un ambito di valutazione.

Definire un unico ambito che racchiuda tutte le vostre sedi presenta dei vantaggi:

- Avrete una sola relazione della valutazione, un solo risultato della valutazione e una sola data di scadenza.

- La valutazione avrà costi ridotti, perché il fornitore di audit TISAX dovrà valutare i processi, le procedure e le risorse centrali una sola volta.

Tuttavia la definizione di un unico ambito può presentare anche degli svantaggi, come ad esempio:

- Tutte le sedi devono avere gli stessi obiettivi di valutazione.
- Il risultato della valutazione è disponibile solo dopo che il fornitore di audit TISAX ha valutato tutte le sedi. Questo può essere un aspetto rilevante se avete bisogno di ricevere un risultato della valutazione con urgenza.
- Il risultato della valutazione è subordinato al superamento della stessa da parte di tutte le sedi. Se una sola sede non supera la valutazione, il risultato non sarà positivo. Una soluzione a questo problema è: a) rimuovere la sede dall'ambito, b) risolvere i problemi, c) aggiungere la sede in seguito con una valutazione di estensione dell'ambito.

4.3.2.4. Personalizzazione dell'ambito

La decisione se avere un solo ambito o più ambiti spetta unicamente a voi. Tuttavia, rispondere alle domande presenti nel seguente grafico può aiutarvi a decidere.

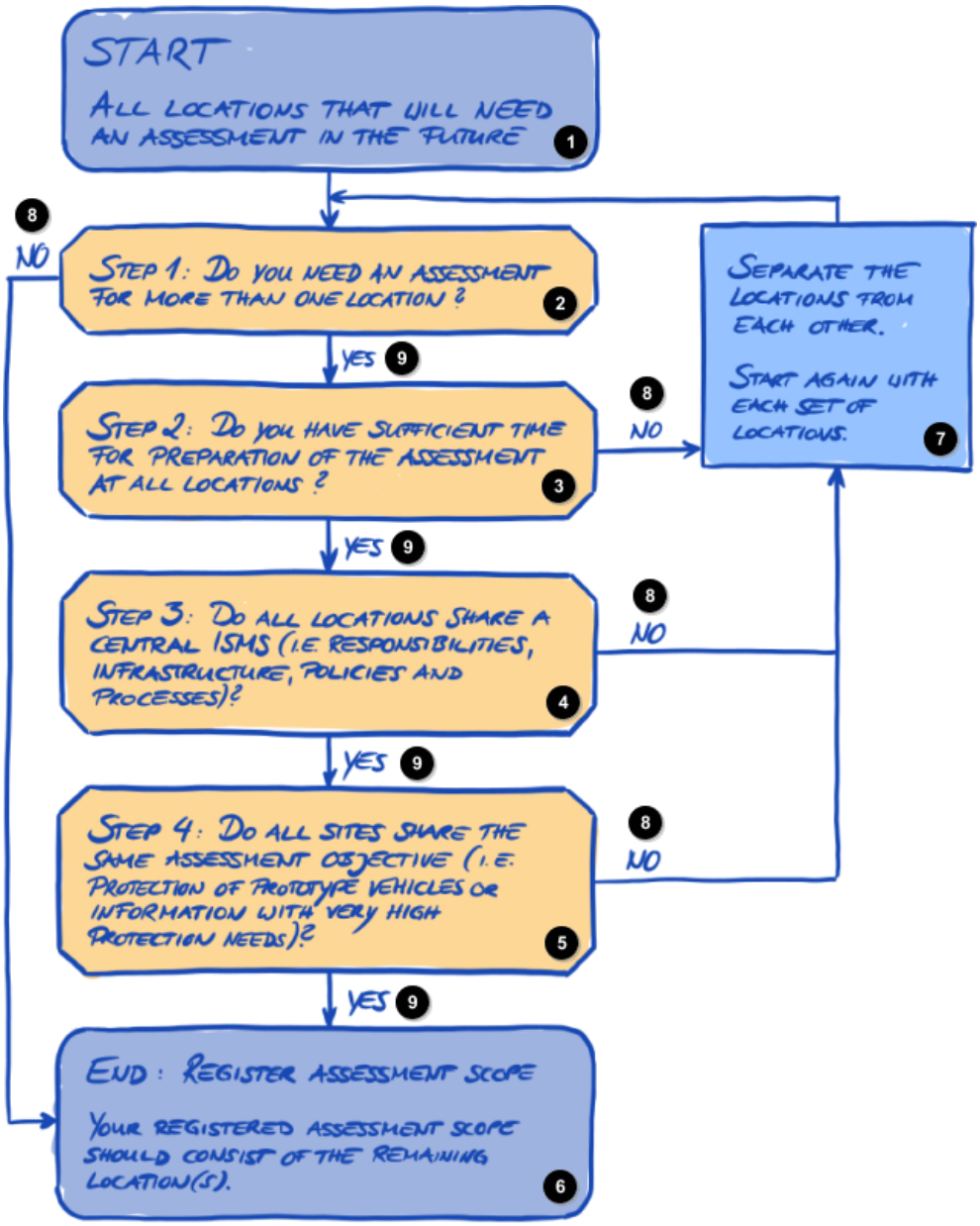


Figura 5. Albero decisionale per la personalizzazione dell'ambito

1. INIZIO
   Tutte le sedi che necessitano di una valutazione in futuro
2. Passaggio 1: Avete bisogno di una valutazione per più di una sede?
3. Passaggio 2: Disponete di tempo sufficiente per prepararvi per la valutazione in tutte le sedi?
4. Passaggio 3: Tutte le sedi condividono un ISMS centrale (responsabilità, infrastruttura, politiche e processi)?
5. Passaggio 4: Tutte le sedi condividono lo stesso obiettivo di valutazione (protezione di prototipi di veicoli o informazioni con esigenze di protezione molto elevate)?

6. Fine: registrazione dell'ambito di valutazione
   L'ambito di valutazione registrato deve comprendere la/le sede/i rimanente/i.
7. Considera le sedi separatamente le une dalle altre.
   Ricomincia da capo con ciascun gruppo di sedi.
8. No
9. Sì

Attenzione:

Non lasciatevi intimidire da questa decisione. È possibile modificare qualsiasi ambito, purché il fornitore di audit non abbia ancora concluso la valutazione.

Ad esempio, durante la preparazione della valutazione potreste scoprire che l'ambito scelto non è adatto --e modificarlo di conseguenza. Oppure il fornitore di audit potrebbe consigliare di modificare l'ambito durante le fasi iniziali della valutazione.

Note aggiuntive:

- Tecnicamente, non è possibile modificare l'ambito di valutazione definito durante la procedura di registrazione online nel portale ENX. Tuttavia, il fornitore di audit può aggiornare l'ambito di valutazione quando carica il risultato della valutazione sul portale ENX.
- Se si fanno aggiunte all'ambito anche la tariffa aumenterà, mentre non è previsto un rimborso se si rimuovono delle sedi dall'ambito. Poiché i fornitori di audit si basano sull'ambito originale per calcolare i costi, dovrete aspettarvi delle modifiche in tal senso.

4.3.2.5. Sedi dell'ambito

Ora che avete deciso quali sedi rientrano nell'ambito di valutazione, potete continuare a raccogliere informazioni specifiche sulle sedi.

Per ogni sede abbiamo bisogno di informazioni come la denominazione e l'indirizzo dell'azienda. Vi chiediamo inoltre alcune informazioni aggiuntive che consentono ai nostri fornitori di audit TISAX di farsi un'idea più precisa della vostra struttura aziendale. In base alle vostre risposte essi formuleranno una stima del lavoro richiesto.

Preparate quindi le seguenti informazioni per ciascuna delle vostre sedi (l'asterisco rosso * indica le informazioni obbligatorie nella procedura online):

Campo	Opzioni
Nome della sede *	N/A
NUMERO D-U-N-S D&B	N/A
Tipo di sede *	Edificio (o edifici) di proprietà e uso esclusivo dell'azienda Edificio (o edifici) affittati dall'azienda Piano/ufficio affittato dall'azienda in un edificio condiviso Ufficio condiviso con altre aziende Data center di proprietà Data center condiviso
Protezione passiva del sito *	Sì No
Settore *(sono possibili più selezioni)*	Information Technology ☐ Servizi IT ☐ Servizi di telecomunicazione ☐ Sviluppo software
	Gestione ☐ Consulenza
	Comunicazione ☐ Marketing ☐ Agenzia ☐ Servizi di stampa ☐ Fotografia ☐ Servizi di traduzione
	Ricerca e sviluppo ☐ Collaudo di veicoli ☐ Simulazione di veicoli ☐ Costruzione di prototipi ☐ Modelli di auto in miniatura ☐ Servizi di sviluppo ☐ Servizi di sviluppo CAx

Campo	Opzioni
	Produzione • Servizi di produzione • Produzione su commissione • Officina • Logistica
	Vendita e post-vendita • Importazione, NSC • Concessionario • Servizi finanziari • Assicurazioni • Liquidazione dei sinistri
	Altro settore *(specificare)*
Dipendenti presso la sede: totali *	0 1-10 11-100 101-1,000 1,001-5,000 Più di 5,000
Dipendenti presso la sede: IT *	0 1-10 11-25 26-50 Più di 50
Dipendenti presso la sede: sicurezza informatica *	0 Part-time 1-5 6-25 Più di 25
Dipendenti presso la sede: sicurezza della sede *	0 Part-time 1-3 4-10 Più di 10

Campo	Opzioni
Certificazioni per questa sede	ISO 27001 Altro *(specificare)* ISAE 3402 SOC2

Tabella 1. Dettagli specifici sulle sedi

Attenzione:

Per quanto riguarda il campo “Settore”: selezionate l’opzione migliore in base alle vostre conoscenze. Non esistono scelte giuste o sbagliate quando si selezionano le opzioni di cui sopra. Se non è presente un’opzione che corrisponde alla vostra tipologia di azienda, indicate quella appropriata in “Altro”.

Per ciascuna sede dovete specificare un “location name” (🇮🇹 “nome della sede”). Il nome della sede consente di individuare una determinata sede con più facilità quando la si assegna a un ambito di valutazione.

Consigliamo di assegnare i nomi delle sedi in base al seguente schema:

Schema: [Riferimento geografico]

Esempio: per l’azienda di fantasia “ACME”

- Francoforte
  (per una sede nella **città** tedesca di Francoforte)

4.3.2.6. Nome dell’ambito

Per ogni ambito è necessario specificare uno “scope name” (🇮🇹 “nome dell’ambito”). Lo scopo principale del nome dell’ambito è quello di facilitare l’identificazione di un determinato ambito nell’elenco generale degli ambiti nel portale ENX. Scegliete un nome che sia utile al lettore e ai vostri colleghi. Per le comunicazioni esterne, utilizzate l’ID Ambito.

Potete usare il nome che volete, ma non è possibile assegnare lo stesso nome a più di un ambito.

Se in seguito desiderate rinnovare la valutazione TISAX, dovrete creare un nuovo ambito (possibilmente identico a quello attuale). Consigliamo quindi di aggiungere l’anno della valutazione al nome dell’ambito.

Consigliamo di assegnare i nomi degli ambiti in base al seguente schema:

Schema: [Riferimento geografico o *funzionale* anno] [della valutazione]

Esempi: per l'azienda di fantasia "ACME"

- 2024
  (senza riferimento geografico se la vostra azienda ha una sola sede)
- Francoforte 2024
  (per un ambito con più sedi nella **città** tedesca di Francoforte)
- Bassa Sassonia 2024
  (per un ambito con tutte le sedi nello **stato federato** tedesco della Bassa Sassonia)
- Germania 2024
  (per un ambito con tutte le sedi nel **Paese** della Germania)
- EMEA 2024
  (per un ambito con tutte le sedi nella **regione** EMEA ("Europa, Medio Oriente, Africa"))
- Sviluppo prototipi 2024
  (riferimento *funzionale* per un ambito con tutte le sedi impegnate nello sviluppo di prototipi)

4.3.2.7. Contatti

Per poter comunicare con voi, raccogliamo i dati di contatto dei referenti presso la vostra azienda.

Chiediamo di fornirci almeno un contatto per la vostra azienda in quanto partecipante TISAX in generale e uno per ciascun ambito di valutazione. Potete anche fornire contatti aggiuntivi.

Durante i preparativi per la registrazione, dovete quindi decidere chi saranno i referenti della vostra azienda da inserire come contatti.

Chiediamo di indicare i seguenti dati di contatto:

	Dato del contatto	**Obbligatorio?**	**Esempio**
1.	Formula di saluto	Sì	Sig.ra, Sig.
2.	Titolo accademico		Dott./Dott.ssa, Ph.D., altro
3.	Nome	Sì	John
4.	Cognome	Sì	Doe
5.	Qualifica professionale	Sì	Responsabile IT
6.	Ufficio	Sì	Information Technology

	Dato del contatto	Obbligatorio?	Esempio
7.	Numero di telefono principale	Sì	+49 69 986692777
8.	Numero di telefono secondario		
9.	Indirizzo e-mail	Sì	john.doe@acme.com
10.	Lingua preferita	Sì	Inglese (impostazione predefinita)
11.	Altre lingue		Tedesco, francese
12.	Identificatore dell'indirizzo personale		HPC 1234
13.	Via	Sì	Bockenheimer Landstraße 97-99
14.	Codice postale	Sì	60325
15.	Città	Sì	Francoforte
16.	Stato/Provincia		
17.	Paese	Sì	Germania

Tabella 2. Dati di contatto

Nota importante:

Si consiglia di assegnare almeno un sostituto per ogni contatto. Qualora un contatto non sia temporaneamente disponibile o abbandoni l'azienda, qualcun altro potrà gestire i dati di partecipante della vostra azienda.
Qualora sia necessario assegnare un nuovo contatto (nel caso non ne siano rimasti altri validi), è necessario seguire un processo complesso. Il nostro processo garantisce che solo le persone che possono dimostrare di essere autorizzate a rappresentare legalmente l'azienda possano approvare l'assegnazione di un nuovo contatto principale.

4.3.2.8. Pubblicazione e condivisione

Lo scopo principale di TISAX è quello di pubblicare il risultato della vostra valutazione rendendolo disponibile per gli altri partecipanti TISAX e di condividerlo con il/i vostro/i partner.

Potete decidere se pubblicare e condividere il risultato della valutazione durante la procedura di registrazione o in qualsiasi momento successivo.

Se avete deciso di intraprendere il processo TISAX in via preventiva, potete già decidere di pubblicare il risultato della valutazione e renderlo disponibile alla comunità dei partecipanti TISAX. Per il resto, non dovete preparare nient'altro in questa fase.

Se è stato il vostro partner a chiedervi di sottoporvi al processo TISAX, prima o poi dovrete condividere il risultato della valutazione. È possibile condividere le informazioni sullo stato con

il partner già durante la registrazione. Una volta che il risultato della valutazione sarà disponibile, il vostro partner sarà automaticamente autorizzato ad accedervi[6].

Per condividere le informazioni sullo stato sono necessarie due cose:

1. L'ID Partecipante TISAX del vostro partner

   L'ID Partecipante TISAX identifica il vostro partner come partecipante TISAX.

   Solitamente, è il vostro partner a dovervi fornire il suo ID Partecipante TISAX.

   Per comodità, il nostro modulo di registrazione offre un elenco a discesa di ID Partecipante per alcune aziende che ricevono frequentemente risultati di valutazione condivisi.[7]

2. Il livello di condivisione necessario

   Il livello di condivisione definisce il grado di accesso al risultato della valutazione da parte del vostro partner.

   Il vostro partner può richiedere un livello di condivisione specifico oppure potete decidere voi fino a quale livello concedergli l'accesso al risultato della valutazione.

   Per maggiori informazioni sui livelli di condivisione, si veda Sezione 6.5, "Livelli di condivisione".

Assicuratevi quindi di disporre di queste informazioni.

Attenzione:

- Potete sempre decidere di pubblicare il risultato della vostra valutazione in un secondo momento.
- Potete sempre creare un'autorizzazione di condivisione per il vostro partner in un secondo momento.

Nota importante:

Se non pubblicate o non condividete il risultato della vostra valutazione, nessuno potrà vederlo.

Nota importante:

Non è possibile annullare la pubblicazione o la condivisione.

Per maggiori informazioni, si veda Sezione 6.4, "Permanenza dei risultati scambiati".

Attenzione:

Può sembrare assurdo, ma in realtà potete condividere il “risultato della valutazione” anche se il processo di valutazione non è ancora iniziato. In questa fase iniziale, condividerete solo lo “stato della valutazione”. Il partecipante con cui condividete il “risultato della valutazione” vedrà in quale fase del processo di valutazione si trova la vostra azienda.

Alcuni partecipanti TISAX devono rilasciare una liberatoria apposita per mostrare le etichette TISAX quando il processo di valutazione non è ancora terminato. In questo caso, il vostro partner potrebbe aver bisogno di vedere lo “stato della valutazione” della vostra azienda nel suo account del portale ENX.

Per maggiori informazioni sullo stato della valutazione, si veda Sezione 7.6, “Allegato: Assessment status (Stato della valutazione)”.

Per maggiori informazioni sulla pubblicazione e la condivisione del risultato della valutazione, si veda Sezione 6, “Scambio (fase 3)”.

4.3.3. Obiettivi di valutazione

L’obiettivo (o gli obiettivi) di valutazione devono essere definiti durante la procedura di registrazione. L’obiettivo di valutazione (assessment objective) determina i requisiti applicabili che il sistema di gestione della sicurezza delle informazioni (ISMS) della vostra azienda deve soddisfare. L’obiettivo di valutazione si basa interamente sul tipo di dati che gestite per conto del vostro partner.

Le sezioni seguenti contengono una descrizione degli obiettivi di valutazione e consigli su come selezionare quelli più adatti per la vostra azienda.

L’uso degli obiettivi di valutazione semplifica la comunicazione relativa a TISAX con il vostro partner e con i nostri fornitori di audit TISAX, in quanto si riferiscono a un elemento specifico a monte del processo di valutazione TISAX.

Attenzione:

Alcuni partner potrebbero chiedere alla vostra azienda di sottoporsi a una valutazione TISAX con un determinato “livello di valutazione” (assessment level, AL) invece di specificare un obiettivo di valutazione.

Per maggiori informazioni sui livelli di valutazione, si veda Sezione 4.3.3.5, “Esigenze di protezione e livelli di valutazione” (sotto-sezione “Informazioni aggiuntive”).

4.3.3.1. Elenco degli obiettivi di valutazione

Attualmente sono disponibili 12 obiettivi di valutazione TISAX. È necessario selezionarne almeno uno, ma si può selezionare anche più di un obiettivo.

Considerate l'obiettivo di valutazione come il punto di riferimento per il sistema di gestione della sicurezza delle informazioni della vostra azienda. L'obiettivo di valutazione è un elemento fondamentale a monte del processo TISAX. Tutti i fornitori di audit TISAX basano la propria strategia di valutazione principalmente sull'obiettivo di valutazione.

Gli attuali obiettivi di valutazione TISAX sono:

N.	Nome	Descrizione
1.	Info high	Handling of information with high protection needs Gestione delle informazioni con esigenze di protezione elevate
2.	Info very high	Handling of information with very high protection needs Gestione delle informazioni con esigenze di protezione molto elevate
3.	Confidential	Handling of information with high protection needs in the context of confidentiality (access to confidential information) Gestione delle informazioni con esigenze di protezione elevate in termini di riservatezza (accesso a informazioni riservate)
4.	Strictly confidential	Handling of information with very high protection needs in the context of confidentiality (access to strictly confidential information) Gestione delle informazioni con esigenze di protezione molto elevate in termini di riservatezza (accesso a informazioni strettamente riservate)

N.	Nome	Descrizione
5.	High availability	Handling of information with high protection needs in the context of *availability* (high availability of information) Gestione delle informazioni con esigenze di protezione elevate in termini di *disponibilità* (disponibilità delle informazioni elevata)
6.	Very high availability	Handling of information with very high protection needs in the context of *availability* (very high availability of information) Gestione delle informazioni con esigenze di protezione molto elevate in termini di *disponibilità* (disponibilità delle informazioni molto elevata)
7.	Proto parts	Protection of Prototype Parts and Components Protezione di parti e componenti di prototipi
8.	Proto vehicles	Protection of Prototype Vehicles Protezione di prototipi di veicoli
9.	Test vehicles	Handling of Test Vehicles Gestione dei veicoli di prova
10.	Proto events	Protection of Prototypes during Events and Film or Photo Shoots Protezione dei prototipi durante eventi e riprese cinematografiche o fotografiche

N.	Nome	Descrizione
11.	Data	Data protection according to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR) Protezione dei dati ai sensi dell’articolo 28 (“Responsabile del trattamento”) del Regolamento generale europeo sulla protezione dei dati (GDPR)
12.	Special data	Data protection according to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR) with special categories of personal data as specified in Article 9 of the GDPR Protezione dei dati relativamente a categorie particolari di dati personali ai sensi dell’articolo 28 (“Responsabile del trattamento”) e come specificato nell’articolo 9 del Regolamento generale europeo sulla protezione dei dati (GDPR)

Tabella 3. Gli attuali obiettivi di valutazione TISAX

Esempio: se la vostra azienda effettua test drive su strade pubbliche, l’obiettivo di valutazione “Test vehicles” è uno dei vostri obiettivi di valutazione.

Attenzione:

È possibile selezionare gli obiettivi di valutazione “Info high” e “Info very high” solo fino al 31 marzo 2024.

È possibile selezionare gli obiettivi di valutazione “Confidential” e “Strictly confidential” solo dal 1 aprile 2024.

Per maggiori informazioni su questa transizione, si veda il seguente articolo di notizie sul nostro sito web:
CHANGES TO TISAX LABELS ACCOMPANYING ISA 6 RELEASE
enx.com/en-US/news/Changes-to-TISAX-Labels-ISA-six-Release/

Nota importante:

All’interno di TISAX, l’“obiettivo di valutazione” è generalmente l’elemento a monte del processo. Tuttavia alcuni partner potrebbero chiedere alla vostra azienda di sottoporsi a una valutazione TISAX con un determinato “livello di valutazione” (AL).

Per maggiori informazioni sulla relazione tra esigenze di protezione e livelli di valutazione, si veda Sezione 4.3.3.5, “Esigenze di protezione e livelli di valutazione”.

4.3.3.2. Obiettivi di valutazione e ISA

L’ISA include tre cataloghi di criteri (sicurezza delle informazioni, protezione dei prototipi, protezione dei dati). Ciascun catalogo di criteri è composto dalle cosiddette “domande di controllo” e dai relativi requisiti.

Ciascun obiettivo di valutazione definisce:

- il/i catalogo/cataloghi di criteri dell’ISA applicabile/i
- le domande di controllo a cui dovete rispondere
- i requisiti che dovete soddisfare

Per alcuni obiettivi di valutazione è applicabile solo un sottoinsieme delle domande di controllo e dei requisiti.

Per ulteriori informazioni di base sugli obiettivi di valutazione TISAX e sulle domande di controllo e i requisiti applicabili, si veda Sezione 5.2.2, “Come interpretare il documento ISA”.

4.3.3.3. Obiettivi di valutazione ed etichette TISAX

Il vostro partner potrebbe fare riferimento alle “etichette TISAX”. Gli “obiettivi di valutazione” e le “etichette TISAX” indicano praticamente lo stesso concetto. La differenza è che si inizia il processo di valutazione con gli “obiettivi di valutazione” e, se si supera la valutazione, si ricevono le “etichette TISAX” corrispondenti.

Esempio: il vostro partner chiede alla vostra azienda di ottenere l’etichetta TISAX “Info high”, quindi selezionate “Info high” come vostro obiettivo di valutazione.

La figura di seguito mostra gli elementi a monte e a valle del processo TISAX:

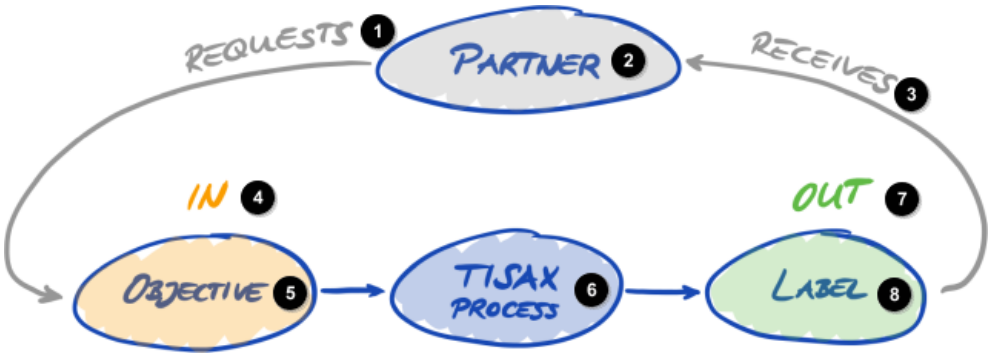


Figura 6. Obiettivi di valutazione ed etichette TISAX

1. Richiede
2. Partner
3. Riceve
4. A MONTE
5. Obiettivo
6. Processo TISAX
7. A VALLE
8. Etichetta

Per maggiori informazioni sulle etichette TISAX, si veda Sezione 5.4.14, “Etichette TISAX”.

4.3.3.4. Selezione degli obiettivi di valutazione

Idealmente, è il vostro partner a dirvi con precisione quali obiettivi di valutazione dovete raggiungere.

La scelta dell’obiettivo di valutazione è invece a vostra discrezione se:

a. volete sottoporre la vostra azienda a una valutazione TISAX prima che sia un partner a chiedervelo, oppure
b. il vostro partner non specifica l’obiettivo di valutazione che dovete raggiungere.

Nota importante:

A questo punto, consigliamo vivamente di tenere in considerazione anche gli altri vostri partner. Sono presenti partner con requisiti uguali o superiori? Prevedete che i partner futuri avranno requisiti più elevati?

Valutate la possibilità di selezionare obiettivi di valutazione con esigenze di protezione maggiori. In questo modo eviterete problemi nel caso in cui altri

> partner abbiano requisiti più elevati.

Se dovete scegliere l'obiettivo di valutazione a vostra discrezione, vi sarà utile considerare i seguenti aspetti:

N.	Obiettivo di valutazione	Informazioni
1.	Info high	Potete desumere le esigenze di protezione (elevate, molto elevate) dalla classificazione dei documenti del vostro partner.
2.	Info very high	
3.	Confidential	Per tutte le aziende che ricevono e trattano informazioni con esigenze di protezione elevate in termini di riservatezza o che sono normalmente classificate come riservate secondo lo schema di classificazione dell'azienda (ad es. White Paper VDA, "Harmonization of classification levels"). Occorre selezionare questa etichetta TISAX in particolare se una divulgazione non autorizzata delle informazioni potrebbe potenzialmente causare danni considerevoli (ad es. danni reputazionali, conseguenze penali o un danno economico).
4.	Strictly confidential	Per tutte le aziende che ricevono e trattano informazioni con esigenze di protezione molto elevate in termini di riservatezza o che sono normalmente classificate come strettamente riservate o segrete secondo lo schema di classificazione dell'azienda (ad es. White Paper VDA, "Harmonization of classification levels"). Occorre selezionare questa etichetta TISAX in particolare se la divulgazione non autorizzata delle informazioni potrebbe potenzialmente causare una minaccia esistenziale o danni catastrofici (ad es. danni reputazionali, conseguenze penali gravi o un danno economico molto elevato).
5.	High availability	Per tutte le aziende presso le quali la capacità di produzione o consegna dei relativi clienti dipende dalla disponibilità dei prodotti o servizi dell'azienda stessa e per le quali un inadempimento causerebbe danni considerevoli ai clienti in un breve periodo di tempo. Esempio: fornitori "just-in-time" di materiali di produzione.

N.	Obiettivo di valutazione	Informazioni
6.	Very high availability	Per tutte le aziende presso le quali la capacità di produzione o consegna dei relativi clienti dipende dalla disponibilità a breve termine dei prodotti e servizi dell'azienda stessa e per le quali un inadempimento causerebbe danni significativi ai clienti in un periodo di tempo molto breve. Esempio: fornitori "just-in-time" per i quali un inadempimento può causare un blocco totale della produzione con tempi di ripresa molto lunghi in un breve periodo di tempo.
7.	Proto parts	Per tutte le aziende che producono, immagazzinano o utilizzano parti o componenti forniti dai clienti, classificati come soggetti a protezione presso le proprie sedi. I requisiti relativi alla sicurezza fisica e alla sicurezza dell'area circostante, i requisiti organizzativi e i requisiti specifici per la gestione dei prototipi fanno parte della valutazione.
8.	Proto vehicles	Per tutte le aziende che producono, immagazzinano o utilizzano veicoli fornite dai clienti, classificati come soggetti a protezione presso le proprie sedi. I requisiti relativi alla sicurezza fisica e alla sicurezza dell'area circostante (compresa l'esistenza di garage e officine protetti), i requisiti organizzativi e i requisiti specifici per la gestione dei prototipi fanno parte della valutazione. Una volta superata la valutazione, riceverete automaticamente l'etichetta TISAX "Protezione di parti e componenti di prototipi".

N.	Obiettivo di valutazione	Informazioni
9.	Test vehicles	Per tutte le aziende che effettuano collaudi e test drive (ad esempio, test drive su strade pubbliche o piste di prova) con veicoli forniti dai clienti classificati come soggetti a protezione. I requisiti organizzativi e i requisiti specifici per la gestione dei prototipi, compresa la mimetizzazione e la gestione dei veicoli durante i test drive su strade pubbliche e piste di prova, fanno parte della valutazione. I requisiti relativi alla sicurezza fisica e alla sicurezza dell'area circostante non fanno necessariamente parte della valutazione. Se le vostre sedi sono adeguatamente equipaggiate, vi consigliamo di selezionare anche l'obiettivo di valutazione "Protezione di prototipi di veicoli".
10.	Proto events	Per tutte le aziende che organizzano presentazioni o eventi (ad esempio, ricerche di mercato, eventi, eventi di marketing) e riprese cinematografiche e fotografiche con parti, veicoli o componenti forniti dai clienti e classificati come soggetti a protezione. I requisiti organizzativi e i requisiti specifici per la gestione dei prototipi, compresi i requisiti per le presentazioni, gli eventi e le riprese cinematografiche e fotografiche in locali protetti e in aree pubbliche, fanno parte della valutazione. I requisiti relativi alla sicurezza fisica e alla sicurezza dell'area circostante non fanno necessariamente parte della valutazione. Se le vostre sedi sono adeguatamente equipaggiate, vi consigliamo di selezionare anche l'obiettivo di valutazione "Protezione di prototipi di veicoli".
11.	Data	Se la vostra azienda tratta dati personali in qualità di responsabile del trattamento ai sensi dell'articolo 28 del GDPR, probabilmente dovrete selezionare "Data".

N.	Obiettivo di valutazione	Informazioni
12.	Special data	Se la vostra azienda tratta categorie particolari di dati personali (ad esempio relativi alla salute o al credo religioso) in qualità di responsabile del trattamento ai sensi dell'articolo 28 del GDPR, probabilmente dovrete selezionare "Special data".

Tabella 4. Consigli per la selezione di un obiettivo di valutazione

Spiegazioni aggiuntive:

- Se avete ricevuto requisiti precisi dal vostro partner, solitamente non è necessario discutere degli obiettivi di valutazione con quest'ultimo. Se invece non vi sono stati forniti requisiti precisi dal partner, consigliamo vivamente di confrontarvi con quest'ultimo prima di avviare il processo di valutazione.
- L'ISA illustra la differenza di implementazione tra le esigenze di protezione "elevate" e quelle "molto elevate" (se presenti) per ciascun requisito.
  Per maggiori informazioni su questo aspetto, si veda Figura 11, "Screenshot: Elementi principali delle domande del catalogo di criteri ISA "Sicurezza delle informazioni"".

4.3.3.5. Esigenze di protezione e livelli di valutazione

Il vostro partner dispone di informazioni di vario tipo e alcune di queste possono necessitare un livello di protezione più elevato rispetto ad altre. L'ISA tiene conto di questo aspetto distinguendo tra tre "esigenze di protezione" (🇬🇧 "protection needs"): normali, elevate e molto elevate. È il vostro partner a classificare le proprie informazioni e ad assegnare solitamente le esigenze di protezione.

Quanto maggiori sono le esigenze di protezione, tanto più il vostro partner è interessato ad assicurarsi che gestiate le sue informazioni in maniera sicura. Per questo motivo TISAX prevede tre "livelli di valutazione" (AL) diversi. Il livello di valutazione stabilisce il metodo di valutazione che il fornitore di audit deve applicare. Un livello di valutazione più elevato richiede un lavoro maggiore, che si traduce in una valutazione più scrupolosa e accurata.

Nella tabella seguente sono indicati i livelli di valutazione che si applicano agli obiettivi di valutazione TISAX:

N.	Obiettivo di valutazione TISAX	Livello di valutazione (AL)
1.	Info high	AL 2
2.	Info very high	AL 3
3.	Confidential	AL 2
4.	Strictly confidential	AL 3

N.	Obiettivo di valutazione TISAX	Livello di valutazione (AL)
5.	High availability	AL 2
6.	Very high availability	AL 3
7.	Proto parts	AL 3
8.	Proto vehicles	AL 3
9.	Test vehicles	AL 3
10.	Proto events	AL 3
11.	Data	AL 2
12.	Special data	AL 3

Tabella 5. Corrispondenza tra gli obiettivi di valutazione TISAX e i livelli di valutazione

Livello di valutazione 1 (AL 1):

Le valutazioni nel livello di valutazione 1 hanno finalità principalmente interne e corrispondono a un'autovalutazione (self-assessment) vera e propria.

Durante una valutazione nel livello di valutazione 1, l'auditor verifica che sia stata completata un'autovalutazione. Non valuta il contenuto dell'autovalutazione e non necessita di ulteriori prove.

I risultati delle valutazioni nel livello di valutazione 1 hanno un grado di affidabilità basso e quindi non vengono utilizzati all'interno di TISAX. È tuttavia possibile che il vostro partner richieda un'autovalutazione di questo tipo al di fuori di TISAX.

Livello di valutazione 2 (AL 2):

Per una valutazione nel livello di valutazione 2, il fornitore di audit controlla l'attendibilità della vostra autovalutazione (per tutte le sedi che rientrano nell'ambito di valutazione). Esegue questo controllo verificando le prove[8] e conducendo un colloquio con il responsabile della sicurezza delle informazioni.

Il fornitore di audit effettua il colloquio generalmente tramite videoconferenza; tuttavia, su richiesta dell'azienda, il colloquio può essere svolto anche di persona.

Se disponete di prove che non volete inviare al fornitore di audit, potete richiedere un'ispezione in loco. In questo modo, il fornitore di audit potrà comunque controllare le vostre prove strettamente riservate.

Attenzione:

Esiste un metodo alternativo per condurre una valutazione nel livello di valutazione 2. Invece di controllare l'attendibilità, il fornitore di audit conduce una valutazione completa a distanza. Questo metodo viene talvolta definito "**livello di valutazione 2.5**".

Rispetto a una valutazione nel livello di valutazione 2, l'auditor *verifica* che l'ISMS della vostra azienda soddisfi i requisiti applicabili. Tuttavia, a differenza di una valutazione nel livello di valutazione 3, l'auditor non conduce le attività in loco descritte nella sezione dedicata al livello di valutazione 3 riportata di seguito.

Una valutazione di questo tipo viene formalmente considerata una valutazione in AL 2.

Il vantaggio dell'AL 2.5 è che l'approccio è metodologicamente compatibile con AL 3. In un momento successivo è quindi possibile passare a una valutazione in AL 3 a tutti gli effetti con il minimo sforzo. Per effettuare questo passaggio, l'auditor deve solo condurre le attività in loco descritte nella sezione relativa ad AL 3 riportata di seguito.

Consigliamo di effettuare valutazioni nel livello di valutazione 2.5 nei seguenti casi:

1. Se al momento avete bisogno solo di etichette TISAX che implicano una valutazione in AL 2, ma non potete escludere che altri partner possano richiedere etichette TISAX che implichino una valutazione in AL 3. Una valutazione in AL 2.5 offre sempre la possibilità per un successivo passaggio ad AL 3.
2. Se riscontrate difficoltà nell'eseguire un'autovalutazione sufficientemente attendibile. Per superare il controllo di attendibilità, l'autovalutazione deve essere definitiva, facilmente comprensibile e comprovata.
   Un'autovalutazione di questo tipo può comportare un notevole lavoro interno, anche per le aziende che godono fondamentalmente di un buon posizionamento.

Per maggiori informazioni sull'aggiornamento del livello di valutazione, si veda Sezione 7.10, "Allegato: Valutazione di estensione dell'ambito".

Questa alternativa è facoltativa e non è necessaria per soddisfare i requisiti di AL 2. La differenza tra AL 2 e AL 2.5 non sarà visibile per i partner con cui condividerete il risultato della valutazione.

Livello di valutazione 3 (AL 3):

Per una valutazione nel livello di valutazione 3, il fornitore di audit esegue una verifica completa della conformità della vostra azienda ai requisiti applicabili. Per preparare la valutazione, l'auditor si avvale dell'autovalutazione e della documentazione presentata. Tuttavia, a differenza del livello di valutazione 2, l'auditor verificherà tutto, eseguendo le seguenti operazioni:

- esaminerà documenti e prove
- effettuerà colloqui programmati con i responsabili dei processi
- analizzerà le condizioni locali
- osserverà lo svolgimento dei processi
- effettuerà colloqui *non* programmati con i soggetti coinvolti nei processi

Attenzione:

I contenuti che seguono fanno riferimento a diversi concetti che verranno spiegati solo più avanti nel presente documento.

Se si sceglie AL 3, il fornitore di audit deve recarsi presso la/e vostra/e sede/i. Qualora, per qualsiasi motivo, ciò non sia temporaneamente possibile in alcun modo o richieda sforzi eccessivi, il fornitore di audit può utilizzare il **metodo di valutazione a distanza con supporto video** per condurre le attività di valutazione in loco.

Il fornitore di audit registrerà questa circostanza nella relazione della valutazione TISAX come una non conformità minore. Non appena il fornitore di audit può recarsi presso la/e vostra/e sede/i, dovrà condurre una valutazione di follow-up che includa tutte le attività in loco che non è stato possibile eseguire in precedenza. Dovrete inoltre programmare la valutazione di follow-up anche se non avete ancora completato le altre azioni correttive.

Rispetto a dover attendere che il fornitore di audit sia disponibile per eseguire le attività in loco, questo approccio vi consente di condividere già le etichette TISAX temporanee con il vostro partner.

Livelli di valutazione e metodi di valutazione

La tabella seguente offre una panoramica semplificata dei metodi di audit associati a ciascun livello di valutazione:

Metodo di valutazione	Livello di valutazione 1 (AL 1)	Livello di valutazione 2 (AL 2)	Livello di valutazione 3 (AL 3)
Autovalutazione	Sì	Sì	Sì
Prove	No	Controllo di attendibilità	Verifica completa
Colloqui	No	Tramite videoconferenza[9]	Di persona, in sede
Ispezione in loco	No	Su richiesta dell'azienda	Sì

Tabella 6. Attribuzione dei metodi di valutazione ai vari livelli di valutazione

Informazioni aggiuntive:

- Differenza tra AL 2 e AL 3
  Dal punto di vista metodologico, i due approcci differiscono in modo significativo. Per le valutazioni nel livello di valutazione 2, l'auditor non verificherà tutto. Si limiterà solo a controllare l'attendibilità. Pertanto, il fornitore di audit non può utilizzare i risultati di una valutazione nel livello di valutazione 2 come base per passare al livello di valutazione 3. Le operazioni da eseguire per passare al livello di valutazione 3 sono essenzialmente le stesse di una nuova valutazione iniziale.
- Controllo di attendibilità vs. verifica
  Un controllo di attendibilità consiste, in termini estremamente semplici, nel verificare l'esistenza e l'*apparente* correttezza di un determinato elemento. Al contrario, durante una verifica viene effettivamente controllato che un determinato elemento corrisponda a quanto dichiarato.
- Classificazione delle informazioni ed esigenze di protezione
  La corrispondenza tra la classificazione delle informazioni (ad esempio riservate o segrete) e le esigenze di protezione può variare da partner a partner. Pertanto, per quanto ci piacerebbe, non possiamo semplicemente fornirvi una tabella con la corrispondenza esatta tra la classificazione delle informazioni del vostro partner e un'esigenza di protezione.
- La sola conoscenza del livello di valutazione non è sufficiente
  Alcuni partner potrebbero chiedere alla vostra azienda di sottoporsi a una valutazione TISAX con un determinato livello di valutazione. Precisiamo tuttavia che la sola conoscenza del livello di valutazione non è sufficiente per avviare il processo TISAX. Un livello di valutazione ha senso solo se abbinato a un catalogo di criteri dell'ISA e a una corrispondente esigenza di protezione. Di solito i partner chiedono alle aziende di ottenere un'etichetta TISAX (catalogo di criteri più esigenza di protezione). Tuttavia, dal momento che le esigenze di protezione corrispondono 1:1 ai livelli di valutazione, è sufficiente conoscere il catalogo (o

i cataloghi) di criteri e il livello di valutazione.

- Gerarchia dei livelli di valutazione
  I livelli di valutazione superiori includono sempre quelli inferiori. Ad esempio, se la vostra valutazione si basa sul livello di valutazione 3, essa soddisferà automaticamente tutti requisiti del livello di valutazione 2.
- I nostri consigli sui livelli di valutazione
  Se dovete selezionare un obiettivo di valutazione (e quindi implicitamente un livello di valutazione corrispondente) a vostra discrezione, vi consigliamo di scegliere obiettivi di valutazione che implichino un livello di valutazione 3. Il lavoro richiesto dalle valutazioni TISAX nel livello di valutazione 3 non è generalmente superiore a quelle nel livello di valutazione 2.
  I fornitori con più partner spesso selezionano obiettivi di valutazione che implicano un livello di valutazione 3. In questo modo, sono preparati a gestire tutte le richieste future e non devono preoccuparsi di altri livelli di valutazione.
- Ulteriori considerazioni commerciali
  Per quanto riguarda i livelli di valutazione, il costo totale di una valutazione TISAX è rappresentato dalla somma delle operazioni interne e del costo della valutazione. Sebbene il costo di una valutazione nel livello di valutazione 2 sia inferiore, le operazioni che dovrete eseguire all'interno della vostra azienda potrebbero essere maggiori. Ciò è dovuto al fatto che una valutazione nel livello di valutazione 2 necessita solitamente di un'autovalutazione più completa e di una documentazione interna più accurata. Per le valutazioni nel livello di valutazione 3, dimostrare come si opera e presentare una documentazione di base è spesso sufficiente per l'auditor in termini di prove. Tuttavia, in mancanza di un'ispezione in loco, l'auditor richiederà una documentazione precisa. Per questo motivo, non è raro che venga scelto il livello di valutazione 3 invece che il livello di valutazione 2. Questa scelta viene comunque fatta dalle aziende più piccole rispetto a quelle più grandi.

4.3.3.6. Obiettivi di valutazione e fornitori della vostra azienda

Con TISAX non è necessario sottoporre tutti i fornitori della vostra azienda agli stessi requisiti. Se il vostro obiettivo di valutazione è "Sicurezza delle informazioni con esigenze di protezione *molto* elevate", ciò NON significa automaticamente che i vostri fornitori debbano raggiungere lo stesso obiettivo di valutazione. Non significa nemmeno che debbano avere etichette TISAX.

Tuttavia, per tutti i vostri fornitori, dovete comunque verificare se l'utilizzo dei loro servizi aumenti i rischi o ne introduca di nuovi.

Di seguito sono riportati due esempi estremamente semplificati:

1. La politica della vostra azienda prevede che la posta elettronica normale non possa essere utilizzata per dati con esigenze di protezione molto elevate. Pertanto, non è necessario che il vostro provider di posta elettronica ottenga l'etichetta TISAX con esigenze di protezione molto elevate.

Lo stesso vale se si inviano solo e-mail crittografate e il provider di posta elettronica non è in grado di visualizzare nessuno dei dati con esigenze di protezione molto elevate.

2. All'interno della vostra azienda i dati stampati con esigenze di protezione molto elevate vengono smaltiti tramite distruggidocumenti. In questo caso, ovviamente, il fornitore dei servizi di smaltimento dei rifiuti non deve soddisfare i vostri stessi requisiti.

Tuttavia, la valutazione dei rischi può rivelare che anche il vostro fornitore deve soddisfare i requisiti per le esigenze di protezione molto elevate. In questo caso, le etichette TISAX sono un'opzione per ottenere tali dimostrazioni.

4.3.4. Tariffa

Il nostro servizio è a pagamento; nel nostro listino prezzi troverete informazioni sulle tariffe applicabili, sui possibili sconti e sulle nostre condizioni di pagamento.

È possibile scaricare il listino prezzi dal nostro sito web al seguente indirizzo:
enx.com/en-US/TISAX/downloads/
Download diretto del PDF:
enx.com/pricelist.pdf

Durante i preparativi per la registrazione è importante tenere conto di alcuni aspetti relativi alla fatturazione:

- Selezione dell'indirizzo di fatturazione
  Per impostazione predefinita, la fattura verrà inviata all'indirizzo indicato come sede del partecipante. Potete tuttavia indicare un indirizzo diverso per la ricezione della fattura.

Nota importante:

Assicuratevi che l'indirizzo di fatturazione sia corretto. Le leggi contabili prevedono che l'indirizzo presente sulla nostra fattura corrisponda esattamente all'indirizzo (di fatturazione) della vostra azienda. Per motivi di conformità, non è possibile modificare un indirizzo di fatturazione una volta emessa la fattura.

- Ordine di riferimento
  Se è necessario che la nostra fattura riporti un numero d'ordine d'acquisto specifico o un dato simile, potete fornirci l'ordine di riferimento.
- Numero di partita IVA
  Tutte le nostre tariffe sono soggette all'imposta sul valore aggiunto (IVA) tedesca, se applicabile.
  Abbiamo bisogno di questo numero di partita IVA per elaborare i pagamenti provenienti dall'UE. È obbligatorio fornire un numero di partita IVA se il vostro indirizzo di fatturazione si trova in uno dei seguenti Paesi:

Austria, Belgio, Bulgaria, Croazia, Cipro (parte greca), Repubblica Ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, Irlanda, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia, Portogallo, Slovacchia, Slovenia, Spagna, Svezia, Regno Unito.

- Gestione dei fornitori

Nota importante:

Precisiamo che, a causa del rapporto di reciprocità tra tutti i partecipanti TISAX, non possiamo accettare condizioni aggiuntive (come, ad esempio, condizioni generali di acquisto, codici di condotta).

Informazioni aggiuntive sul nostro processo di fatturazione:

- Non possiamo accettare condizioni di acquisto individuali.
- Accettiamo:
  - bonifici sul conto corrente bancario indicato in fattura
  - pagamenti con carta di credito (durante la procedura di registrazione tramite il nostro fornitore di servizi di pagamento “Stripe”).
- La nostra fattura conterrà i seguenti riferimenti alla vostra registrazione:
  - Il nome e l’indirizzo e-mail del contatto principale della vostra azienda partecipante
  - Il nome dell’ambito di valutazione

  Un esempio di fattura è disponibile nell’appendice nella sezione Sezione 7.1, “Allegato: Esempio di fattura”.

- La maggior parte dei dati generalmente necessari per l’elaborazione della fattura sono riportati direttamente su di essa. Queste e altre informazioni sono disponibili nel nostro documento “Information for Members and Business Partners” (“Informazioni per i membri e i partner commerciali”). Potete scriverci un’e-mail e provvederemo a inviarvi una versione aggiornata.

Attenzione:

Siamo consapevoli che a volte il processo di approvazione dei pagamenti all’interno di un’azienda possa essere piuttosto lungo. Per questo motivo, la prosecuzione con le fasi immediatamente successive del processo TISAX non è subordinata alla ricezione del pagamento. Tuttavia, tenete presente che non è possibile condividere il risultato della vostra valutazione fino a quando non avremo ricevuto il pagamento.
Vi consigliamo pertanto di assicurarvi che la fattura venga inviata al

destinatario appropriato e che contenga il relativo ordine di riferimento, se applicabile. Potete anche verificare internamente l'avvenuto pagamento della fattura.

Nota importante:

Noi, in qualità di ENX Association, emettiamo la fattura relativa alla nostra tariffa. Questa è solo una parte del costo totale di una valutazione TISAX. Il vostro fornitore di audit TISAX fattura i costi relativi alla/e valutazione/i.

Per maggiori informazioni sui costi relativi al fornitore di audit, si veda Sezione 5.3.4, "Valutazione delle offerte".

Nota importante:

La tariffa deve essere corrisposta indipendentemente dal fatto che:

- si prosegua o meno con il processo TISAX.
- si superi con successo il processo di valutazione TISAX.

Pertanto, potreste ricevere la fattura prima di aver iniziato la valutazione iniziale.

4.4. Portale ENX

La sezione seguente descrive la procedura di registrazione online, durante la quale dovrete inserire tutti i dati raccolti, come consigliato nella sezione precedente. Prima di iniziare la procedura di registrazione online, vi illustriamo brevemente lo scopo e i vantaggi del portale ENX.

Il portale ENX ci consente di mantenere un database di tutti i partecipanti TISAX e svolge un ruolo importante durante l'intero processo TISAX. Durante la registrazione a TISAX dovrete inserire i dati della vostra azienda che i fornitori di audit TISAX potranno quindi utilizzare (se avete dato il consenso) per calcolare le loro offerte e pianificare le procedure di valutazione. Una volta completato il processo di valutazione TISAX, potrete utilizzare la piattaforma di scambio sul portale ENX per condividere il risultato della valutazione con il vostro partner.

Il portale si chiama "portale ENX" e non "portale TISAX" perché lo utilizziamo anche per gestire altre attività aziendali (come la rete ENX).

4.5. Procedura di registrazione online

Se avete eseguito tutti i preparativi in base a quanto consigliato sopra (Sezione 4.3, "Preparazione per la registrazione"), potete avviare la procedura di registrazione online.

4.5.1. Tempistiche

Il tempo necessario dipende fortemente dal numero di ambiti e sedi che registrate. Se state registrando la vostra azienda come partecipante per la prima volta con un ambito e una sede, potete aspettarvi una tempistica minima di 20 minuti.

Consigliamo di completare la registrazione in un'unica sessione, perché al momento non è semplice riprendere alcuni passaggi in un secondo momento. Qualora abbiate comunque bisogno di interrompere la procedura, vi contatteremo per chiedervi i dati mancanti.

4.5.2. Da dove iniziare

Avviate la procedura di registrazione sul nostro sito web all'indirizzo:
enx.com/en-us/Account/Login/Register?returnUrl=%2FTISAX%2Ftisax-initial-registration%2F

Non dovete fare altro che seguire le istruzioni sullo schermo, tuttavia di seguito trovate una breve descrizione della procedura.

4.5.3. Account sul portale

Per prima cosa dovete creare un account per la vostra azienda nel portale ENX. L'account sul portale è necessario per poter gestire i "dati di partecipante" della vostra azienda.

Attenzione:

Se il portale ENX dovesse informarvi che l'indirizzo e-mail da voi indicato è già in uso, contattateci. Questo messaggio potrebbe significare che per qualche motivo la vostra azienda è già presente nel nostro sistema.

Attenzione:

Come descritto, gli account sul portale non sono necessariamente "contatti del partecipante" o "contatti di ambito" (si veda sotto) con un ruolo attivo nel processo di valutazione.

Viceversa, un "contatto del partecipante" o "contatto di ambito" non include automaticamente gli stessi diritti di gestione dei dati del partecipante di un account sul portale. Ciò significa che i colleghi indicati come "contatto del partecipante" o "contatto di ambito" non possono accedere automaticamente ai dati del partecipante nel portale ENX.

Se si desidera assegnare il diritto di gestire i dati del partecipante a un contatto già creato nel portale ENX (indipendentemente dal fatto che gli sia stato assegnato un ruolo o meno), è necessario invitare il contatto in questione. Per maggiori informazioni, si veda l'ultima nota in Sezione 4.5.5, "Contatto del

partecipante”.

4.5.4. Registrazione del partecipante

Il secondo passo consiste nel registrare la propria azienda come partecipante TISAX. Con “partecipante TISAX” si intende l’azienda che scambia i risultati della valutazione con gli altri partecipanti.

4.5.5. Contatto del partecipante

Si tratta della persona generalmente responsabile di tutti gli argomenti relativi alla valutazione della sicurezza delle informazioni della vostra azienda. Potete essere voi o qualcun altro all’interno dell’azienda.

Di solito tutto ciò di cui abbiamo bisogno è il contatto principale del partecipante. Qualora desideriate che tutte le comunicazioni inviate da noi e dai nostri fornitori di audit TISAX relativamente a questa registrazione siano inviate anche ad altre persone, aggiungete ulteriori contatti del partecipante.

Nota importante:

Si consiglia di assegnare almeno un sostituto per ogni contatto. Qualora un contatto non sia temporaneamente disponibile o abbandoni l’azienda, qualcun altro potrà gestire i dati di partecipante della vostra azienda.
Qualora sia necessario assegnare un nuovo contatto (nel caso non ne siano rimasti altri validi), è necessario seguire un processo complesso. Il nostro processo garantisce che solo le persone che possono dimostrare di essere autorizzate a rappresentare legalmente l’azienda possano approvare l’assegnazione di un nuovo contatto principale.

Attenzione:

Potete sempre aggiungere o rimuovere i contatti in un momento successivo (anche una volta terminata la procedura di registrazione online e dopo aver completato le valutazioni).

Attenzione:

Non è possibile utilizzare indirizzi e-mail di gruppo per i contatti del partecipante (come “info@acme.com” o “IT@acme.com”).

Questa disposizione è in linea con i requisiti dell’ISA relativi agli accessi degli utenti.

Attenzione:

Potete scegliere se consentire a ciascun contatto di accedere ai dati di partecipante della vostra azienda Si è verificata una delle seguenti situazioni:

1. aggiungendo semplicemente il contatto in questione, che viene quindi memorizzato nel nostro sistema, ma non può accedere e gestire alcun dato,
2. oppure invitando il contatto. Il portale ENX invia quindi un'e-mail di invito al contatto, che dovrà seguire il link di invito nella stessa contenuto. Una volta creato il proprio account personale per il portale ENX, il contatto potrà gestire i dati di partecipante della vostra azienda.

Per creare un nuovo contatto: Sign in (Accedi) > MY TISAX (IL MIO TISAX) > ADMINISTRATORS (AMMINISTRATORI) > Create new TISAX Administrator (Crea nuovo amministratore TISAX)

Per invitare un contatto: Sign in (Accedi) > MY TISAX (IL MIO TISAX) > ADMINISTRATORS (AMMINISTRATORI) > Andate alla fine della riga della tabella relativa al contatto e fate clic sul pulsante con la freccia verso il baso > Edit TISAX Administrator (Modifica amministratore TISAX) > Andate alla sezione "ENX PORTAL ACCESS" (ACCESSO AL PORTALE ENX) > Impostate "INVITE THIS CONTACT" (INVITA QUESTO CONTATTO) su "Yes" (Sì) > Fate clic su "Save Contact" (Salva contatto)

4.5.6. Condizioni generali

Il terzo passaggio consiste nell'accettare le "Condizioni generali di partecipazione a TISAX".

Vi consigliamo di consultare le spiegazioni nella Sezione 4.3.1, "Le basi giuridiche".

4.5.7. Registrazione dell'ambito di valutazione

Il quarto passaggio consiste nel registrare l'ambito di valutazione della vostra valutazione della sicurezza delle informazioni.

Vi viene chiesto di eseguire le seguenti operazioni:

1. Assegnare un nome all'ambito di valutazione.
   Lo scopo principale del nome dell'ambito è quello di facilitare l'identificazione di un determinato ambito nell'elenco generale degli ambiti nel portale ENX.
   Vi consigliamo di consultare le spiegazioni nella Sezione 4.3.2.6, "Nome dell'ambito"
2. Selezionare un tipo di ambito di valutazione.
   (standard, personalizzato)
   Vi consigliamo di consultare le spiegazioni nella Sezione 4.3.2, "L'ambito di valutazione

TISAX”.

3. Specificare il contatto principale di ambito.
   Si tratta della persona generalmente responsabile della valutazione di un determinato ambito. Potete essere voi o qualcun altro all’interno dell’azienda.
   Di solito tutto ciò di cui abbiamo bisogno è il contatto principale di ambito. Qualora desideriate che tutte le comunicazioni che inviamo relativamente a questo particolare ambito siano inviate anche ad altre persone, potete aggiungere ulteriori contatti del partecipante.
4. Selezionare il/i vostro/i obiettivo/i di valutazione.
   Vi consigliamo di consultare le spiegazioni nella Sezione 4.3.3, “Obiettivi di valutazione”.
5. Aggiungere la/le sede/i dell’ambito di valutazione.
   Vi chiediamo di specificare tutte le sedi che rientrano nell’ambito di valutazione.
   Vi consigliamo di consultare le spiegazioni nella Sezione 4.3.2, “L’ambito di valutazione TISAX”.

Attenzione:

Una volta creata una nuova sede, non è possibile modificarla. Nel caso in cui siano necessarie modifiche minori (cambio della denominazione dell’azienda, errori di battitura nel nome della via, nel codice postale, nella città, ecc.), contattateci e provvederemo noi ad apportare le modifiche.

Nota importante:

Questa nota è rilevante solo se state rinnovando le etichette TISAX della vostra azienda.

Vi chiediamo di riutilizzare i dati delle sedi esistenti che avete creato e usato durante la registrazione dell’ambito precedente. Non create nuovi dati di una sede con lo stesso indirizzo.

Il motivo è che alcuni partecipanti TISAX elaborano automaticamente i risultati delle valutazioni dei loro partner sincronizzando il proprio sistema con il portale ENX. Anche piccole differenze possono bloccare la sincronizzazione. Inoltre, è importante non intasare i dati dei partecipanti con inutili doppioni.

6. Selezionare i livelli di pubblicazione e condivisione (facoltativo).
   Potete già decidere di pubblicare il risultato della vostra valutazione rendendolo disponibile agli altri partecipanti TISAX e di condividerlo con il/i vostro/i partner. Di norma, veniamo autorizzati a mostrare almeno che la vostra azienda è un partecipante e che ha superato il processo TISAX con successo.

Potete tranquillamente saltare questo passaggio durante la registrazione iniziale e definire l'accesso al risultato della vostra valutazione in un secondo momento.
Vi consigliamo di consultare le spiegazioni nella Sezione 4.3.2.8, "Pubblicazione e condivisione".

Nota importante:

Non è possibile revocare le autorizzazioni di pubblicazione o condivisione. Per maggiori informazioni, si veda Sezione 6.4, "Permanenza dei risultati scambiati".

7. Specificare il destinatario della fattura.
   Chiediamo di specificare a chi dobbiamo inviare la/e nostra/e fattura/e.
   Vi consigliamo di consultare le spiegazioni nella Sezione 4.3.4, "Tariffa".

Attenzione:

In questa fase eventuali errori hanno una rilevanza minima. Anche se in un secondo momento vi accorgete che avreste dovuto registrare un ambito leggermente diverso (avete dimenticato una sede, dovete aggiungere un altro obiettivo di valutazione, ecc.), il fornitore di audit può comunque eseguire la valutazione.

Esempio: l'auditor stabilisce che l'ambito deve contenere una ulteriore sede che inizialmente non avevate inserito. L'auditor procederà con la sua attività e successivamente aggiornerà l'ambito di valutazione nel portale ENX, caricando al tempo stesso il risultato della valutazione.

Attenzione:

Ogni ambito di valutazione ha il proprio ciclo di vita. In questa fase, lo stato dell'ambito di valutazione è "Incompleto", "In attesa dell'ordine" o "In attesa dell'approvazione di ENX".

Per maggiori informazioni sullo stato di una valutazione, si veda Sezione 7.5.1, "Panoramica: Assessment scope status (Stato dell'ambito di valutazione)".

Attenzione:

Per le aziende di grandi dimensioni con molte sedi, TISAX offre la valutazione di gruppo semplificata. Potete prendere in considerazione questa opzione se:

- il vostro ambito include almeno tre sedi[10] e

- il sistema di gestione della sicurezza delle informazioni della vostra azienda è perfettamente funzionante e organizzato a livello centrale[11].

Nel caso di una valutazione di gruppo semplificata il lavoro da fare inizialmente è maggiore, tuttavia tale sforzo viene ripagato all'aumentare del numero di sedi.

Per maggiori informazioni sulla "valutazione di gruppo semplificata", si veda il documento "TISAX Simplified Group Assessment" ("Valutazione di gruppo semplificata TISAX").

È possibile scaricare il documento "Valutazione di gruppo semplificata TISAX" dal nostro sito web all'indirizzo:
enx.com/en-US/TISAX/downloads/

Download diretto del PDF:
enx.com/sga.pdf

Attenzione:

Una volta che avremo registrato il vostro ambito di valutazione, non potrete modificarlo autonomamente.

Se potete assicurarci in maniera credibile di NON aver ancora inviato il vostro "TISAX Scope Excerpt" ("Estratto dell'ambito TISAX") ai nostri fornitori di audit, contattateci e provvederemo noi a modificarlo.

Se avete già inviato il vostro "TISAX Scope Excerpt" ("Estratto dell'ambito TISAX") a uno (o più) dei nostri fornitori di audit, create semplicemente la/le nuova/e sede/i nel portale ENX (se applicabile) e discutete di qualsiasi modifica con il vostro fornitore di audit. Il fornitore di audit condurrà la valutazione in base alle modifiche e aggiornerà le informazioni sull'ambito nel portale ENX.

Attenzione:

Non potete cancellare autonomamente un ambito di valutazione nel portale ENX. Se avete creato un ambito di valutazione per errore, contattateci e provvederemo noi a cancellarlo.

4.5.8. E-mail di conferma

Una volta completati tutti i passaggi obbligatori di cui sopra, controlleremo la vostra domanda e vi invieremo un'e-mail di conferma.

Questa e-mail contiene due elementi importanti:

- Un elenco con i contatti di tutti i fornitori di audit TISAX
  Dovete scegliere uno dei nostri fornitori di audit TISAX che conduca una valutazione del vostro ambito di valutazione. Potete utilizzare questi contatti per richiedere offerte.
  Per maggiori informazioni sulla selezione del fornitore di audit, si veda Sezione 5.3, “Selezione del fornitore di audit”.
- Il “TISAX Scope Excerpt” (“Estratto dell’ambito TISAX”) sotto forma di file PDF allegato.

  Questo documento contiene:

  - Le informazioni che abbiamo archiviato nel nostro database
  - Il vostro ID Partecipante
    Si veda Sezione 4.5.8.1, “Participant ID (ID Partecipante)” qui di seguito.
  - Il/I vostro/i ID Ambito
    Si veda Sezione 4.5.8.2, “Scope ID (ID Ambito)” qui di seguito.

Per un esempio della nostra e-mail di conferma, si veda Sezione 7.2, “Allegato: Esempio di e-mail di conferma”.

Per un esempio del “TISAX Scope Excerpt” (“Estratto dell’ambito TISAX”), si veda Sezione 7.3, “Allegato: Esempio dell’Estratto dell’ambito TISAX”.

Generalmente la nostra e-mail di conferma viene inviata entro tre giorni lavorativi.

Se non venite contattati entro sette giorni lavorativi, verificate a) di aver fornito tutte le informazioni e b) che lo stato dell’ambito di valutazione sia “In attesa dell’approvazione di ENX”. Inizieremo a elaborare la vostra registrazione solo quando tutte le informazioni saranno complete. Se ritenete che tutte le informazioni siano complete, ma non avete ancora ricevuto nessuna comunicazione da parte nostra, contattateci.

L’e-mail di conferma viene inviata al contatto principale del partecipante.

Attenzione:

Ogni ambito di valutazione ha il proprio ciclo di vita. In questa fase, lo stato dell’ambito di valutazione è “In attesa dell’approvazione di ENX”.

Per maggiori informazioni sullo stato di una valutazione, si veda Sezione 7.5.5, “Assessment scope status “Awaiting your payment” (Stato dell’ambito di valutazione “In attesa del pagamento”)”.

Le due sotto-sezioni riportate di seguito forniscono informazioni dettagliate sullo scopo del vostro ID Partecipante e ID Ambito.

4.5.8.1. Participant ID (ID Partecipante)

L'ID Partecipante:

- identifica un partecipante TISAX.
- è univoco per ciascun partecipante.
- viene assegnato da noi al completamento della registrazione.
- è un prerequisito per richiedere una valutazione della sicurezza delle informazioni da parte di uno dei nostri fornitori di audit TISAX.
- ha l'aspetto seguente:

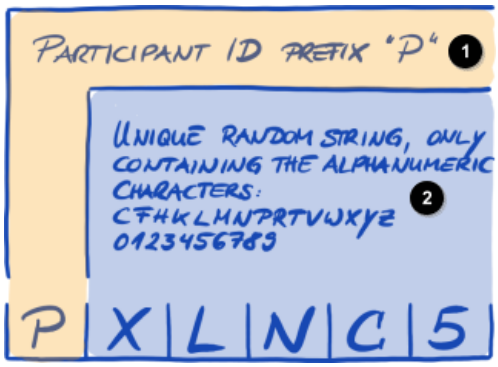


Figura 7. Formato dell'ID Partecipante[12]

1. Prefisso "P" dell'ID Partecipante
2. Stringa casuale e univoca contenente solo le seguenti lettere e i seguenti numeri:
   CFHKLMNPRTVWXYZ
   0123456789

Attenzione:

Esistono due modi per trovare il proprio ID Partecipante:

1. Verificate all'interno del vostro "TISAX Scope Excerpt" ("Estratto dell'ambito TISAX").
   Si veda Sezione 4.5.8, "E-mail di conferma" di cui sopra.
2. Accedete al portale ENX, andate alla barra di navigazione principale e selezionate "DASHBOARD" ("DASHBOARD"). Qui troverete il vostro ID Partecipante.

4.5.8.2. Scope ID (ID Ambito)

L'ID Ambito:

- identifica un ambito di valutazione.

- è univoco per ciascun ambito di valutazione.
- viene assegnato da noi al completamento della registrazione.
- è un prerequisito per poter richiedere una valutazione della sicurezza delle informazioni da parte di uno dei nostri fornitori di audit TISAX.
- ha l'aspetto seguente:

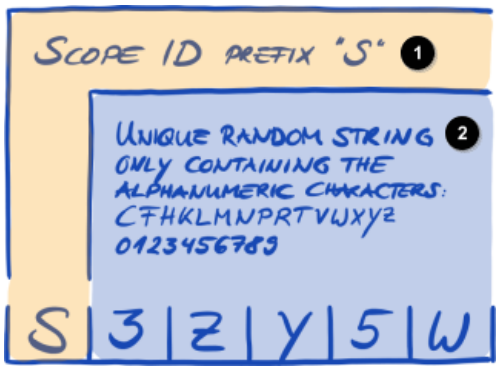


Figura 8. Formato dell'ID Ambito

1. Prefisso "S" dell'ID Ambito
2. Stringa casuale e univoca contenente solo le seguenti lettere e i seguenti numeri:
   CFHKLMNPRTVWXYZ
   0123456789

Attenzione:

Esistono due modi per trovare il proprio ID Ambito:

1. Verificate all'interno del vostro "TISAX Scope Excerpt" ("Estratto dell'ambito TISAX").
   Si veda Sezione 4.5.8, "E-mail di conferma" di cui sopra.
2. Accedete al portale ENXl, andate alla barra di navigazione principale, selezionate "MY TISAX" (IL MIO TISAX), quindi "SCOPES AND ASSESSMENTS" (AMBITI E VALUTAZIONI). Qui troverete il/i vostro/i ID Ambito.

Attenzione:

Ogni ambito di valutazione (identificato dal relativo ID Ambito) ha il proprio ciclo di vita.

Per maggiori informazioni sullo stato di una valutazione, si veda Sezione 7.5, "Allegato: Assessment scope status (Stato dell'ambito di valutazione)".

4.5.9. Informazioni sullo stato

In questa fase sono due gli stati rilevanti che usiamo per descrivere l’avanzamento della vostra azienda nel processo TISAX:

1. Stato del partecipante
2. Stato dell’ambito di valutazione

Il grafico riportato di seguito illustra le condizioni che devono essere soddisfatte per raggiungere un determinato stato:

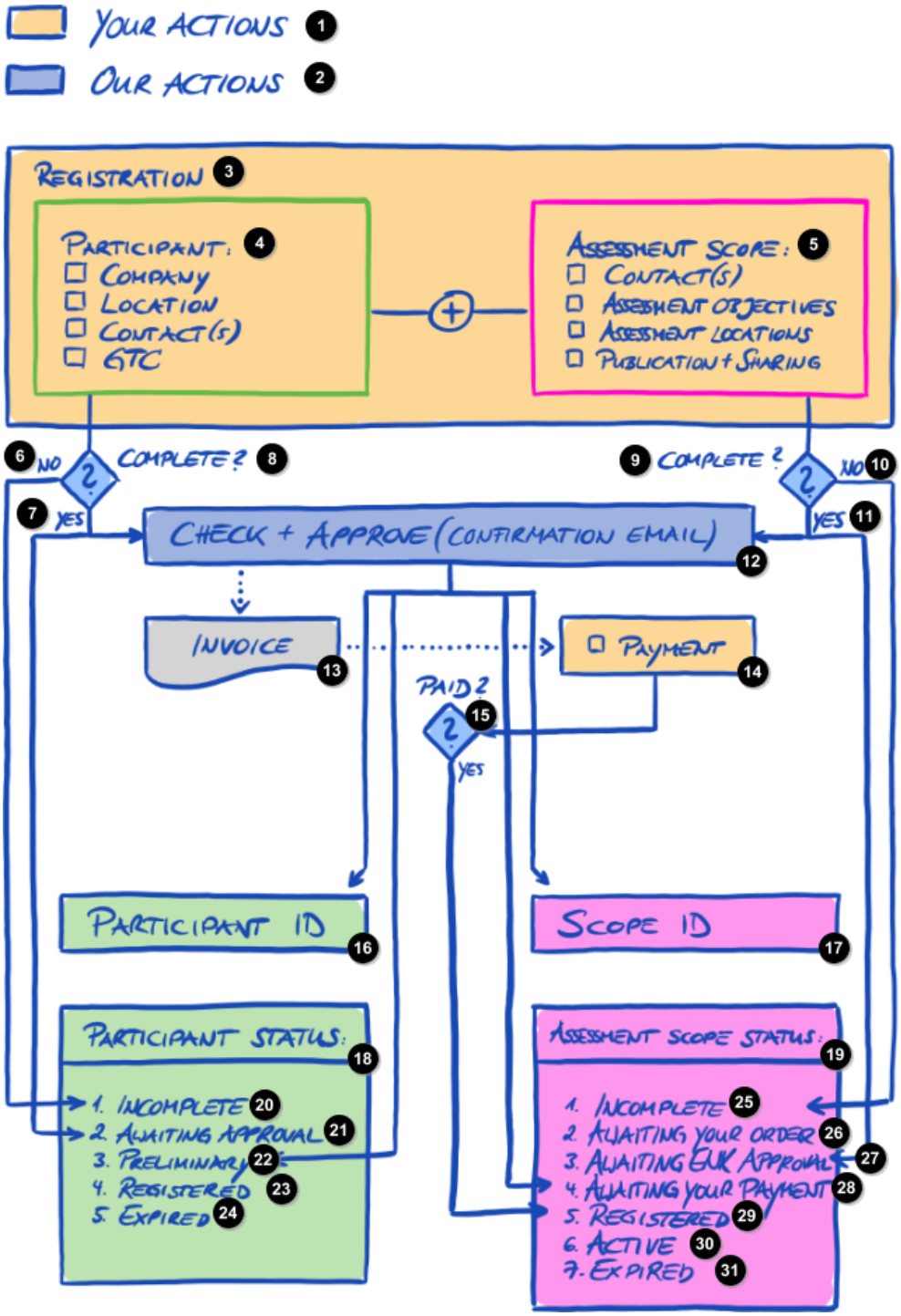


Figura 9. Condizioni per lo stato del partecipante e lo stato dell'ambito di valutazione

1. Le vostre azioni
2. Le nostre azioni
3. Registrazione

4. Partecipante:
[ ] Azienda
[ ] Sede
[ ] Contatto/i
[ ] CG

5. Ambito di valutazione:
[ ] Contatto/i
[ ] Obiettivi di valutazione
[ ] Sedi della valutazione
[ ] Pubblicazione + Condivisione

6. No

7. Sì

8. Completata?

9. Completata?

10. No

11. Sì

12. Verifica + Approvazione (e-mail di conferma)

13. Fattura

14. [ ] Pagamento

15. Pagamento effettuato?

16. ID Partecipante

17. ID Ambito

18. Stato del partecipante:

19. Stato dell’ambito di valutazione:

20. 1. Incompleto

21. 2. In attesa di approvazione

22. 3. Preliminare

23. Registrato

24. Scaduto

25. 1. Incompleto

26. 2. In attesa dell’ordine

27 3. In attesa dell'approvazione di ENX

28 4. In attesa del pagamento

29 5. Registrato

30 6. Attivo

31 7. Scaduto

Le definizioni degli stati e le azioni da compiere per passare allo stato successivo sono disponibili nell'allegato.

Per maggiori informazioni sullo:

- stato del partecipante, si veda Sezione 7.4, "Allegato: Participant status (Stato del partecipante)".
- stato dell'ambito di valutazione, si veda Sezione 7.5, "Allegato: Assessment scope status (Stato dell'ambito di valutazione)".

4.5.10. Modifiche alle informazioni di registrazione

Attenzione:

Per qualsiasi domanda sul ciclo di vita dei dati, si veda Sezione 7.9, "Allegato: Gestione del ciclo di vita dei dati del partecipante". Questa sezione contiene le istruzioni su come modificare o aggiornare i vostri dati, come la denominazione o le informazioni di contatto della vostra azienda.

Congratulazioni, la vostra azienda è ora registrata come partecipante TISAX. Siete pronti a passare alla fase successiva del processo TISAX.

5. Valutazione (fase 2)

Il tempo di lettura stimato per la sezione relativa alla valutazione è di 30-35 minuti.

5.1. Panoramica

La valutazione TISAX rappresenta la seconda fase del processo. È in questa fase che si svolge la maggior parte del lavoro per ottenere una valutazione TISAX.

Le sezioni che seguono vi guideranno durante la valutazione:

1. Inizieremo spiegando come potete utilizzare l'autovalutazione ISA per scoprire se siete pronti per una valutazione TISAX.
2. Successivamente troverete consigli su come scegliere uno dei nostri fornitori di audit TISAX.
3. Quindi descriveremo il processo di valutazione.
4. Infine, vi spiegheremo l'"esito del processo": il risultato della valutazione e le relative etichette TISAX.

5.2. Autovalutazione basata sull'ISA

Per essere pronti ad affrontare una valutazione TISAX, dovete innanzitutto disporre di un sistema di gestione della sicurezza delle informazioni (ISMS) pienamente efficiente. Per scoprire se il vostro ISMS corrisponde al livello di maturità previsto, dovete condurre un'autovalutazione basata sull'ISA.

L'"Information Security Assessment" (ISA) è un catalogo di criteri pubblicato dall'"Associazione tedesca dell'industria automobilistica" (Verband der Automobilindustrie e.V. - VDA). Esso rappresenta lo standard del settore automobilistico per le valutazioni della sicurezza delle informazioni.

Le sezioni seguenti si concentrano sulle istruzioni pratiche per condurre un'autovalutazione basata sull'ISA.

Le spiegazioni, gli esempi e gli screenshot contenuti in questo manuale si basano sulla versione 5 dell'ISA.

Attenzione:

Le informazioni sulle modifiche rispetto alle versioni precedenti dell'ISA sono disponibili nel relativo foglio Excel "Change history" ("Cronologia delle modifiche").

Attenzione:

> Per informazioni su quale versione ISA sia applicabile al risultato della vostra valutazione quando la VDA pubblica nuove versioni, si veda Sezione 7.11, “Allegato: Gestione del ciclo di vita dell’ISA”.

5.2.1. Download del documento ISA

Cominciate la vostra autovalutazione scaricando il documento ISA.

Potete scaricarlo dal nostro sito web al seguente indirizzo:
enx.com/en-US/TISAX/downloads/

Download diretto del file Excel:
portal.enx.com/isa5-en.xlsx

Il documento ISA è disponibile anche in tedesco:
enx.com/de-de/TISAX/downloads/

5.2.2. Come interpretare il documento ISA

Prima di iniziare l’autovalutazione, di seguito trovate alcune spiegazioni che potrebbero esservi utili. Queste vengono fornite in aggiunta alle spiegazioni e alle definizioni ufficiali contenute nel documento ISA, ponendo un’attenzione particolare all’uso ai fini delle valutazioni TISAX.

5.2.2.1. Cataloghi di criteri

L’ISA dispone al momento di tre “cataloghi di criteri”[13]:

1.	Sicurezza delle informazioni	Information Security
2.	Protezione dei prototipi	Prototype Protection
3.	Protezione dei dati	Data Protection

Ciascun catalogo di criteri ha il proprio foglio Excel:

Figura 10. Screenshot: Cataloghi di criteri ISA sotto forma di fogli Excel

Quale catalogo di criteri è rilevante per la vostra azienda? La risposta dipende dal/i vostro/i obiettivo/i di valutazione.

Ciascun obiettivo di valutazione definisce quali requisiti di quale catalogo di criteri si applicano. Per alcuni obiettivi di valutazione si applicano solo i requisiti di *un* catalogo di criteri, mentre per altri si applicano i requisiti di *più* cataloghi di criteri.

Gli obiettivi di valutazione menzionati sopra corrispondono ai seguenti cataloghi di criteri:

N.	Obiettivo di valutazione (Assessment objective)	Catalogo/cataloghi di criteri ISA
1.	Info high	Information Security (Sicurezza delle informazioni)
2.	Info very high	Information Security (Sicurezza delle informazioni)
3.	Confidential	Information Security (Sicurezza delle informazioni)
4.	Strictly confidential	Information Security (Sicurezza delle informazioni)
5.	High availability	Information Security (Sicurezza delle informazioni)
6.	Very high availability	Information Security (Sicurezza delle informazioni)
7.	Proto parts	Prototype Protection (Protezione dei prototipi)
8.	Proto vehicles	Prototype Protection (Protezione dei prototipi)
9.	Test vehicles	Prototype Protection (Protezione dei prototipi)
10.	Proto events	Prototype Protection (Protezione dei prototipi)
11.	Data	Information Security (Sicurezza delle informazioni) Data Protection (Protezione dei dati)
12.	Special data	Information Security (Sicurezza delle informazioni) Data Protection (Protezione dei dati)

Tabella 7. Corrispondenza tra gli obiettivi di valutazione TISAX e i cataloghi di criteri ISA

Esempio: se avete selezionato l'obiettivo di valutazione "Protezione dei dati", dovrete rispondere alle domande dei cataloghi di criteri "Sicurezza delle informazioni" E "Protezione dei dati".

Avrete notato che c'è più di un obiettivo di valutazione per ogni catalogo di criteri. Come fare quindi a capire quali requisiti sono applicabili a quale obiettivo di valutazione?

La tabella seguente mostra quali sono i requisiti applicabili:

N.	Obiettivo di valutazione (Assessment objective)	Requisiti applicabili
1.	Info high	▪ Catalogo di criteri “Information Security” (“Sicurezza delle informazioni”) ◦ Colonna “Requirements (must)” (“Requisiti (obbligatori)”) ◦ Colonna “Requirements (should)” (“Requisiti (consigliati)”) ◦ Colonna “Additional requirements for high protection needs” (“Requisiti aggiuntivi per esigenze di protezione elevate”)
2.	Info very high	▪ Catalogo di criteri “Information Security” (“Sicurezza delle informazioni”) ◦ Colonna “Requirements (must)” (“Requisiti (obbligatori)”) ◦ Colonna “Requirements (should)” (“Requisiti (consigliati)”) ◦ Colonna “Additional requirements for high protection needs” (“Requisiti aggiuntivi per esigenze di protezione elevate”) ◦ Colonna ()“Requisiti aggiuntivi per esigenze di protezione molto elevate”
3.	Confidential	▪ Catalogo di criteri “Information Security” (“Sicurezza delle informazioni”) ◦ Colonna “Requirements (must)” (“Requisiti (obbligatori)”) ◦ Colonna “Requirements (should)” (“Requisiti (consigliati)”) ◦ Colonna “Additional requirements for high protection needs” (“Requisiti aggiuntivi per esigenze di protezione elevate”) (solo quelli contrassegnati con una “**C**” di **C**onfidentiality (**R**iservatezza))

N.	Obiettivo di valutazione (Assessment objective)	Requisiti applicabili
4.	Strictly confidential	▪ Catalogo di criteri “Information Security” (“Sicurezza delle informazioni”) ◦ Colonna “Requirements (must)” (“Requisiti (obbligatori)”) ◦ Colonna “Requirements (should)” (“Requisiti (consigliati)”) ◦ Colonna “Additional requirements for high protection needs” (“Requisiti aggiuntivi per esigenze di protezione elevate”) (solo quelli contrassegnati con una “**C**” di **C**onfidentiality (**R**iservatezza)) ◦ Colonna ( )“Requisiti aggiuntivi per esigenze di protezione molto elevate” (solo quelli contrassegnati con una “**C**” di **C**onfidentiality (**R**iservatezza))
5.	High availability	▪ Catalogo di criteri “Information Security” (“Sicurezza delle informazioni”) ◦ Colonna “Requirements (must)” (“Requisiti (obbligatori)”) ◦ Colonna “Requirements (should)” (“Requisiti (consigliati)”) ◦ Colonna “Additional requirements for high protection needs” (“Requisiti aggiuntivi per esigenze di protezione elevate”) (solo quelli contrassegnati con una “**A**” di **A**vailability (**D**isponibilità))

N.	Obiettivo di valutazione (Assessment objective)	Requisiti applicabili
6.	Very high availability	▪ Catalogo di criteri “Information Security” (“Sicurezza delle informazioni”) ◦ Colonna “Requirements (must)” (“Requisiti (obbligatori)”) ◦ Colonna “Requirements (should)” (“Requisiti (consigliati)”) ◦ Colonna “Additional requirements for high protection needs” (“Requisiti aggiuntivi per esigenze di protezione elevate”) (solo quelli contrassegnati con una “**A**” di **A**vailability (**D**isponibilità)) ◦ Colonna ( )“Requisiti aggiuntivi per esigenze di protezione molto elevate” (solo quelli contrassegnati con una “**A**” di **A**vailability (**D**isponibilità))
7.	Proto parts	▪ Catalogo di criteri “Prototype Protection” (“Protezione dei prototipi”) Solo i seguenti capitoli: 8.1 Physical and Environmental Security (8.1 Sicurezza fisica e ambientale) 8.2 Organizational Requirements (8.2 Requisiti organizzativi) 8.3 Handling of vehicles, components and parts (8.3 Gestione di veicoli, componenti e parti) ◦ Colonna “Requirements (must)” (“Requisiti (obbligatori)”) ◦ Colonna “Requirements (should)” (“Requisiti (consigliati)”)

N.	Obiettivo di valutazione (Assessment objective)	Requisiti applicabili
8.	Proto vehicles	▪ Catalogo di criteri “Prototype Protection” (“Protezione dei prototipi”) Solo i seguenti capitoli: 8.1 Physical and Environmental Security (8.1 Sicurezza fisica e ambientale) 8.2 Organizational Requirements (8.2 Requisiti organizzativi) 8.3 Handling of vehicles, components and parts (8.3 Gestione di veicoli, componenti e parti) ◦ Colonna “Requirements (must)” (“Requisiti (obbligatori)”) ◦ Colonna “Requirements (should)” (“Requisiti (consigliati)”) ◦ Colonna “Additional requirements for vehicles classified as requiring protection” (“Requisiti aggiuntivi per i veicoli classificati come soggetti a protezione”)
9.	Test vehicles	▪ Catalogo di criteri “Prototype Protection” (“Protezione dei prototipi”) Solo i seguenti capitoli: 8.2 Organizational Requirements (8.2 Requisiti organizzativi) 8.3 Handling of vehicles, components and parts (8.3 Gestione di veicoli, componenti e parti) 8.4 Requirements for trial vehicles (8,4 Requisiti per veicoli di prova) ◦ Colonna “Requirements (must)” (“Requisiti (obbligatori)”) ◦ Colonna “Requirements (should)” (“Requisiti (consigliati)”)

N.	Obiettivo di valutazione (🇬🇧 Assessment objective)	Requisiti applicabili
10.	Proto events	▪ Catalogo di criteri “Prototype Protection” (🇮🇹 “Protezione dei prototipi”) Solo i seguenti capitoli: 8.2 Organizational Requirements (🇮🇹 8.2 Requisiti organizzativi) 8.3 Handling of vehicles, components and parts (🇮🇹 8.3 Gestione di veicoli, componenti e parti) 8.5 Requirements for events and shootings (🇮🇹 8.5 Requisiti per eventi e riprese) ◦ Colonna “Requirements (must)” (🇮🇹 “Requisiti (obbligatori)”) ◦ Colonna “Requirements (should)” (🇮🇹 “Requisiti (consigliati)”)
11.	Data	▪ Catalogo di criteri “Information Security” (🇮🇹 “Sicurezza delle informazioni”) ◦ Colonna “Requirements (must)” (🇮🇹 “Requisiti (obbligatori)”) ◦ Colonna “Requirements (should)” (🇮🇹 “Requisiti (consigliati)”) ◦ Colonna “Additional requirements for high protection needs” (🇮🇹 “Requisiti aggiuntivi per esigenze di protezione elevate”) (solo quelli contrassegnati con una “**C**” di **C**onfidentiality (🇮🇹 **R**iservatezza)) ▪ Catalogo di criteri “Data Protection” (🇮🇹 “Protezione dei dati”) ◦ Colonna “Requirements (must)” (🇮🇹 “Requisiti (obbligatori)”)

N.	Obiettivo di valutazione (Assessment objective)	Requisiti applicabili
12.	Special data	▪ Catalogo di criteri “Information Security” (“Sicurezza delle informazioni”) ◦ Colonna “Requirements (must)” (“Requisiti (obbligatori)”) ◦ Colonna “Requirements (should)” (“Requisiti (consigliati)”) ◦ Colonna “Additional requirements for high protection needs” (“Requisiti aggiuntivi per esigenze di protezione elevate”) (solo quelli contrassegnati con una “**C**” di **C**onfidentiality (**R**iservatezza)) ◦ Colonna ( )“Requisiti aggiuntivi per esigenze di protezione molto elevate” (solo quelli contrassegnati con una “**C**” di **C**onfidentiality (**R**iservatezza)) ▪ Catalogo di criteri “Data Protection” (“Protezione dei dati”) ◦ Colonna “Requirements (must)” (“Requisiti (obbligatori)”)

Tabella 8. Applicabilità dei requisiti agli obiettivi di valutazione

Attenzione:

Ciascun requisito nelle due colonne “Requisiti aggiuntivi per esigenze di protezione elevate” e “Requisiti aggiuntivi per esigenze di protezione molto elevate” è contrassegnato da una “**C**” di **C**onfidentiality (**R**iservatezza), da una “**I**” di **I**ntegrity (**I**ntegrità) o da una “**A**” di **A**vailability (**D**isponibilità) oppure da una qualsiasi combinazione di queste tre lettere.

Quando la tabella di cui sopra restringe i requisiti in queste due colonne a quelli contrassegnati da *una* delle lettere sopra citate, sono sempre inclusi i requisiti che sono contrassegnati anche da *altre* lettere oltre a questa.

Esempio: tutti i requisiti contrassegnati con “(C)”, “(C, I, A)” o “(C, I)” sono applicabili nei casi in cui la lettera “C” è specificata nella tabella di cui sopra (ad se. nell’obiettivo di valutazione “Special data”).

Lo screenshot seguente mostra gli elementi principali delle domande di controllo nel catalogo di criteri “Sicurezza delle informazioni” (gli altri cataloghi di criteri presentano solo un

sottoinsieme di questi elementi). Tutti gli elementi sono spiegati più avanti.

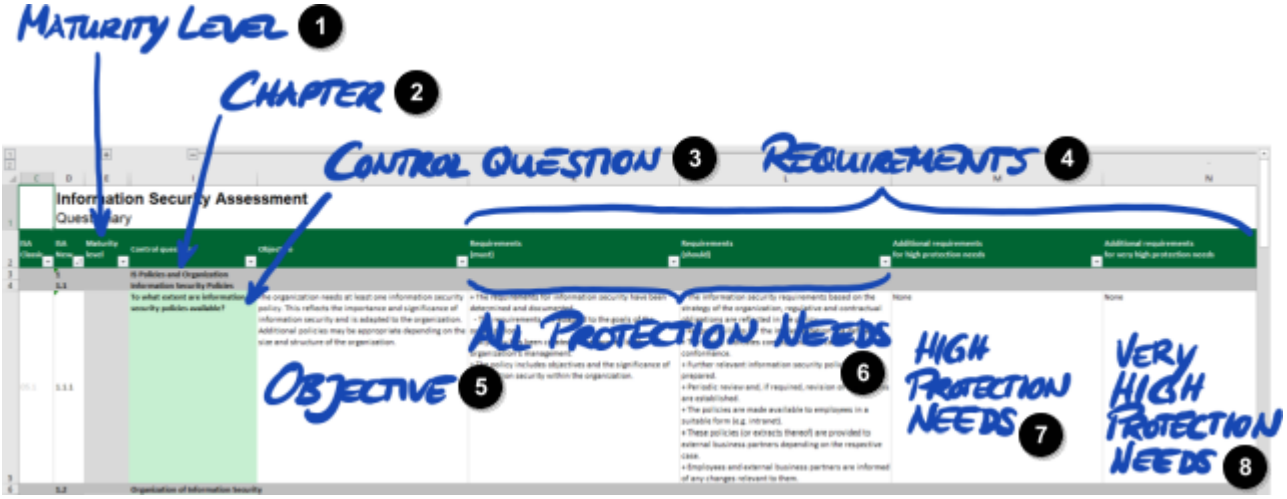


Figura 11. Screenshot: Elementi principali delle domande del catalogo di criteri ISA "Sicurezza delle informazioni"

1. Livello di maturità
2. Capitolo
3. Domanda di controllo
4. Requisiti
5. Obiettivo
6. Tutte le esigenze di protezione
7. Esigenze di protezione elevate
8. Esigenze di protezione molto elevate

5.2.2.2. Capitoli

Ciascun catalogo di criteri raggruppa le domande in capitoli.

Esempio: "2 Risorse umane"

Il raggruppamento si basa sulle responsabilità tipiche all'interno di un'azienda. Questi reparti sono specificati nella colonna "Usual person responsible for process implementation" ("Responsabile abituale dell'implementazione del processo") ("HR", "Risorse umane" nell'esempio di cui sopra).

5.2.2.3. Domande di controllo

Le domande per ogni catalogo di criteri sono disponibili nei rispettivi fogli Excel.

Esempio: "4.1.2 Qual è il grado di protezione dell'accesso degli utenti ai servizi di rete, ai sistemi

IT e alle applicazioni IT?”.

Le domande di controllo vengono anche chiamate “controlli” nel “linguaggio degli auditor”. Gli standard ISO su cui si basa l’ISA utilizzano il termine “controllo”.

5.2.2.4. Campi del modulo di autovalutazione

Tra le colonne “Maturity level” (“Livello di maturità”) e “Control question” (“Domanda di controllo”) si trovano i campi del modulo da compilare quando si conduce un’autovalutazione:

Campo del modulo	Scopo	Obbligatorio?
Implementation description (Descrizione dell’implementazione) (Colonna F)	Qui dovete descrivere brevemente cosa avete implementato per gestire questa domanda di controllo all’interno della vostra azienda.	Sì
Reference Documentation (Documentazione di riferimento) (Colonna G)	Qui dovete specificare in quale/i documento/i viene dimostrata l’implementazione.	Sì
Findings/Result (Rilievi/Risultato) (Colonna H)	Qui potete annotare tutti i rilievi per i quali ritenete che ci sia un divario tra la situazione ideale e quella effettiva.	No

Tabella 9. Campi del modulo di autovalutazione e relativo scopo

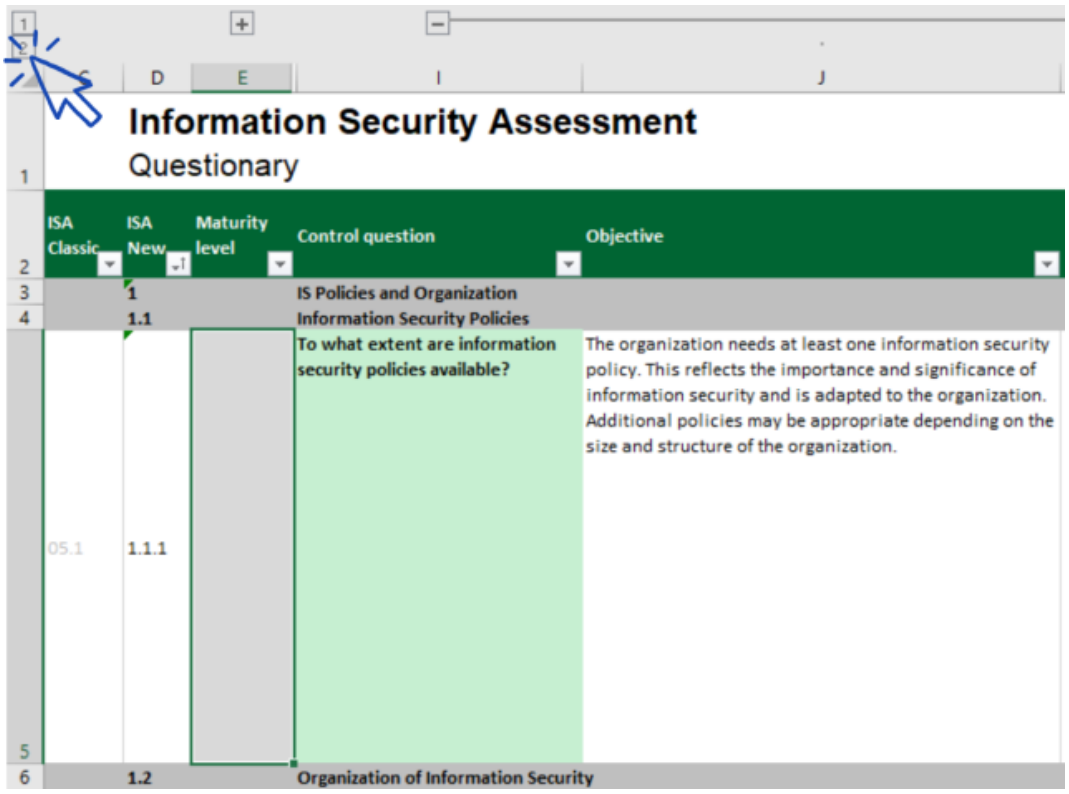
È obbligatorio inserire solo una breve descrizione dell’implementazione e il riferimento alla vostra documentazione. Queste informazioni aiuteranno i nostri fornitori di audit TISAX a comprendere meglio la vostra azienda e a preparare la valutazione.

Sono disponibili altre colonne opzionali a supporto della vostra autovalutazione:

- Measures/recommendations (Misure/consigli) (Colonna R)
- Date of assessment (Data della valutazione) (Colonna S)
- Date of completion (Data di completamento) (Colonna T)
- Responsible department (Reparto responsabile) (Colonna U)
- Contact (Contatto) (Colonna V)

Nota importante:

Se aprite il file Excel scaricato e selezionate uno dei fogli di lavoro del catalogo di criteri (ad esempio, Sicurezza delle informazioni), probabilmente non vedrete immediatamente i campi del modulo di autovalutazione. Per visualizzarli, è necessario fare clic sul pulsante di raggruppamento per il livello "2"[14]. Il pulsante si trova sopra e a sinistra della cella C1. In questo modo si espande la visualizzazione e vengono mostrati i campi del modulo di autovalutazione.



Un altro consiglio è quello di utilizzare i tasti freccia per scorrere verso il basso. A causa delle grandi dimensioni delle celle, lo scorrimento con la barra di scorrimento può richiedere eccellenti doti di motricità fine. Se si utilizza la funzione di scorrimento del dispositivo di puntamento, si rischia anche di saltare accidentalmente alcune delle celle più grandi.

5.2.2.5. Obiettivo

A destra della colonna "Domanda di controllo" si trova la colonna "Obiettivo" (colonna J). Il suo contenuto descrive gli obiettivi da raggiungere relativamente a questo aspetto della gestione della sicurezza delle informazioni.

Esempio (per la domanda di controllo 4.1.2): "Solo gli utenti identificati in modo sicuro (autenticati) devono accedere ai sistemi informatici. A tal fine, l'identità di un utente viene stabilita in modo sicuro mediante procedure adeguate".

5.2.2.6. Requisiti

I requisiti sono ciò che ci si aspetta che la vostra azienda soddisfi per raggiungere l'obiettivo in questione.

I requisiti sono suddivisi in quattro colonne:

1. Requirements (must) (Requisiti (obbligatori)) (Colonna K)
2. Requirements (should) (Requisiti (consigliati)) (Colonna L)
3. Additional requirements for high protection needs (Requisiti aggiuntivi per esigenze di protezione elevate) (Colonna M)
4. Additional requirements for very high protection needs (Requisiti aggiuntivi per esigenze di protezione molto elevate) (Colonna N)

È necessario soddisfare tutti i requisiti fino all'esigenza di protezione che dovete raggiungere (che potete ricavare dall'obiettivo di valutazione).

Per alcuni obiettivi di valutazione è applicabile solo un sottoinsieme dei requisiti. Per maggiori informazioni sull'applicabilità dei requisiti si veda Tabella 8, "Applicabilità dei requisiti agli obiettivi di valutazione" in Sezione 5.2.2.1, "Cataloghi di criteri" e in particolare note alla fine della sezione.

Per maggiori informazioni sulle definizioni dell'ISA dei livelli dei requisiti "obbligatori" e "consigliati", si vedano i "Termini chiave" nel foglio Excel "Definizioni".

Nota importante:

È molto importante capire che ciascun requisito deve essere interpretato in base al contesto e allo spirito dell'obiettivo. Anche se un requisito è stato rispettato alla lettera, non è detto che il fornitore di audit confermi che la vostra azienda soddisfa tale requisito nel contesto e nello spirito dell'obiettivo (colonna J).

I requisiti e la loro formulazione si basano sull'implementazione teorica da parte di un'azienda media fittizia di dimensioni sconosciute.

Il fornitore di audit deve sempre considerare l'obiettivo rispetto all'implementazione unica presso la vostra azienda. Ciò che è appropriato per un'azienda media potrebbe non essere sufficiente nella vostra situazione specifica.

Per maggiori informazioni, si veda Sezione 5.2.5, "Gestione del risultato dell'autovalutazione".

5.2.2.7. Livelli di maturità

L'ISA utilizza il concetto dei "maturity levels" ("livelli di maturità") per valutare la qualità di tutti gli aspetti del sistema di gestione della sicurezza delle informazioni della vostra azienda. Quanto più sofisticato è il sistema di gestione della sicurezza delle informazioni della vostra azienda, tanto più alto sarà il vostro livello di maturità.

L'ISA distingue sei livelli di maturità. La definizione dettagliata è disponibile nel foglio Excel "Maturity levels" ("Livelli di maturità"). Per offrirvi una panoramica completa dei livelli di maturità, riportiamo le descrizioni informali presenti nell'ISA:

Maturity level (Livello di maturità)	**In una sola parola**	**Descrizione**
0	Incomplete (Incompleto)	Un processo non è disponibile, non viene seguito o non è adatto per raggiungere l'obiettivo in questione.
1	Performed (Eseguito)	Viene seguito un processo non documentato o non completamente documentato e vi sono indicatori che mostrano il raggiungimento del suo obiettivo.
2	Managed (Gestito)	Viene seguito un processo che raggiunge il suo obiettivo. Sono disponibili prove della documentazione e dell'implementazione del processo.
3	Established (Consolidato)	Viene seguito un processo standard integrato nel sistema generale. Le dipendenze da altri processi sono documentate e le appropriate interfacce sono create. Vi sono prove che il processo è stato usato in maniera sostenibile e attiva per un periodo prolungato.
4	Predictable (Prevedibile)	Viene seguito un processo consolidato. L'efficacia del processo è costantemente monitorata attraverso la raccolta di dati chiave. Vengono stabiliti dei valori limite in corrispondenza dei quali il processo viene considerato insufficientemente efficace e necessita di un adeguamento (indicatori chiave di prestazione).
5	Optimizing (Ottimizzato)	Viene seguito un processo prevedibile che ha come obiettivo principale il miglioramento continuo. Il miglioramento viene portato avanti attivamente da risorse dedicate.

Tabella 10. Descrizione informale dei livelli di maturità

Dovete valutare il livello di maturità del sistema di gestione della sicurezza delle informazioni della vostra azienda per ogni domanda. Inserite il vostro livello di maturità nella colonna "Maturity level" ("Livello di maturità") (colonna E).

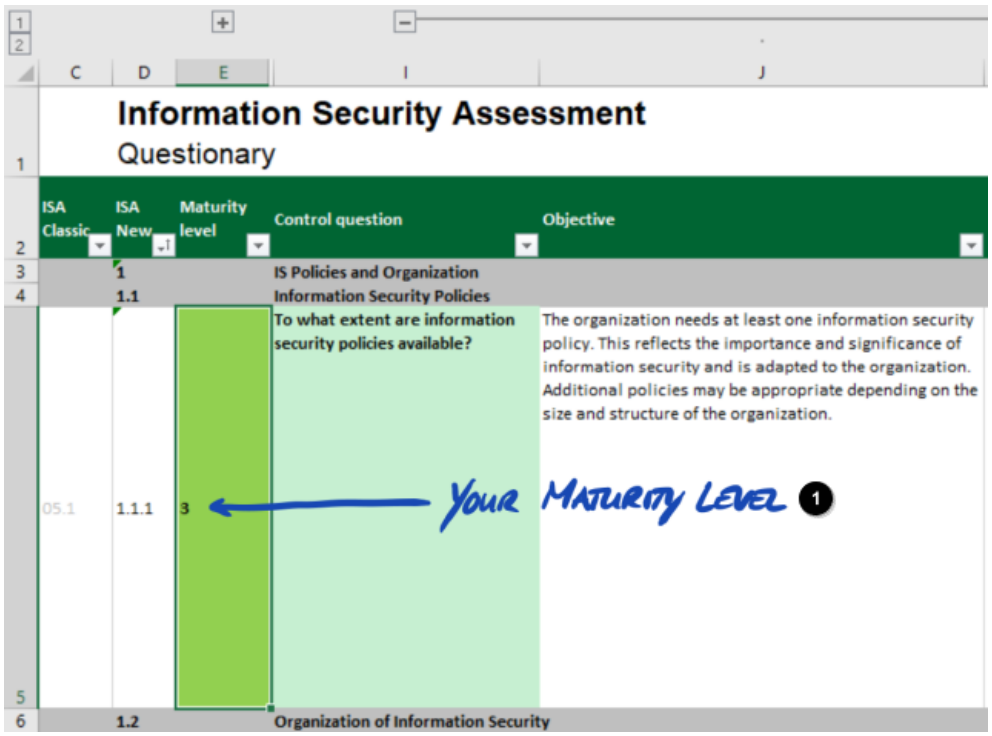


Figura 12. Screenshot: Esempio di selezione del livello di maturità nel documento ISA (foglio Excel "Sicurezza delle informazioni")

1 Livello di maturità della vostra azienda

Per maggiori informazioni sui livelli di maturità target e il loro impatto sul risultato della valutazione, si veda Sezione 5.2.4, "Interpretazione del risultato dell'autovalutazione".

Ora che avete acquisito queste nuove conoscenze, siete pronti per iniziare l'autovalutazione.

5.2.3. Esecuzione dell'autovalutazione

Aprite il file Excel, leggete tutte le domande di controllo di ciascun catalogo di criteri applicabile al vostro o ai vostri obiettivi di valutazione e stabilite il livello di maturità che corrisponde allo stato attuale del sistema di gestione della sicurezza delle informazioni della vostra azienda. Eseguite questa operazione al meglio delle vostre possibilità. Non ci sono scelte giuste o sbagliate in questa fase.

Una volta completata l'autovalutazione, la colonna "Risultato" (H) del foglio Excel "Risultati (ISA5)" deve essere completamente compilata, con numeri (0-5) o con "N/A" ("non applicabile").

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3
1.2.3	To what extent are information security requirements taken into account in projects?	3	3
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	3
1.3.1	To what extent are information assets identified and recorded?	3	3
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	3
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	3
1.4.1	To what extent are information security risks managed?	3	3
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	3
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	3
1.6.1	To what extent are information security events processed?	3	3

❶ GREEN = ✓

Figura 13. Screenshot: Esempio del foglio "Risultati (ISA5)" nel documento ISA

❶ Verde

In caso di domande sull'ISA, contattateci.

5.2.4. Interpretazione del risultato dell'autovalutazione

Le cinque sotto-sezioni riportate di seguito spiegano come analizzare e interpretare il risultato dell'autovalutazione. Questa analisi vi aiuterà a capire se la vostra azienda è pronta o meno per una valutazione TISAX.

5.2.4.1. Analisi

Il punteggio ottenuto riassume il risultato dell'autovalutazione.

Il punteggio ("Risultato con abbassamento al livello di maturità target") è disponibile nel foglio Excel "Risultati (ISA5)" (cella D6). Il concetto di "abbassamento" verrà spiegato a breve.

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

Details: YOUR RESULT SCORE 1 MAXIMUM RESULT SCORE 2

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figura 14. Screenshot: Il punteggio della vostra azienda e il punteggio massimo (foglio Excel "Risultati (ISA5)", celle D6 e G6)

1. Punteggio della vostra azienda
2. Punteggio massimo

Per comprendere e successivamente interpretare il risultato dell'autovalutazione e il punteggio ottenuto, è necessario distinguere tra due livelli di analisi:

1. Livello della domanda
   Questo livello include tutte le domande. Per ciascuna domanda è previsto un livello di maturità target e il livello di maturità della vostra azienda.
2. Livello del punteggio
   Questo livello include il risultato complessivo che riassume i risultati di tutte le domande. Viene indicato il punteggio massimo e il punteggio della vostra azienda.

La figura riportata di seguito mostra i livelli di analisi:

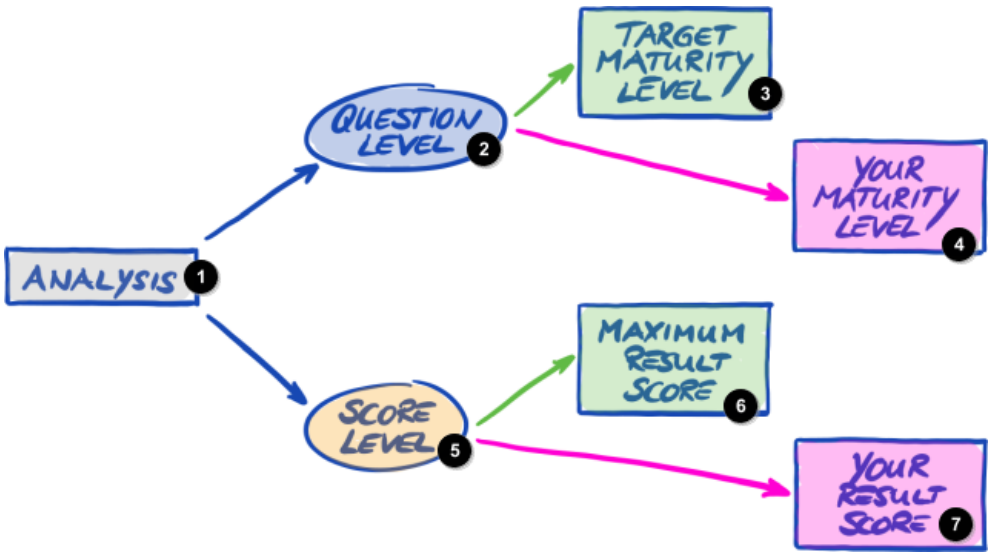


Figura 15. Analisi del risultato dell'autovalutazione a livello di domanda e a livello di punteggio

1. Analisi
2. Livello della domanda
3. Livello di maturità target
4. Livello di maturità della vostra azienda
5. Livello del punteggio
6. Punteggio massimo
7. Punteggio della vostra azienda

La figura riportata di seguito mostra dove trovare i risultati a livello di punteggio e i risultati a livello di domanda:

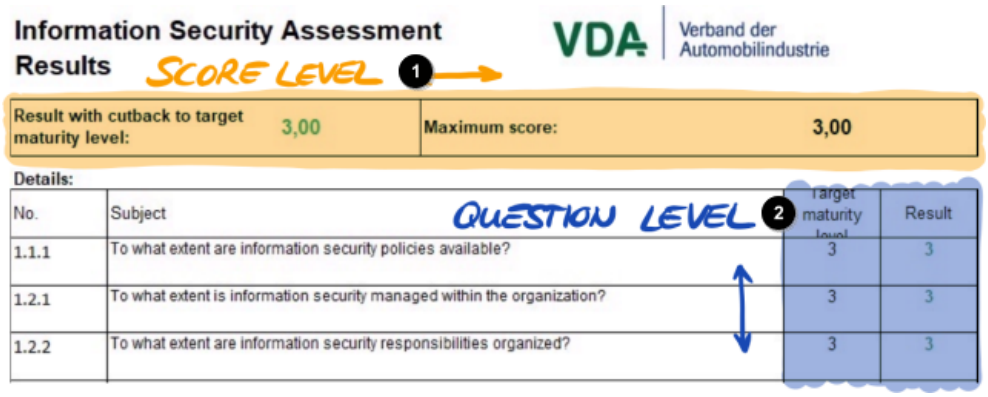


Figura 16. Livello del punteggio e livello della domanda nel foglio Excel "Risultati (ISA5)"

1. Livello del punteggio
2. Livello della domanda

La figura riportata di seguito mostra una panoramica semplificata dei livelli di analisi, le definizioni dei target ISA e i risultati della vostra azienda:

Figura 17. I target e i risultati della vostra azienda a livello di domanda e a livello di punteggio

1. Livello di maturità target
2. Livello di maturità della vostra azienda
3. Livello della domanda
4. Q (Domanda)
5. TML (livello di maturità target)
6. YML (livello di maturità della vostra azienda)
7. Punteggio massimo
8. Punteggio della vostra azienda
9. Livello del punteggio

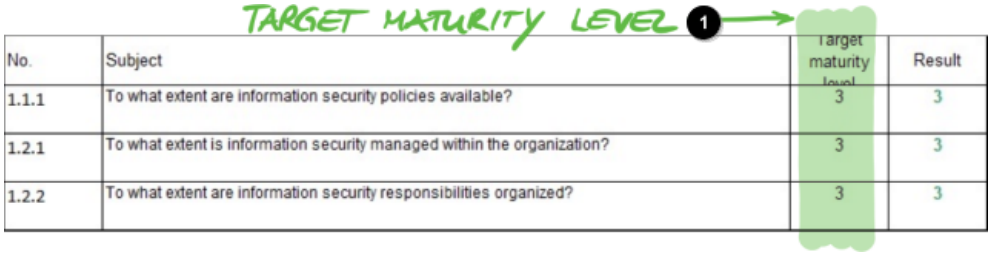
Le sezioni seguenti illustrano in dettaglio il risultato e la relativa analisi.

5.2.4.2. Il livello di maturità target (a livello di domanda)

L'ISA stabilisce un "livello di maturità target" pari a 3 per ogni domanda.

Per maggiori informazioni sulla definizione di ogni livello di maturità, si veda Sezione 5.2.2, "Come interpretare il documento ISA".

L'ISA stabilisce i livelli di maturità target nel foglio Excel "Risultati (ISA5)" (a partire dalla colonna G, riga 22; si veda la figura riportata di seguito).



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figura 18. La definizione del livello di maturità target nel foglio Excel "Risultati (ISA5)"

1. Livello di maturità target

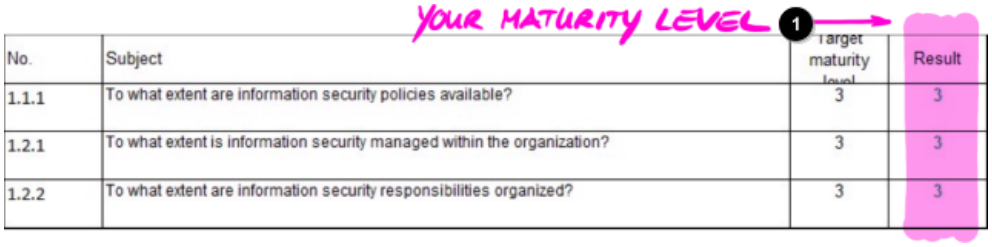
5.2.4.3. Il risultato della vostra azienda (a livello di domanda)

Per ricevere le etichette TISAX, di solito è necessario che i livelli di maturità per ogni domanda siano uguali o superiori al livello di maturità target.

Esempio: se il livello di maturità target per la domanda X è "3", il livello di maturità della vostra azienda per quella domanda deve essere pari o superiore a "3". Se il livello di maturità della vostra azienda per la domanda in questione è inferiore a "3", non potrete ricevere le etichette TISAX.

Ciò vale per tutte le domande. Se il livello di maturità target per due domande è pari a "3", non è possibile compensare un livello di maturità "2" per una domanda con un livello di maturità "4" per l'altra domanda.

Il documento ISA trasferisce automaticamente i livelli di maturità della vostra azienda dal foglio Excel "Sicurezza delle informazioni" (colonna E) al foglio Excel "Risultati (ISA5)" (a partire dalla colonna H, riga 23):



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figura 19. I livelli di maturità della vostra azienda nel foglio Excel "Risultati (ISA5)"

1. Livello di maturità target della vostra azienda

Il livello di maturità target della vostra azienda è soggetto a un calcolo prima che il documento ISA lo riassuma nel vostro punteggio. In pratica, il livello di maturità della vostra azienda viene “abbassato” al livello di maturità target. Ciò avviene per fare in modo che le domande per le quali il livello di maturità della vostra azienda è *superiore* al livello di maturità target non compensino le domande per le quali il livello di maturità della vostra azienda è *inferiore* al livello di maturità target.

Ecco in che modo l’ISA calcola il risultato della vostra azienda a livello di domanda:

- Viene preso in considerazione il livello di maturità della vostra azienda e confrontato con il livello di maturità target di una data domanda.
- Se il livello di maturità della vostra azienda è superiore al livello di maturità target, esso viene “abbassato” al livello di maturità target.
- Se il livello di maturità della vostra azienda è inferiore o pari al livello di maturità target, non viene eseguita nessuna operazione per la domanda in questione.

Esempio (si veda la figura riportata di seguito): il livello di maturità target è “3”. Il livello di maturità della vostra azienda è “4”. Il “risultato abbassato” della vostra azienda per questa domanda sarà “3”.

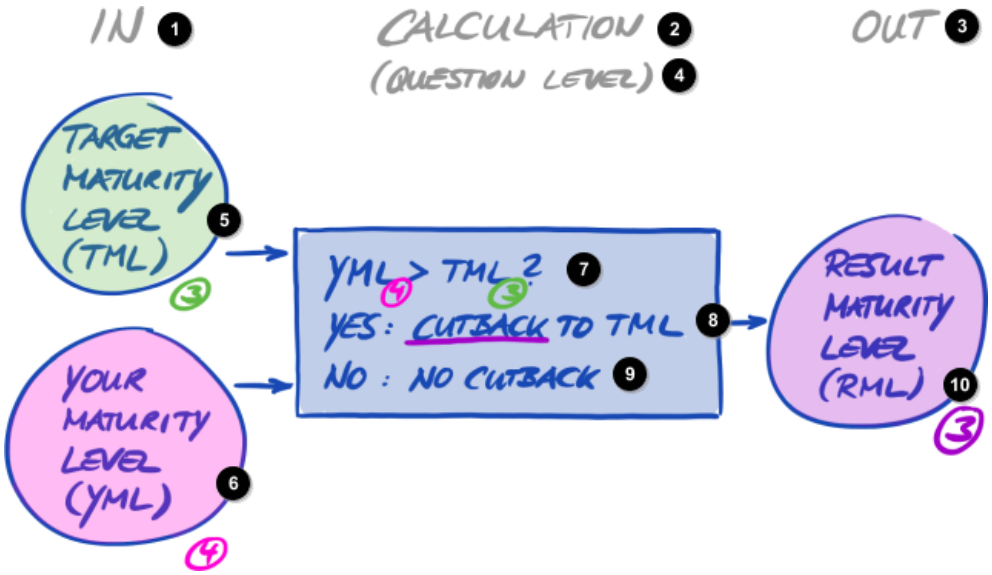


Figura 20. Calcolo per l’abbassamento del risultato del livello di maturità

1. A monte
2. Calcolo
3. A valle
4. (Livello della domanda)

5. Livello di maturità target (TML)
6. Livello di maturità della vostra azienda (YML)
7. YML > TML?
8. Sì: abbassamento al TML
9. No: nessun abbassamento
10. Risultato del livello di maturità (RML)

La figura qui di seguito mostra che il vostro livello di maturità è superiore rispetto al livello di maturità target, ISA lo abbassa (i colori verde, arancione e rosso combaciano con i colori usati nella colonna “Risultato”, si veda Figura 19, “I livelli di maturità della vostra azienda nel foglio Excel “Risultati (ISA5)””).

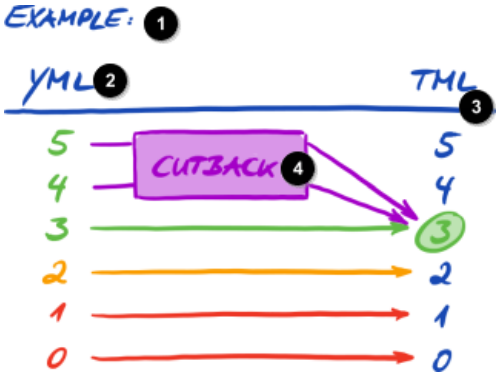


Figura 21. Rappresentazione dell’abbassamento con i colori usati nel foglio Excel “Risultati (ISA5)”

1. Esempio:
2. YML
3. TML
4. Abbassamento

Di seguito è riportato un altro modo per rappresentare i livelli di maturità a livello di domanda. I colori dei cerchi illustrano il livello di maturità target o la “distanza” da esso (esempio: il cerchio è arancione se il livello di maturità è a “-1” dal livello di maturità target). I segni di spunta rappresentano il livello di maturità della vostra azienda.

Figura 22. Livelli di maturità a livello di domanda

1. Livello di maturità
2. Domanda
3. Abbassamento
4. Livello di maturità target (TML)
5. Uno o più punti in più rispetto al TML
6. Un punto in meno rispetto al TML
7. Due o più punti in meno rispetto al TML
8. Livello di maturità della vostra azienda (YML)
9. Abbassamento al TML

Attenzione:

È possibile superare con successo una valutazione TISAX anche se non si raggiunge il livello di maturità target per tutte le domande. L'aspetto principale da considerare in questi casi è se si è in presenza o meno di un rischio rilevante. Se il livello di maturità della vostra azienda è inferiore al valore target, ma non vi è alcun rischio, tale livello potrebbe essere sufficiente.

5.2.4.4. Il valore target (a livello di punteggio)

L'ISA stabilisce un livello di maturità complessivo "ideale", ossia il "punteggio del risultato massimo" (o "Punteggio massimo", cella G6).

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

MAXIMUM RESULT SCORE

Details:

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

1

Figura 23. Punteggio massimo (foglio Excel “Risultati (ISA5)”)

1 Punteggio massimo

In teoria, questo livello di maturità complessivo rappresenta la media di tutti i livelli di maturità target (a livello di domanda) e dovrebbe corrispondere a un punteggio massimo di “3,0”.

Tuttavia, tale livello è pari a “3,0” solo se tutte le domande sono applicabili alla situazione della vostra azienda. Non appena una domanda non è applicabile alla situazione della vostra azienda, la media cambia e il punteggio massimo diventa inferiore a “3,0”.

Sulla base di una rappresentazione riportata sopra (Figura 22, “Livelli di maturità a livello di domanda”), è possibile vedere nella figura di seguito cosa viene calcolato nella media per il punteggio massimo:

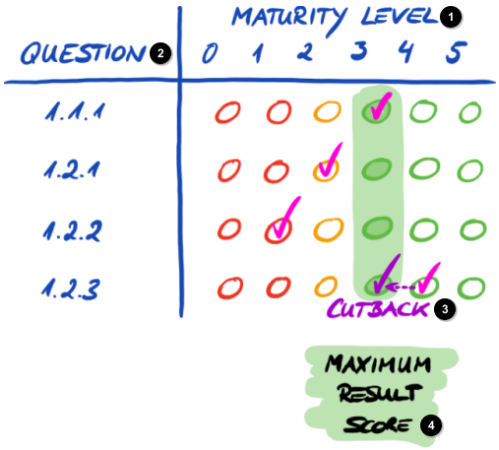


Figura 24. Il punteggio massimo (a livello di punteggio)

1 Livello di maturità

2 Domanda

3 Abbassamento

4 Punteggio massimo

5.2.4.5. Il risultato della vostra azienda (a livello di punteggio)

Il punteggio complessivo della vostra azienda (“Risultato con abbassamento ai livelli di maturità target”, cella D6):

- riassume il livello di maturità complessivo del sistema di gestione della sicurezza delle informazioni della vostra azienda.
- corrisponde alla media di tutti i vostri livelli di maturità (a livello di domanda).
- può essere inferiore o pari al punteggio massimo.
- dovrebbe essere il più vicino possibile al punteggio massimo. Più il punteggio della vostra azienda è inferiore al punteggio massimo, minori sono le probabilità che riceviate etichette TISAX.

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

Details: YOUR RESULT SCORE ❶

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figura 25. Il punteggio della vostra azienda (foglio Excel “Risultati (ISA5)”)

❶ Punteggio della vostra azienda

Sempre utilizzando una rappresentazione riportata sopra (Figura 22, “Livelli di maturità a livello di domanda”), è possibile vedere nella figura di seguito cosa viene calcolato nella media per il punteggio:

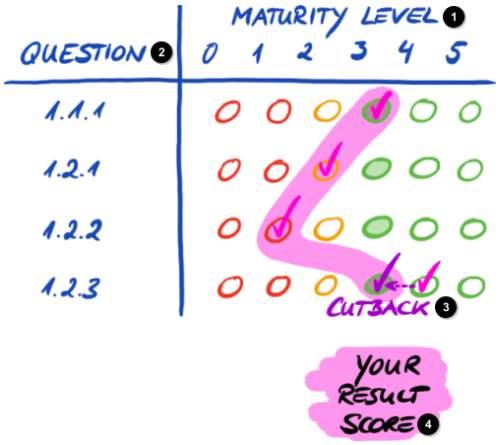


Figura 26. Il punteggio della vostra azienda (a livello di punteggio)

1. Livello di maturità
2. Domanda
3. Abbassamento
4. Punteggio della vostra azienda

Il punteggio indica se:

- la vostra azienda è pronta per una valutazione TISAX.
- potete aspettarvi di ricevere etichette TISAX.

Se il punteggio della vostra azienda (“Risultato con abbassamento ai livelli di maturità target”) è inferiore a “3,0”, significa che almeno per una domanda il livello di maturità della vostra azienda non corrisponde al livello di maturità target. In questo caso, dovrete probabilmente migliorare il sistema di gestione della sicurezza delle informazioni della vostra azienda prima che questa sia pronta per una valutazione TISAX.

Attenzione:

Per il punteggio complessivo, sono previsti limiti formali per una “distanza” accettabile tra il punteggio della vostra azienda e il punteggio massimo (“Risultato con abbassamento ai livelli di maturità target”).

Se il punteggio della vostra azienda è inferiore di oltre:

- il 10%, il risultato complessivo della valutazione sarà “non conforme di livello minore”.
- il 30%, il risultato complessivo della valutazione sarà “non conforme di livello grave”.

Nota importante:

Un punteggio (“Risultato con abbassamento ai livelli di maturità target”) pari a “3” non garantisce il superamento della valutazione TISAX senza rilievi negativi. Tenete presente che il fornitore di audit potrebbe considerare alcuni aspetti in modo diverso da voi.

5.2.4.6. La vostra azienda è pronta?

Lo scopo dell’analisi di cui sopra è capire se la vostra azienda è pronta per una valutazione TISAX.

La vostra azienda è sicuramente pronta per una valutazione TISAX se il punteggio ottenuto

("Risultato con abbassamento ai livelli di maturità target") è pari (o vicino a) "3,0". In tal caso, tutti i valori della colonna "Risultati" (H) sono verdi (non arancioni o rossi).

Se non sono verdi, occorre gestire il risultato dell'autovalutazione (si veda Sezione 5.2.5, "Gestione del risultato dell'autovalutazione").

La figura riportata di seguito mostra il diagramma a ragnatela ISA nel foglio Excel "Risultati (ISA5)". La linea verde indica il livello di maturità target per capitolo. Se i vostri livelli di maturità si trovano in corrispondenza o al di sopra di questa linea, la vostra azienda è pronta per una valutazione TISAX. Se si trovano invece al di sotto di questa linea, ciò potrebbe non essere sufficiente per ricevere etichette TISAX.

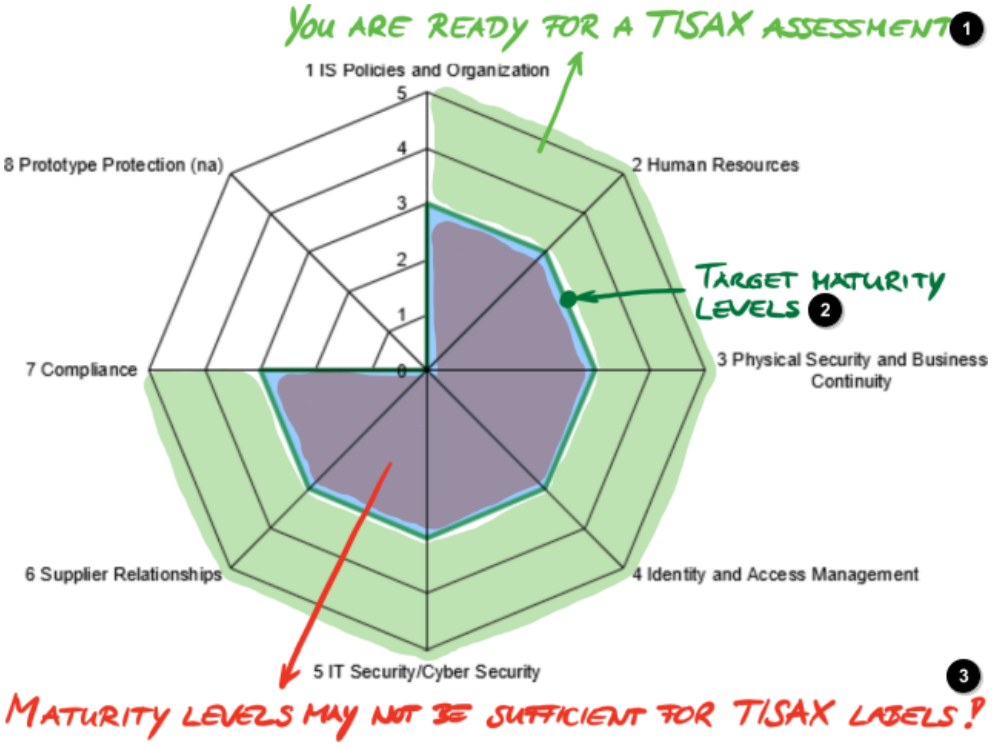


Figura 27. Screenshot: Raggiungimento del livello di maturità target nel diagramma a ragnatela ISA (foglio Excel "Risultati (ISA5)")

1. La vostra azienda è pronta per una valutazione TISAX
2. Livelli di maturità target
3. I livelli di maturità potrebbero non essere sufficienti per le etichette TISAX!

Se si "scompone" il diagramma a ragnatela ISA fino al livello della domanda, si ottiene una rappresentazione simile in verde/rosso a livello della domanda:

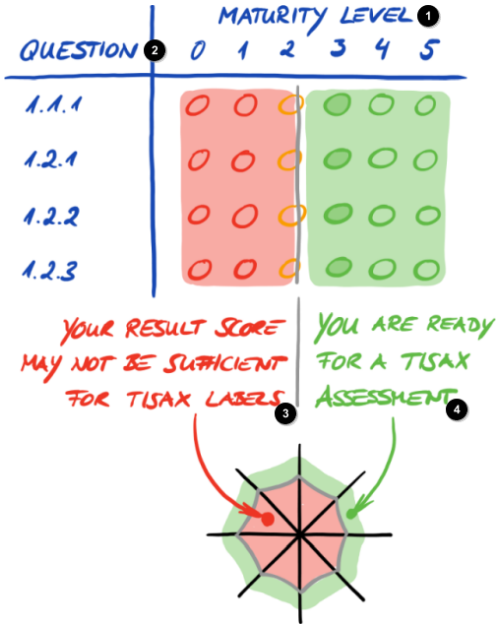


Figura 28. “Scomposizione” del diagramma a ragnatela ISA

1. Livello di maturità
2. Domanda
3. Il vostro punteggio potrebbe non essere sufficiente per le etichette TISAX
4. La vostra azienda è pronta per una valutazione TISAX

5.2.5. Gestione del risultato dell’autovalutazione

Il risultato dell’autovalutazione potrebbe mostrare che è necessario migliorare il sistema di gestione della sicurezza delle informazioni della vostra azienda prima che questa sia pronta per ricevere le etichette TISAX.

Potreste già sapere come colmare alcuni divari tra il livello di maturità della vostra azienda e il livello di maturità target, mentre per altri, invece, potreste aver bisogno di una consulenza esterna. In tal caso, potete rivolgervi ai nostri fornitori di audit TISAX per ricevere un servizio di consulenza. Nell’ambito di TISAX essi possono effettuare consulenze, tuttavia ciò non è obbligatorio. Si precisa che il fornitore di audit a cui vi rivolgete per un’attività di consulenza non potrà più condurre valutazioni TISAX per la vostra azienda.

Nota importante:

Una *mancata* gestione adeguata del risultato dell’autovalutazione *prima* di sottoporsi a una valutazione rappresenta un ostacolo importante per molte aziende. Vi invitiamo a non sottovalutare il lavoro che potrebbe essere necessario per adeguare il sistema di gestione della sicurezza delle informazioni della vostra azienda in base ai requisiti. Molte aziende hanno

bisogno di predisporre in maniera formale un progetto di ampia portata per prepararsi a una valutazione TISAX.

Attenzione:

Se cercate un supporto esterno per completare il processo TISAX, scoprirete che diverse aziende offrono servizi di consulenza e formazione. Nessuna di queste aziende è associata a noi.

Allo stato attuale:

- non offriamo corsi di formazione ufficiali, né direttamente né tramite terzi.
- non ci pronunciamo sulla qualità dei servizi offerti da terzi e consigliamo quindi di agire con prudenza.

Attenzione:

Si sconsiglia di richiedere od ordinare servizi come una “valutazione preliminare” o una “analisi dei divari”. Pur riconoscendo il desiderio di prepararsi alla valutazione con queste modalità, in quasi tutti i casi è più sensato iniziare subito la valutazione.

Per maggiori informazioni sul motivo per cui sconsigliamo le valutazioni preliminari, si veda Sezione 7.7, “Allegato: Motivazioni a sfavore delle “valutazioni preliminari” e delle “analisi dei divari””.

5.3. Selezione del fornitore di audit

Solo i fornitori di audit convenzionati con noi sono autorizzati a condurre le valutazioni TISAX[15]. I fornitori di audit TISAX possono condurre valutazioni TISAX per la vostra azienda solo se non hanno ricevuto in precedenza incarichi di consulenza da parte vostra.

Tutti i nostri fornitori di audit TISAX sono obbligati a condurre valutazioni TISAX solo per le aziende registrate come partecipanti TISAX.

Nota importante:

Dovreste cominciare a contattare i nostri fornitori di audit non appena avrete registrato un ambito di valutazione TISAX per scoprire come diventare fornitori di audit TISAX. La loro disponibilità è soggetta a determinati tempi di attesa, pertanto contattarli *dopo* aver terminato i preparativi potrebbe comportare inutili ritardi.

Attenzione:

Ogni ambito di valutazione ha il proprio ciclo di vita. In questa fase il vostro ambito di valutazione deve avere lo stato “Approvato” o “Registrato”.

Per maggiori informazioni sullo stato di una valutazione, si veda Sezione 7.5.5, “Assessment scope status “Awaiting your payment” (Stato dell’ambito di valutazione “In attesa del pagamento”)”.

5.3.1. Dati di contatto

Potete contattare tutti i fornitori di audit TISAX e richiedere delle offerte non appena avrete registrato un ambito di valutazione TISAX. I loro dati di contatto sono riportati nell’e-mail di conferma della registrazione che avete ricevuto[16] (si veda Sezione 4.5.8, “E-mail di conferma”).

Attenzione:

Vi invitiamo a chiedere offerte ai nostri fornitori di audit TISAX solo DOPO che avrete registrato la vostra azienda. I fornitori di audit verificheranno l’effettiva registrazione e hanno l’obbligo di rifiutare richieste prive di registrazione.

È anche per questo motivo che i dati di contatto dei fornitori di audit sono indicati solo nell’e-mail di conferma della registrazione e non sul nostro sito web pubblico.

5.3.2. Copertura

Sebbene al momento molti dei fornitori di audit abbiano sede in Germania, è importante tenere presente che tutti i nostri fornitori di audit sono generalmente in grado di condurre valutazioni TISAX in tutto il mondo. La maggior parte di loro dispone persino di dipendenti propri in molti Paesi.

Sul nostro sito web è presente una pagina in cui è possibile selezionare il proprio Paese e vedere quale fornitore di audit dispone di personale commerciale locale e/o auditor locali (enx.com/en-US/TISAX/xap/).

5.3.3. Richiesta di offerte

Per consentire ai nostri fornitori di audit TISAX di calcolare con precisione il lavoro previsto per la valutazione, è necessario includere sempre il “TISAX Scope Excerpt” (“Estratto dell’ambito TISAX”).

Figura 29. Immagine in miniatura di un estratto dell'ambito (prima pagina)

Per maggiori informazioni, si veda Sezione 4.5.8, "E-mail di conferma".

Attenzione:

L'imparzialità è una caratteristica fondamentale dei nostri fornitori di audit TISAX, i quali si assicureranno che non vi siano conflitti di interessi. Si consiglia di tenere conto di questo aspetto quando li si contatta poiché, se la vostra azienda è in qualche modo legata a un fornitore di audit, non potete aspettarvi di essere valutati da tale soggetto.

5.3.4. Valutazione delle offerte

Potete scegliere liberamente uno qualsiasi dei nostri fornitori di audit TISAX. Tutti i fornitori di audit sono vincolati dallo stesso contratto e conducono le valutazioni sulla base degli stessi criteri e degli stessi metodi di audit. In termini di risultato della valutazione, non vi saranno differenze a prescindere dal fornitore di audit scelto. Il risultato della vostra valutazione sarà accettato da tutti i partecipanti TISAX.

Oltre a fattori ovvi come il prezzo, la reputazione e la cortesia, vi sono altri aspetti di un'offerta da tenere in considerazione:

- Disponibilità:
  Quando può cominciare il processo di valutazione? Questo potrebbe essere un aspetto importante se la vostra azienda ha urgenza di ricevere una valutazione TISAX.
- Spese di viaggio per gli appuntamenti in loco:
  Un fornitore di audit con sedi nel vostro Paese potrebbe applicare spese di viaggio inferiori.
- Lingua:
  L'auditor è in grado di comunicare con tutti i soggetti della vostra azienda coinvolti nei colloqui nella lingua madre?
- Portata dell'offerta:
  Quali valutazioni sono incluse?
  Per maggiori informazioni su questo aspetto, si veda Sezione 5.4.3, "Tipologie di valutazione

TISAX”.
Normalmente le offerte comprendono la valutazione iniziale e la valutazione del piano d’azione correttivo. Poiché è difficile prevedere il lavoro necessario per le valutazioni di follow-up, la relativa offerta viene generalmente fornita una volta che sono state completate le altre valutazioni.

Infine un aspetto fondamentale è legato alla fiducia: dovrete instaurare un rapporto di fiducia con il vostro fornitore di audit dal momento che egli dovrà acquisire conoscenze approfondite sulla vostra azienda.

Attenzione:

Si sconsiglia di richiedere od ordinare servizi come una “valutazione preliminare” o una “analisi dei divari”. Pur riconoscendo il desiderio di prepararsi alla valutazione con queste modalità, in quasi tutti i casi è più sensato iniziare subito la valutazione.

Per maggiori informazioni sul motivo per cui sconsigliamo le valutazioni preliminari, si veda Sezione 7.7, “Allegato: Motivazioni a sfavore delle “valutazioni preliminari” e delle “analisi dei divari””.

Attenzione:

Anche se ci piacerebbe potervi dire a quanto ammonterà l’offerta dei nostri fornitori di audit per condurre la valutazione, ci teniamo a precisare che non ci è possibile fornire questa informazione poiché i costi dipendono da troppi fattori. Inoltre, i nostri fornitori di audit sono liberi di effettuare i propri calcoli di natura commerciale.

Tuttavia, possiamo fornirvi alcune stime piuttosto approssimative sul numero di uomini/giorno che i nostri fornitori di audit vi addebiteranno. Per un’azienda media di piccole dimensioni con una sola sede, dovreste aspettarvi un’offerta che va da tre uomini/giorno e mezzo a quattro uomini/giorno per una valutazione nel livello di valutazione 2 e da cinque a sei uomini/giorno per una valutazione nel livello di valutazione 3.

Attenzione:

Ogni valutazione ha il proprio ciclo di vita.

Per maggiori informazioni sullo stato di una valutazione, si veda Sezione 7.6, “Allegato: Assessment status (Stato della valutazione)”.

Una volta che avrete scelto uno dei nostri fornitori di audit TISAX, potrete iniziare il processo di

valutazione TISAX.

5.4. Il processo di valutazione TISAX

5.4.1. Panoramica

Il processo di valutazione TISAX consiste in diverse tipologie di valutazione. Nella maggior parte dei casi, sarà effettuata più di una valutazione.

Il processo di valutazione deve essere visto come una sequenza di fasi interconnesse tra loro in cui:

- Voi predisponete il sistema di gestione della sicurezza delle informazioni della vostra azienda affinché sia perfettamente efficiente.
- Il fornitore di audit verifica se il sistema di gestione della sicurezza delle informazioni della vostra azienda soddisfa una serie di requisiti predefiniti e nel farlo potrebbe rilevare dei divari.
- La vostra azienda provvede a colmare tali divari entro termini prestabiliti.
- Il fornitore di audit verifica nuovamente se i divari sono stati colmati.

Queste fasi si alternano fino a quando tutti divari non sono stati colmati.

È importante capire che siete *voi* ad avviare ciascuna sotto-fase del processo di valutazione. L'intero processo di valutazione è sotto il vostro controllo. E ovviamente siete voi a decidere se interrompere e abbandonare il processo di valutazione ogni volta che lo desiderate.[17]

La macro-struttura del processo di valutazione TISAX è la seguente:

- Riunione iniziale
  La vostra azienda pianifica i dettagli del processo di valutazione con il fornitore di audit.
- Fase 1 della valutazione
  Il fornitore di audit verifica l'autovalutazione della vostra azienda.
- Fase 2 della valutazione
  Il fornitore di audit conduce la/le valutazione/i.

5.4.2. Riunione iniziale

Il processo di valutazione TISAX comincia con la riunione iniziale, durante la quale vengono pianificati i dettagli del processo di valutazione. Di solito, la riunione iniziale si svolge tramite conference call. Sarà il fornitore di audit a guidarvi durante la riunione.

Verranno discussi, tra gli altri, i seguenti argomenti:

- Chi sono i partecipanti alla riunione?

- Chi è l'azienda sottoposta a valutazione?
- Come funziona il processo di valutazione TISAX?
- Qual è l'ambito di valutazione? È corretto?
- È escluso qualsiasi conflitto di interessi?
- Come si presenta una buona autovalutazione?
- Chi è responsabile di cosa?
- Come si comunica?
- Quando si svolge la valutazione (e quali sono le altre tempistiche)?
- Chi deve partecipare alla/e valutazione/i?
- Chi si può contattare in caso di reclami?

Il periodo che intercorre tra la fine della riunione iniziale e la consegna dell'autovalutazione è in genere compreso tra uno e tre mesi. Tuttavia, anche un periodo di sei mesi non è insolito. La durata di tale periodo dipende dallo stato di preparazione della vostra azienda e TISAX non impone alcuna scadenza specifica. Potete prendervi tutto il tempo che vi serve per preparare la vostra autovalutazione e per prepararvi alla valutazione.

5.4.3. Tipologie di valutazione TISAX

Il processo di valutazione TISAX è composto dalle seguenti tre tipologie di valutazione TISAX:

- Valutazione iniziale (🇬🇧 Initial assessment)
- Valutazione del piano d'azione correttivo (🇬🇧 Corrective action plan assessment)
- Valutazione di follow-up (🇬🇧 Follow-up assessment) [18]

La valutazione iniziale viene sempre eseguita, mentre le altre due valutazioni TISAX potrebbero venire eseguite, anche più volte. Esse verranno effettuate fino a quando:

- tutti i divari non saranno colmati
- o la vostra azienda non abbandona il processo di valutazione TISAX
- o non viene raggiunto il periodo di tempo massimo di nove mesi dopo la fine della riunione di chiusura della valutazione iniziale (a questo punto è necessario condurre un'altra valutazione iniziale).

Tutte le valutazioni TISAX sono descritte nelle sezioni riportate di seguito.

Attenzione:

Ogni valutazione ha il proprio ciclo di vita.

> Per maggiori informazioni sullo stato di una valutazione, si veda Sezione 7.6, “Allegato: Assessment status (🇮🇹 Stato della valutazione)”.

5.4.4. Elementi delle valutazioni TISAX

Ciascuna valutazione TISAX è composta dai seguenti elementi:

- Riunione formale di apertura[19][20]
  - Il suo scopo è affrontare tutti gli argomenti organizzativi.
  - Non deve necessariamente essere in presenza.
  - Gli argomenti possono essere affrontati in una sola sessione o suddivisi in più occasioni.
  - Si tratta di un “contenitore logico” di tutti gli argomenti organizzativi *pre*-valutazione.
- Procedura di valutazione
  - Il vostro fornitore di audit verifica tutti i requisiti.
  - Vengono selezionati i metodi di valutazione in base al rispettivo livello di valutazione.
- Riunione formale di chiusura[21]
  - Rappresenta la conclusione di una valutazione TISAX.
  - Il fornitore di audit presenta i rilievi emersi.
  - Il fornitore di audit annuncia il risultato della valutazione.
  - Non deve necessariamente essere in presenza.
  - Si tratta di un “contenitore logico” di tutti gli argomenti organizzativi *post*-valutazione.

Dopo la “riunione di chiusura” il fornitore di audit prepara e invia alla vostra azienda la bozza della “relazione della valutazione TISAX” aggiornata. Potete sollevare obiezioni se ritenete che il fornitore di audit abbia interpretato male alcuni aspetti.[22] Il fornitore di audit provvederà quindi a emettere la “relazione della valutazione TISAX” definitiva.

Tutti questi elementi saranno descritti nelle sezioni riportate di seguito.

5.4.5. Informazioni sulla conformità

Prima di continuare a illustrare il processo di valutazione TISAX, vogliamo spiegarvi un concetto chiave che è essenziale per la comprensione delle sezioni che seguono.

Lo scopo di una valutazione TISAX è stabilire se il sistema di gestione della sicurezza delle informazioni della vostra azienda soddisfa una serie di requisiti predefiniti. Il fornitore di audit verifica se il sistema di gestione della sicurezza delle informazioni della vostra azienda “è conforme” (🇬🇧 “conforms”) ai requisiti.

Fase 1: i controlli vengono effettuati per ciascun requisito applicabile singolarmente.

Se l’approccio della vostra azienda “è conforme” a tutti i requisiti, supererete la valutazione e riceverete le etichette TISAX che corrispondono ai vostri obiettivi di valutazione.

Qualsiasi aspetto che sia inferiore a una conformità completa o ideale rispetto ai requisiti viene chiamato “rilievo” (finding). TISAX distingue tra quattro tipi di rilievi:

N.	Tipo	Definizione	Reazione	Esempi
1.	Non conformità *grave* (*Major* non-conformity)	Una non conformità *grave*: ▪ crea un rischio immediato e significativo per la sicurezza delle informazioni della vostra azienda ▪ **o** genera dubbi sull’efficacia complessiva del sistema di gestione della sicurezza delle informazioni della vostra azienda	Cosa dovete fare: ▪ risolvere immediatamente le non conformità *gravi* con misure compensative adeguate ▪ implementare le azioni correttive senza inutili ritardi	▪ Non conformità sistematiche ▪ Carenze di implementazione che creano rischi critici per la sicurezza delle informazioni riservate ▪ Carenze di implementazione non risolte con un’azione correttiva appropriata
2.	Non conformità *minore* (*Minor* non-conformity)	Una non conformità *minore*: ▪ *non* crea un rischio immediato e significativo per la sicurezza delle informazioni della vostra azienda ▪ **e** *non* genera dubbi sull’efficacia complessiva del sistema di gestione della sicurezza delle informazioni della vostra azienda	Cosa dovete fare: ▪ implementare le azioni correttive senza inutili ritardi	▪ Errori isolati o sporadici ▪ Non conformità o carenze nell’implementazione dei requisiti o delle politiche della vostra azienda

N.	Tipo	Definizione	Reazione	Esempi
3.	Osservazione (Observation)	Un'osservazione è una non conformità rispetto ai requisiti o alle politiche della vostra azienda; non crea un rischio immediato per la sicurezza delle vostre informazioni ma potrebbe farlo in futuro.	Cosa dovete fare: ▪ analizzare, monitorare e valutare con attenzione i possibili rischi ▪ decidere come gestire l'osservazione	N/A
4.	Margine di miglioramento (Room for improvement)	Una discrepanza che non rientra nelle tipologie sopra menzionate e che non crea un rischio per la sicurezza delle informazioni della vostra azienda, ma che offre evidenti margini di miglioramento.	Potete decidere se e come gestire questo tipo di rilievo.	N/A

Tabella 11. I quattro tipi di rilievi

Fase 2: tutti i risultati della fase precedente relativa a "ciascun requisito" sono accorpati nel risultato complessivo della valutazione.

Il risultato complessivo della valutazione può essere:

a. Conforme (Conform)
Il risultato complessivo della valutazione è "conforme" quando tutti i requisiti sono soddisfatti.

b. Non conforme di livello minore (Minor non-conform)
Il risultato complessivo della valutazione è "non conforme di livello minore" se un requisito presenta almeno una "non conformità minore".

c. Non conforme di livello grave (Major non-conform)
Il risultato complessivo della valutazione è "non conforme di livello grave" se un requisito presenta almeno una "non conformità grave".
(In mancanza di un piano d'azione correttivo approvato, qualsiasi non conformità determina un risultato complessivo della valutazione "non conforme di livello grave".)

Se il risultato complessivo della valutazione è:

- “non conforme di livello minore”, la vostra azienda potrà ricevere etichette TISAX *temporanee* fino a quando tutte le non conformità non saranno risolte.
- “non conforme di livello grave”, la vostra azienda dovrà risolvere il rispettivo problema prima di poter ricevere qualsiasi etichetta TISAX.
  Adottando misure compensative e azioni correttive adeguate approvate dal fornitore di audit, è possibile modificare il risultato complessivo della valutazione da “non conforme di livello grave” a “non conforme di livello minore” e quindi ricevere etichette TISAX temporanee.

È importante ricordare che il risultato complessivo della valutazione migliorerà nel corso dell’intero processo di valutazione TISAX.

Facciamo un esempio estremamente semplificato: dopo la valutazione iniziale il risultato complessivo della valutazione potrebbe essere “non conforme di livello grave”. In seguito, provvedete quindi a mitigare il rischio corrispondente e il risultato complessivo della valutazione passa da “non conforme di livello grave” a “non conforme di livello minore”. Una volta eliminato il rischio, il risultato complessivo finale della valutazione sarà “conforme”.

Tutto ciò verrà descritto in maniera molto più dettagliata in seguito. Inoltre maggiori informazioni sulle etichette TISAX sono riportate più sotto in Sezione 5.4.14, “Etichette TISAX”.

5.4.6. La preparazione della vostra azienda per il processo di valutazione TISAX

Il fornitore di audit predisporrà la valutazione sulla base della vostra autovalutazione. Ricordatevi quindi di rendere disponibile la vostra autovalutazione per il fornitore di audit in anticipo. Le scadenze esatte per la consegna vengono concordate durante la riunione iniziale.

Se il fornitore di audit sarà adeguatamente informato, la valutazione richiederà meno tempo. Oltre all’autovalutazione, il fornitore di audit vi chiederà anche la relativa documentazione prima di condurre la valutazione. Può trattarsi di documenti a cui avete fatto riferimento nell’autovalutazione e di altra documentazione che il fornitore di audit considera rilevante.

Egli programmerà quindi la procedura di valutazione sulla base di queste informazioni.

5.4.7. Valutazione iniziale

Si tratta della prima valutazione TISAX e rappresenta formalmente l’inizio del processo di valutazione TISAX.

Nota importante:

La valutazione iniziale segna l’inizio di due periodi importanti:

1. Il periodo di validità massimo delle etichette TISAX è di tre anni.
2. Il periodo per risolvere le non conformità è di nove mesi. Se tutte le non conformità non vengono risolte entro questo periodo, la vostra azienda non riceverà le etichette TISAX. Tuttavia, nel caso in cui questa scadenza non venga rispettata, è possibile proseguire direttamente con una nuova valutazione iniziale.

Entrambi i periodi decorrono dal giorno della riunione di chiusura della valutazione iniziale.

Attenzione:

Oltre ai due periodi descritti sopra, non vi sono altri vincoli temporali. Non sono ad esempio previste scadenze per il completamento della procedura di registrazione online, per contattare i nostri fornitori di audit o per condurre la riunione iniziale. Siete voi a decidere quando avviare la valutazione iniziale.

5.4.7.1. La prima riunione formale di apertura

Come per tutte le valutazioni TISAX, la valutazione iniziale comincia con una riunione formale di apertura. La riunione formale di apertura viene generalmente condotta tramite conference call o videoconferenza. Nel caso di aziende di piccole dimensioni che hanno eventualmente già maturato un po' di esperienza con altri audit, questa riunione non richiede molto tempo.

Lo scopo di questa riunione è:

- verificare i prerequisiti della valutazione
- presentare il responsabile del progetto di valutazione e il team di valutazione
- pianificare la valutazione

5.4.7.2. Procedura di valutazione

Il fornitore di audit conduce la valutazione iniziale in base alla pianificazione effettuata. I relativi dettagli dipendono dagli obiettivi di valutazione della vostra azienda. La valutazione consiste per lo più di conference call, interviste in sede e ispezioni in sede in vari gradi di profondità[23].

Il fornitore di audit presenta tutti i rilievi emersi durante la valutazione iniziale.

5.4.7.3. Riunione di chiusura

Durante la riunione di chiusura il fornitore di audit riassume nuovamente i rilievi emersi.

5.4.7.4. Relazione della valutazione TISAX

Dopo la riunione di chiusura il fornitore di audit prepara e invia alla vostra azienda la bozza della “relazione della valutazione TISAX”. Potete sollevare obiezioni se ritenete che il fornitore di audit abbia interpretato male alcuni aspetti.[24] Il fornitore di audit provvederà quindi a emettere la “relazione della valutazione TISAX”.

A questo punto il risultato complessivo della valutazione sarà:

- Conforme, o
- Non conforme di livello grave
  La presenza di non conformità (minori) non risolte comporta sempre un risultato complessivo della valutazione corrispondente a “non conforme di livello grave”. Il risultato complessivo della valutazione può passare a “non conforme di livello minore” solo dopo che avrete definito le azioni attraverso cui implementare le misure finalizzate a risolvere le non conformità.
  Per maggiori informazioni su questo aspetto, si veda Sezione 5.4.9.4, “Etichette TISAX temporanee”.

Se il risultato complessivo della valutazione è “conforme” fin dalla valutazione iniziale, potete saltare il resto della sezione relativa alla valutazione e procedere con la fase di scambio del risultato.

Se il risultato complessivo della valutazione è “non conforme di livello grave” il passo successivo da seguire è quello di elaborare un piano su come risolvere i rilievi emersi e colmare eventuali divari rilevati dal fornitore di audit. Il piano viene ufficialmente chiamato “piano d’azione correttivo” (🇬🇧 “corrective action plan”).

Attenzione:

Se, prima dell’inizio della valutazione, siete a conoscenza di una situazione che comporterà una non conformità e non siete in grado di risolverla prima della valutazione, potete già elaborare un’azione correttiva (compresa la data di implementazione) e presentarla al fornitore di audit durante la valutazione. In teoria in questo modo il risultato complessivo della valutazione potrebbe essere “non conforme di livello minore”. Si tratta tuttavia di una circostanza *rara*.

5.4.8. Preparazione del piano d’azione correttivo

Il “piano d’azione correttivo” (🇬🇧 “corrective action plan”) stabilisce le modalità con cui prevedete di risolvere i rilievi emersi durante la valutazione iniziale. Il fornitore di audit valuterà l’adeguatezza del “piano d’azione correttivo” (si veda la sezione seguente).

Per elaborare il “piano d’azione correttivo”, dovete prendere in considerazione i seguenti

requisiti:

- Rilievo
  - Dovete indicare quale rilievo l'azione correttiva punta a risolvere.
- Causa principale
  - Dovete identificare e specificare la causa principale del rilievo.
- Azioni correttive
  - Per ciascuna non conformità dovete stabilire una o più "azioni correttive" attraverso cui implementare le misure finalizzate a risolvere la non conformità in questione.
- Data di implementazione
  - Dovete stabilire una data di implementazione per ciascuna azione correttiva.
  - Il periodo di implementazione deve essere tale da fornire tempo sufficiente per l'attuazione completa delle misure.
- Misure compensative
  - Per tutte le non conformità che creano rischi critici, è necessario stabilire misure compensative che risolvano le non conformità fino a quando le azioni correttive non saranno implementate.
- Periodo di implementazione
  - Il periodo di implementazione deve essere giustificato per tutte le azioni correttive la cui attuazione richiede più di tre mesi.
  - Per tutte le azioni correttive la cui attuazione richiede più di tre mesi, dovete inoltre fornire prove che dimostrino che non è possibile attuarle più rapidamente.
  - Il periodo di implementazione di qualsiasi azione correttiva non può essere superiore a nove mesi.

Una volta completato il piano d'azione correttivo, potete richiedere la "valutazione del piano d'azione correttivo".

Nota importante:

Consigliamo di avviare l'implementazione il prima possibile. Non è necessario attendere il risultato della "valutazione del piano d'azione correttivo".
La "valutazione del piano d'azione correttivo" generalmente avviene una volta inviato il piano d'azione correttivo al fornitore di audit.

Attenzione:

I requisiti di TISAX riguardano solo il contenuto e non la forma dei piani d'azione correttivi.

> La maggior parte dei nostri fornitori di audit mette a disposizione dei modelli per i piani d'azione correttivi.

5.4.9. Valutazione del piano d'azione correttivo

Lo scopo della "valutazione del piano d'azione correttivo" è verificare che il vostro "piano d'azione correttivo" (si veda sopra) soddisfi i requisiti TISAX.

Voi inviate quindi il "piano d'azione correttivo" al vostro fornitore di audit, il quale lo valuta in base ai requisiti (si veda sopra). Se il piano soddisfa i requisiti, il fornitore di audit emetterà la "relazione della valutazione TISAX" aggiornata.

Questa valutazione generalmente non richiede molto tempo. Nella maggior parte dei casi viene effettuata attraverso conference call o videoconferenza, a volte anche solo tramite e-mail.

5.4.9.1. Motivazioni alla base di una valutazione del piano d'azione correttivo

Le motivazioni alla base di una "valutazione del piano d'azione correttivo" sono:

- Non conformità residue dopo
  - una valutazione iniziale
  - una valutazione di follow-up
  - una valutazione di estensione dell'ambito
- Un "piano d'azione correttivo" che è già stato valutato ma non ha soddisfatto i requisiti
- I fattori determinanti alla base del calcolo dei periodi di implementazione di un piano d'azione correttivo sono cambiati

5.4.9.2. Combinazione con la valutazione iniziale

La "valutazione del piano d'azione correttivo" non è necessariamente un evento a sé stante. Potete già presentare il vostro "piano d'azione correttivo" durante la riunione di chiusura della valutazione iniziale. Il fornitore di audit potrà quindi direttamente eseguire la "valutazione del piano d'azione correttivo".

Se associate la "valutazione del piano d'azione correttivo" con la valutazione iniziale e il vostro "piano d'azione correttivo" soddisfa i requisiti, potete concordare con il fornitore di audit che non avete bisogno di una "relazione della valutazione iniziale". Al suo posto il fornitore di audit preparerà solamente la "relazione della valutazione del piano d'azione correttivo". Questa relazione vi consente di ricevere direttamente etichette TISAX temporanee.

5.4.9.3. Requisiti del piano d'azione correttivo

Il fornitore di audit valuta il vostro "piano d'azione correttivo" sulla base dei seguenti requisiti:

- Adeguatezza delle misure
  - Il fornitore di audit valuterà l'adeguatezza di un'azione correttiva in base alla sua capacità di risolvere la causa principale della non conformità.
- Mitigazione dei rischi critici attraverso misure compensative adeguate[25]
- Adeguatezza dei periodi di implementazione
  - I periodi di implementazione decorrono dal giorno in cui si conclude la valutazione iniziale.
- Periodi di implementazione non superiori a:
  - tre mesi senza giustificazione aggiuntiva
  - sei mesi senza giustificazione aggiuntiva e prove
  - nove mesi

5.4.9.4. Etichette TISAX temporanee

Se il risultato complessivo della valutazione è "non conforme di livello minore" riceverete etichette TISAX temporanee.

Il vantaggio delle etichette TISAX temporanee consiste nel fatto che il vostro partner generalmente le accetterà a condizione che in seguito riceviate le etichette TISAX definitive. Ciò può essere utile se avete urgenza di dimostrare al vostro partner l'efficacia del sistema di gestione della sicurezza delle informazioni della vostra azienda.

Il prerequisito per ricevere le etichette TISAX temporanee è una relazione della valutazione del piano d'azione correttivo con risultato complessivo della valutazione "non conforme di livello minore".

Le etichette TISAX temporanee sono esattamente uguali alle etichette TISAX definitive. L'unica differenza è data dal periodo di validità più breve delle etichette TISAX temporanee.

Le etichette TISAX temporanee sono valide per un massimo di nove mesi dopo la riunione di chiusura della valutazione iniziale. Il periodo di validità delle etichette TISAX temporanee viene stabilito sulla base del periodo di implementazione più lungo delle azioni correttive.

Esempi:

- Viene rilevata una sola non conformità per la vostra azienda, per la quale dovete eseguire la verifica di una policy interna. Il relativo periodo di implementazione è di *due* mesi.
  Le etichette TISAX temporanee saranno quindi valide per *due* mesi.
- Dovete gestire la non conformità relativa alla verifica della policy di cui sopra, alla quale se ne aggiunge un'altra che prevede la costruzione di un nuovo muro esterno come azione correttiva. Per via delle tempistiche necessarie per ottenere le dovute approvazioni dal comune, il relativo periodo di implementazione è di *otto* mesi.

Le etichette TISAX temporanee saranno quindi valide per *otto* mesi.

Per maggiori informazioni sui requisiti per i periodi di implementazione, si veda Sezione 5.4.9.3, “Requisiti del piano d’azione correttivo”

Attenzione:

La “valutazione del piano d’azione correttivo” è facoltativa.

Potete passare direttamente alla valutazione di follow-up se:

- non avete bisogno di etichette TISAX temporanee e
- siete sicuri di poter implementare tutte le azioni correttive senza che il vostro piano venga approvato dal fornitore di audit

Una volta completate tutte le azioni correttive, è necessario richiedere la “valutazione di follow-up”.

5.4.10. Valutazione di follow-up

Lo scopo della “valutazione di follow-up” è quello di valutare se tutte le non conformità precedentemente identificate sono state risolte. Di solito si richiede la valutazione di follow-up quando si è certi che tutte le non conformità sono state risolte.

Potete tuttavia effettuare tutte le valutazioni di follow-up di cui avete bisogno. Se durante una valutazione di follow-up il fornitore di audit rileva ancora la presenza di non conformità residue o addirittura nuove, è sufficiente aggiornare il piano d’azione correttivo e ricominciare questa parte del processo di valutazione.

Questa valutazione può avvenire sia durante una riunione di persona che attraverso una conference call o videoconferenza.

5.4.10.1. Tempistiche

Il fornitore di audit può condurre la/e valutazione/i di follow-up entro un massimo di nove mesi dalla conclusione della valutazione iniziale[26].

5.4.10.2. Prerequisiti

Se non avete bisogno di etichette TISAX temporanee, potete richiedere direttamente una valutazione di follow-up. Non è necessario eseguire una “valutazione del piano d’azione correttivo” prima di una valutazione di follow-up.

5.4.10.3. Scadenza delle etichette TISAX temporanee

Nel caso in cui abbiate bisogno di etichette TISAX temporanee, è importante assicurarsi che non

ci siano ritardi per quanto riguarda la ricezione delle etichette TISAX definitive. Si consiglia quindi di richiedere la valutazione di follow-up con largo anticipo rispetto all'ultima data di scadenza possibile[27]. Il motivo è quello di avere un margine di tempo sufficiente per risolvere eventuali rilievi minori individuati durante la valutazione di follow-up.

5.4.11. Grafico del processo di valutazione TISAX

Le sezioni precedenti sono riassunte nel seguente grafico relativo al processo:

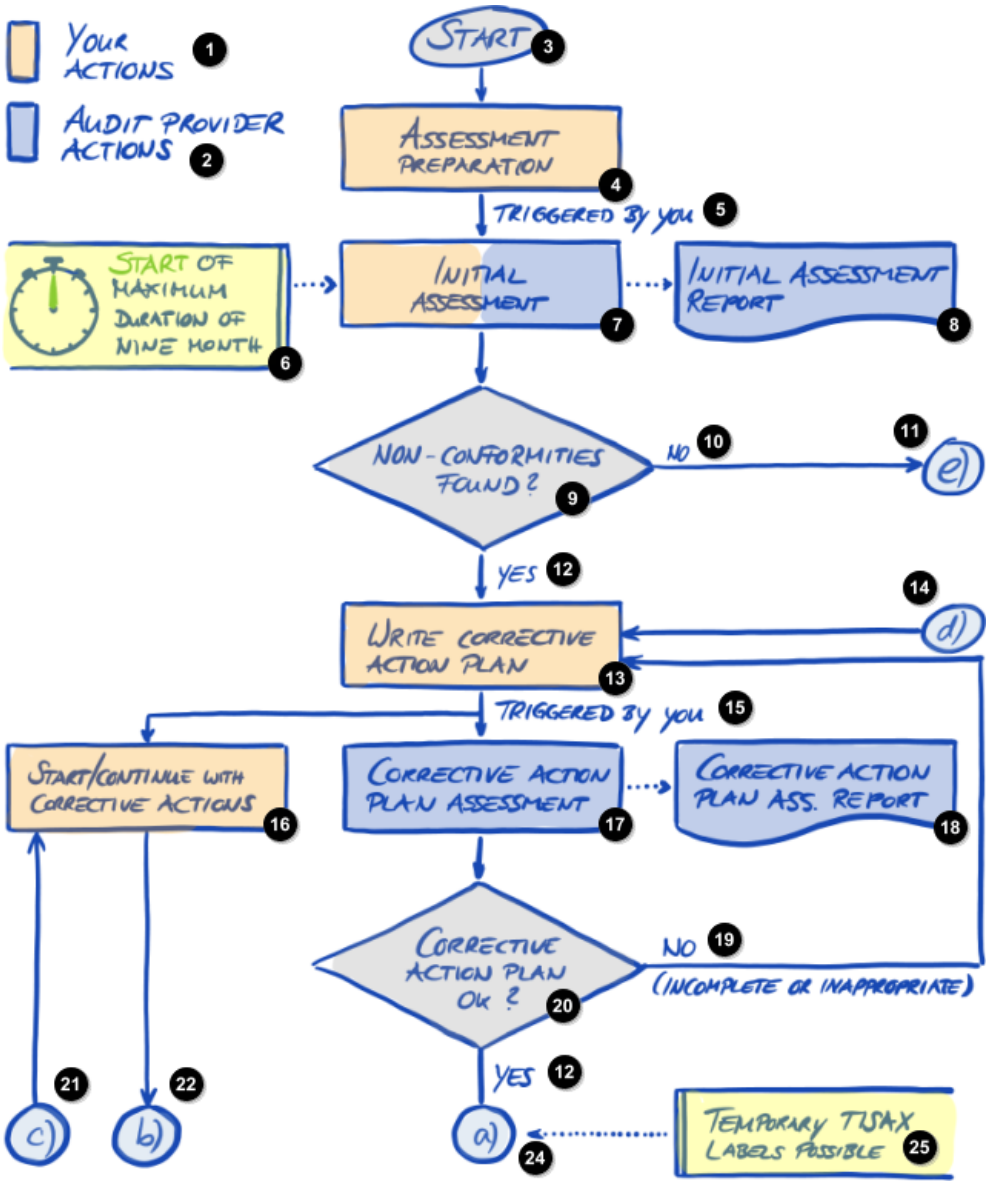


Figura 30. Grafico del processo di valutazione TISAX (parte 1/2)

1. Le vostre azioni
2. Le azioni del fornitore di audit
3. Inizio

4. Preparazione della valutazione
5. Attivazione da parte vostra
6. Inizio del periodo massimo di nove mesi
7. Valutazione iniziale
8. Relazione della valutazione iniziale
9. Rilevazione di non conformità?
10. No
11. e)
12. Sì
13. Elaborazione di un piano d’azione correttivo
14. d)
15. Attivazione da parte vostra
16. Avvio/proseguimento delle azioni correttive
17. Valutazione del piano d’azione correttivo
18. Relazione della valutazione del piano d’azione correttivo
19. No (incompleto o non adeguato)
20. Piano d’azione correttivo ok?
21. c)
22. b)
24. a)
25. Etichette TISAX temporanee possibili

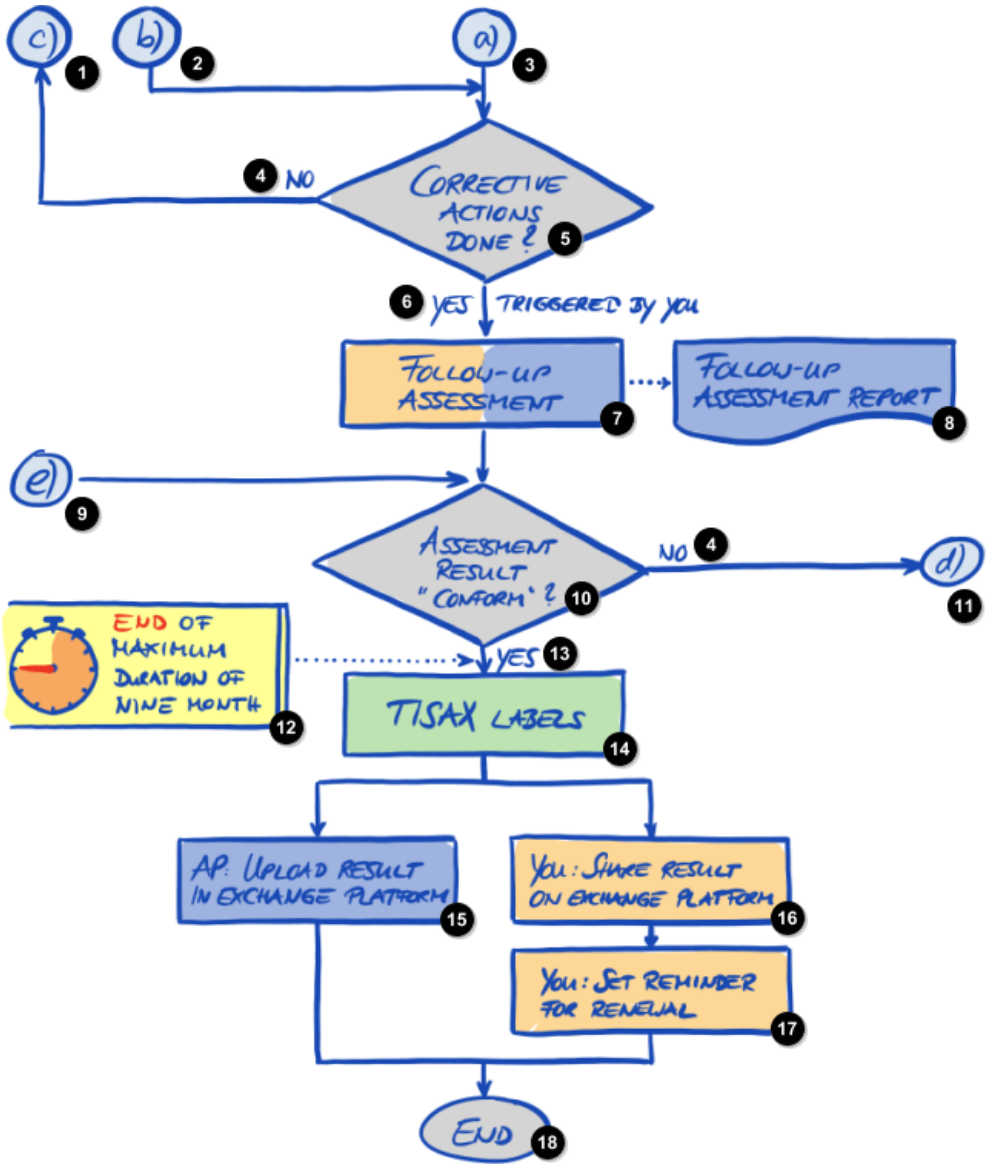


Figura 31. Grafico del processo di valutazione TISAX (parte 2/2)

1. c)
2. b)
3. a)
4. No
5. Azioni correttive eseguite?
6. Sì, attivazione da parte vostra
7. Valutazione di follow-up
8. Relazione della valutazione di follow-up
9. e)

10. Risultato della valutazione “conforme”?
11. d)
12. Termine del periodo massimo di nove mesi
13. Sì
14. Etichette TISAX
15. Fornitore di audit: caricamento del risultato sulla piattaforma di scambio
16. Vostra azienda: condivisione del risultato sulla piattaforma di scambio
17. Vostra azienda: configurazione del promemoria per il rinnovo
18. Fine

5.4.12. Assessment ID (ID Valutazione)

Ciascuna valutazione TISAX di un ambito di valutazione è identificata attraverso un “ID Valutazione”. Questo ID si riferisce al risultato della vostra valutazione e alla relativa relazione della valutazione TISAX.

Di seguito è riportato il formato dell’ID Valutazione:

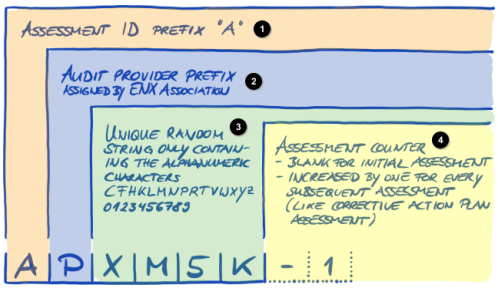


Figura 32. Formato dell’ID Valutazione

1. Prefisso “A” dell’ID Valutazione
2. Prefisso del fornitore di audit assegnato da ENX Association
3. Stringa casuale e univoca contenente solo le seguenti lettere e i seguenti numeri:
   CFHKLMNPRTVWXYZ
   0123456789
4. Contatore delle valutazioni
   - Vuoto per la valutazione iniziale
   - Aumentato di uno per ciascuna valutazione successiva (come la valutazione del piano d’azione correttivo)

Generalmente l’ID Valutazione viene utilizzato nelle comunicazioni inviate alla vostra azienda

dal fornitore di audit.

5.4.13. Relazione della valutazione TISAX

La “relazione della valutazione TISAX” (“TISAX assessment report”):

- viene (aggiornata ed) emessa dopo ciascuna valutazione TISAX.
- documenta i rilievi riscontrati dal fornitore di audit.
- contiene il risultato complessivo della valutazione (conforme, non conforme di livello minore, non conforme di livello grave).
- contiene tutte le altre informazioni relative alla valutazione TISAX (come l’obiettivo di valutazione, l’ambito, le persone e le sedi coinvolte).

La “relazione della valutazione TISAX” può appartenere a una delle seguenti tipologie (a seconda della tipologia di valutazione):

- Relazione della valutazione *iniziale* (*Initial* assessment report)
- Relazione della valutazione del *piano d’azione correttivo* (*Corrective action plan* assessment report)
- Relazione della valutazione di *follow-up* (*Follow-up* assessment report) [28]

La “relazione della valutazione TISAX” segue sempre la stessa struttura[29]. Il fornitore di audit si limita ad ampliarla dopo ciascuna tipologia di valutazione. Ciò significa che dovrete fare riferimento solo all’ultima versione della relazione della valutazione TISAX, poiché essa comprende sempre il contenuto della/e versione/i precedente/i.

Le prime sezioni della “relazione della valutazione TISAX” sono quelle che alla fine vengono condivise con il partner.

Una delle caratteristiche principali di TISAX è che siete unicamente voi a decidere quali parti della relazione della valutazione TISAX condividere con il vostro partner o qualsiasi altro partecipante. La struttura della relazione della valutazione TISAX è stata progettata per consentire questo tipo di condivisione selettiva. Ciascuna sezione offre un livello di dettaglio maggiore.

Ecco come si presenta la struttura della “relazione della valutazione TISAX”:

- A. Informazioni relative alla valutazione
  Denominazione dell’azienda, ambito di valutazione, ID Ambito, ID Valutazione, livello di valutazione, obiettivo/i di valutazione, data/e della valutazione, fornitore di audit
  Questa sezione non contiene alcun risultato della valutazione.
- B. Risultati in sintesi
  Riepilogo del risultato della valutazione (conforme, non conforme di livello minore, non

conforme di livello grave), numero di rilievi, categorizzazione astratta dei rischi risultanti

- C. Riassunto del risultato della valutazione
  Sintesi del risultato della valutazione per capitolo (ad esempio “9 Controllo degli accessi”) e per catalogo di criteri (ad esempio “Sicurezza delle informazioni”)
- D. Livelli di maturità dell’ISA di VDA (scheda dei risultati)
  Livello di maturità per ciascun requisito
- E. Risultati della valutazione in dettaglio
  Descrizione dettagliata di tutti i rilievi, dei risultati della valutazione dei rischi corrispondenti, delle misure necessarie, del periodo di implementazione

Nella fase di “scambio” (descritta di seguito) siete voi a decidere fino a quale livello il vostro partner avrà accesso al contenuto della vostra relazione della valutazione TISAX.

5.4.14. Etichette TISAX

Abbiamo accennato brevemente a questo argomento nella sezione relativa alla preparazione per la registrazione. Come spiegato, quello che una volta era un obiettivo di valutazione è diventato un’etichetta TISAX.

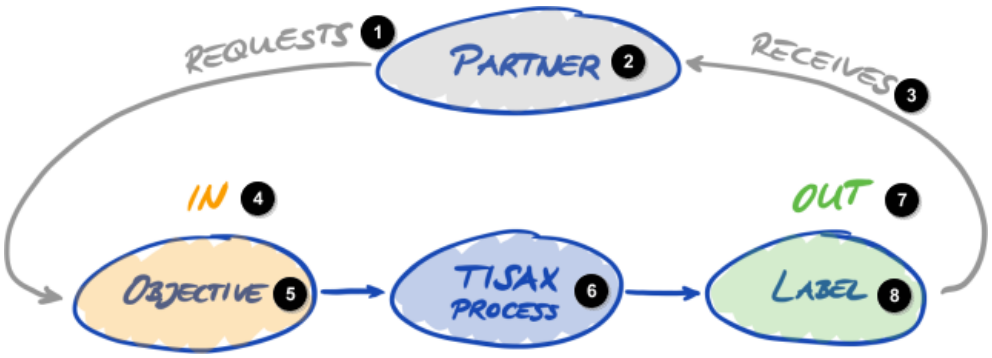


Figura 33. Obiettivi di valutazione ed etichette TISAX

1. Richiede
2. Partner
3. Riceve
4. A MONTE
5. Obiettivo
6. Processo TISAX
7. A VALLE
8. Etichetta

Le etichette TISAX:

- sono il risultato del processo di valutazione TISAX.
- riassumono il risultato della valutazione.
- sono la conferma che il sistema di gestione della sicurezza delle informazioni della vostra azienda soddisfa una serie di requisiti predefiniti.

L'uso delle etichette TISAX semplifica la comunicazione relativa a TISAX con il vostro partner e fornitore di audit TISAX, in quanto si riferiscono a un elemento specifico a valle del processo di valutazione TISAX.

5.4.14.1. Gerarchia delle etichette TISAX

La corrispondenza tra gli obiettivi di valutazione e le relative etichette TISAX è piuttosto semplice. C'è però un altro aspetto importante da tenere a mente: *alcune* etichette TISAX sono collegate in maniera gerarchica. Ciò significa che se alla vostra azienda viene assegnata una determinata etichetta TISAX, riceverete automaticamente le etichette TISAX "sottostanti" a essa.

Esempio: se il vostro obiettivo di valutazione era "Very high availability", riceverete la corrispondente etichetta TISAX "Very high availability". Tuttavia, poiché l'obiettivo di valutazione Very high availability è un sovrainsieme di "High availability", riceverete automaticamente anche l'etichetta TISAX "High availability".

Tale gerarchia attualmente vale per le seguenti etichette TISAX:

- "Info high" è un sovrainsieme di "Confidential" e "High availability".
- "Info very high" è un sovrainsieme di "Strictly confidential" e "Very high availability".
- "Strictly confidential" è un sovrainsieme di "Confidential"
- "Very high availability" è un sovrainsieme di "High availability"
- "Special data" è un sovrainsieme di "Data"

Attenzione:

È anche possibile ricevere le etichette TISAX retroattivamente. Quando introduciamo una nuova etichetta che è un sottoinsieme di una delle etichette TISAX che la vostra azienda ha già ricevuto, ricevete automaticamente la nuova etichetta.

Esempio: avete ottenuto l'etichetta TISAX "Info high" in un momento in cui l'etichetta "High availability" non esisteva ancora. Quando abbiamo introdotto l'etichetta High availability, il nostro sistema l'ha automaticamente assegnata alla vostra azienda.

Queste relazioni gerarchiche possono essere dedotte confrontando i requisiti applicabili specificati in Tabella 8, "Applicabilità dei requisiti agli obiettivi di valutazione".

Questo aspetto potrebbe sembrare poco importante per alcuni partecipanti. Immaginate però che un partner vi chieda di mostrare l'etichetta TISAX "Very high availability", mentre un altro vi chiede l'etichetta TISAX "High availability". In una situazione di questo tipo possedere entrambe le etichette TISAX semplifica le cose per tutti, perché non è necessario spiegare che "High availability" è un sovrainsieme di "Very high availability". Ciò è particolarmente importante per quei partner per i quali il possesso di determinate etichette TISAX fa parte di un processo di acquisto piuttosto rigoroso. In questo modo non dovete spiegare che "Very high availability" è "meglio" di "High availability": vi limiterete a mostrare tutte le vostre etichette TISAX e la persona che conduce la valutazione può semplicemente spuntare il requisito "deve possedere l'etichetta TISAX 'High availability'".

5.4.14.2. Periodo di validità delle etichette TISAX

Generalmente le etichette TISAX hanno una validità di tre anni. Il periodo di validità decorre a partire dalla fine del processo di valutazione (anche prima dell'emissione della relazione della valutazione TISAX).

Il periodo di validità può essere più breve se si verificano cambiamenti significativi in merito all'ambito di valutazione TISAX.

Esempi: cambio di sede della vostra azienda, nuove sedi. (Per istruzioni su cosa fare in tali casi, si veda Sezione 7.9.3.2, "Come richiedere la modifica di una sede" e Sezione 7.9.3.4, "Come aggiungere un'ulteriore sede".)

Attenzione:

Le etichette TISAX della vostra azienda sono consultabili solo nel portale ENX. Non vengono registrate nella relazione della valutazione TISAX.

5.4.14.3. Rinnovo delle etichette TISAX

Per mantenere le etichette TISAX nel lungo termine, è necessario rinnovarle[30] ogni tre anni.

Per farlo fondamentalmente è necessario ripetere il processo TISAX (registrare un ambito di valutazione, sottoporsi nuovamente alla valutazione TISAX, condividere il risultato della valutazione). La registrazione è un po' più semplice, in quanto non è necessario re-inserire la propria azienda come partecipante TISAX. Inoltre potete anche riutilizzare tutti i contatti e le sedi della vostra azienda già memorizzati nel database TISAX.

Nota importante:

Occorre registrare un NUOVO ambito PRIMA di contattare il fornitore di audit. Il fornitore di audit può avviare un nuovo processo di valutazione solo se siete in grado di fornire un nuovo ID Ambito.

Nella maggior parte dei casi registrare un nuovo ambito è un'operazione semplice: è sufficiente assegnare un nome al nuovo ambito, aggiungere i contatti, selezionare uno o più obiettivi di valutazione e aggiungere le sedi. È possibile riutilizzare i contatti e le sedi già presenti nel sistema provenienti da qualsiasi ambito registrato in precedenza.

Nota importante:

Vi chiediamo di riutilizzare i dati delle sedi esistenti che avete creato e usato durante la registrazione dell'ambito precedente. Non create nuovi dati di una sede con lo stesso indirizzo.

Il motivo è che alcuni partecipanti TISAX elaborano automaticamente i risultati delle valutazioni dei loro partner sincronizzando il proprio sistema con il portale ENX. Anche piccole differenze possono bloccare la sincronizzazione. Inoltre, è importante non intasare i dati dei partecipanti con inutili doppioni.

Nota importante:

Se avete come requisito il possesso costante di etichette TISAX valide durante la relazione con il vostro partner, vi consigliamo vivamente di inserire un promemoria nel vostro calendario per avviare il processo di rinnovo necessario.

Consigliamo di iniziare il rinnovo almeno un anno prima della scadenza delle etichette TISAX.

Ora che avete ricevuto le vostre etichette TISAX, potete procedere con l'ultima fase e condividerle con il vostro partner.

6. Scambio (fase 3)

Il tempo di lettura stimato per la sezione relativa allo scambio è di 7 minuti.

Avete completato il processo TISAX, ma il vostro partner non ha ancora ricevuto nessuna “prova” che il sistema di gestione della sicurezza delle informazioni della vostra azienda è in grado di proteggere i suoi dati riservati. Questa sezione descrive quindi come condividere il risultato della valutazione con il vostro partner e come presentare le prove richieste.

6.1. Premessa

Una delle caratteristiche principali di TISAX prevede che il risultato della valutazione sia completamente sotto il vostro controllo. Senza la vostra esplicita autorizzazione, tutte le informazioni relative alla valutazione della vostra azienda non vengono condivise con altri soggetti.

6.2. La piattaforma di scambio

La piattaforma di scambio viene fornita dal portale ENX.

Il vostro fornitore di audit caricherà le prime due sezioni (A e B) della vostra relazione della valutazione TISAX. In questa fase, le informazioni sono disponibili solo per voi.

Potete utilizzare l’account creato durante la registrazione per accedere al portale e usare la piattaforma di scambio.

È possibile accedere al portale dal seguente indirizzo:
enx.com/en-US/SignIn

6.3. Prerequisiti generali

Potete condividere il risultato della valutazione con il vostro partner solo se sono soddisfatti questi due prerequisiti:

1. Il vostro fornitore di audit ha inviato il risultato della valutazione alla piattaforma di scambio.
   Solitamente il risultato della valutazione è disponibile sulla piattaforma di scambio 5-10 giorni lavorativi dopo l’emissione della relazione della valutazione TISAX.
2. Abbiamo ricevuto il pagamento della tariffa prevista da parte vostra (se applicabile).

Lo stato dell’ambito di valutazione è “Attivo” quando entrambi i prerequisiti sono soddisfatti.

Attenzione:

> Ogni ambito di valutazione ha il proprio ciclo di vita. In questa fase il vostro ambito di valutazione deve avere lo stato “Attivo”.
>
> Per maggiori informazioni sullo stato di una valutazione, si veda Sezione 7.5.5, “Assessment scope status “Awaiting your payment” (Stato dell’ambito di valutazione “In attesa del pagamento”)”.

Per verificare se il risultato della valutazione è pronto per essere condiviso (stato dell’ambito di valutazione = Attivo), seguite questi passaggi:

1. Accedete al portale ENX.
2. Andate alla barra di navigazione principale e selezionate “MY TISAX” (“IL MIO TISAX”).
3. Dal menu a discesa, selezionate “SCOPES AND ASSESSMENTS” (“AMBITI E VALUTAZIONI”).
4. Andate alla tabella e cercate la riga con il vostro ambito di valutazione.
5. Verificate che l’ambito di valutazione abbia lo stato “Active” (“Attivo”) (colonna “Scope Status” (“Stato dell’ambito”)).

6.4. Permanenza dei risultati scambiati

> Nota importante:
>
> Non è possibile revocare le autorizzazioni di pubblicazione o condivisione.
>
> Il motivo è che vogliamo che tutti i partecipanti passivi possano contare su un accesso continuo a tutti i risultati delle valutazioni che hanno ricevuto, altrimenti dovrebbero gestire e archiviare i risultati delle valutazioni autonomamente.
>
> L’autorizzazione rimane valida per l’intero periodo di validità della valutazione TISAX.
>
> Se avete concesso un’autorizzazione di pubblicazione o condivisione per errore, contattateci immediatamente.

6.5. Livelli di condivisione

I livelli di condivisione corrispondono 1:1 alle sezioni principali A-E della relazione della valutazione TISAX.

	Sezioni principali della relazione della valutazione TISAX	Livelli di condivisione sulla piattaforma di scambio
1	A. Informazioni relative alla valutazione (Assessment Related Information)	
2	B. Risultati in sintesi (Summarized Results)	
3	C. Riassunto del risultato della valutazione (Assessment result summary)	
4	D. Livelli di maturità dell'ISA di VDA (scheda dei risultati) (Maturity Levels of VDA ISA (Result Tab))	
5	E. Risultati della valutazione in dettaglio (Detailed Assessment Results)	

Tabella 12. Sezioni principali della relazione della valutazione TISAX e livelli di condivisione sulla piattaforma di scambio

Più alto è il livello di condivisione, maggiori saranno i dettagli sulla valutazione TISAX accessibili ai rispettivi partecipanti.

Per maggiori dettagli sul contenuto di ogni sezione della relazione della valutazione TISAX, si veda Sezione 5.4.7.4, "Relazione della valutazione TISAX".

6.6. Pubblicazione del risultato della valutazione sulla piattaforma di scambio

È possibile condividere il risultato della valutazione con tutti gli altri partecipanti TISAX pubblicandolo sulla piattaforma di scambio. In questo modo tutti gli altri partecipanti TISAX possono accedere al risultato della valutazione fino al livello di condivisione concesso.

È possibile pubblicare il risultato della valutazione solo se il risultato complessivo della valutazione è "conforme".

I livelli di condivisione per la pubblicazione del risultato della valutazione sulla piattaforma di scambio sono limitati alle seguenti opzioni:

- Do not publish (Default) (Nessuna pubblicazione (impostazione predefinita))
- A. Assessment Related Information (A. Informazioni relative alla valutazione)
- A + Labels (A + Etichette)
- A + Labels + B. Summarized Results (A + Etichette + B. Risultati in sintesi)

Consigliamo il livello di condivisione "A + Labels" ("A + Etichette") come tipologia di pubblicazione generale.

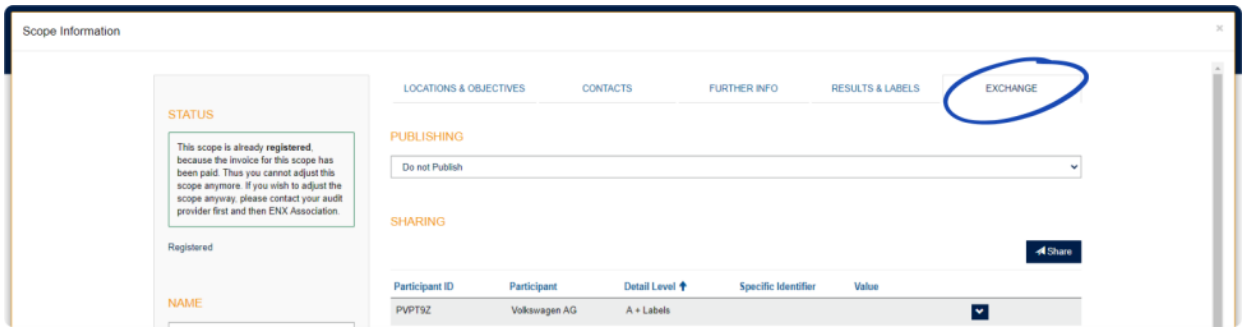
Nota importante:

È possibile pubblicare il risultato della valutazione solo se i prerequisiti

descritti in Sezione 6.3, “Prerequisiti generali” sono soddisfatti.

Per pubblicare il risultato della valutazione sulla piattaforma di scambio, seguite questi passaggi:

1. Accedete al portale ENX.
2. Andate alla barra di navigazione principale e selezionate “MY TISAX” (“IL MIO TISAX”).
3. Dal menu a discesa, selezionate “SCOPES AND ASSESSMENTS” (“AMBITI E VALUTAZIONI”).
4. Andate alla tabella e cercate la riga con il vostro ambito di valutazione.
5. Verificate che l’ambito di valutazione abbia lo stato “Active” (“Attivo”) (colonna “Scope Status” (“Stato dell’ambito”)).
6. Andate alla fine della riga della tabella corrispondente al vostro ambito di valutazione e fate clic sul pulsante con la freccia verso il basso .
7. Selezionate “Scope Information” (“Informazioni sull’ambito”).
8. Nella nuova finestra (“Scope Information” (“Informazioni sull’ambito”)), selezionate la scheda “EXCHANGE” (“SCAMBIO”).



9. Andate alla sezione “PUBLISHING” (“PUBBLICAZIONE”), aprite il menu a discesa e selezionate il livello di condivisione che preferite (si veda quanto consigliato sopra).

Attenzione:

I risultati della valutazione sono pubblicati solo sulla piattaforma di scambio e l’accesso è consentito solo agli altri partecipanti TISAX. Non è disponibile un elenco pubblico di tutti i partecipanti TISAX: sul sito web pubblico di TISAX è riportato solo il numero totale dei partecipanti TISAX.

6.7. Condivisione del risultato della valutazione con un partecipante specifico

Oltre all’opzione già citata che consente di pubblicare il risultato della valutazione TISAX sulla piattaforma di scambio, è possibile condividerlo in maniera selettiva con determinati

partecipanti TISAX con un livello di condivisione più elevato.

A differenza della pubblicazione di cui sopra, potete condividere il risultato della valutazione anche se il risultato complessivo della valutazione è non conforme (di livello grave/minore).

La condivisione dei risultati della valutazione è parte integrante di TISAX. Il sistema di gestione della sicurezza delle informazioni della vostra azienda viene valutato una sola volta, ma potete poi condividere il risultato della valutazione con tutti i partner che volete.

Le opzioni per condividere il risultato della valutazione sulla piattaforma di scambio sono:

1. A: Assessment Related Information (A: Informazioni relative alla valutazione)
2. A + Labels (A + Etichette)
3. A + Labels + B: Assessment Summary (A + Etichette + B: Riassunto della valutazione)
4. A + Labels + B + C: Summarized Results (A + Etichette + B + C: Risultati in sintesi)
5. A + Labels + B + C + D: Detailed Assessment Results (A + Etichette + B + C + D: Risultati della valutazione in dettaglio)
6. A + Labels + B + C + D + E: Maturity Levels according to ISA (A + Etichette + B + C + D + E: Livelli di maturità secondo l'ISA)

Consigliamo il livello di condivisione "A + Labels" ("A + Etichette") per la condivisione. Tale livello è sufficiente per la maggioranza dei partner, ma potete sempre selezionarne uno maggiore in un secondo momento.

Attenzione:

Alcuni partecipanti TISAX elaborano automaticamente i risultati delle valutazioni dei loro partner sincronizzando il proprio sistema con il portale ENX. Solo i risultati della valutazione condivisi specificamente con questo partecipante vengono sincronizzati. Una sola pubblicazione, come descritto in Sezione 6.6, "Pubblicazione del risultato della valutazione sulla piattaforma di scambio", non è riconosciuta.

BMW è un esempio di OEM che si avvalgono di TISAX. Se siete partner di BMW, assicuratevi di condividere (non solo pubblicare) il risultato della valutazione con BMW.

6.7.1. Prerequisiti

Di seguito sono indicati i prerequisiti per condividere il risultato della valutazione con il vostro partner (o qualsiasi altro partecipante TISAX):

- Potete condividere il risultato della valutazione TISAX solo con altri partecipanti TISAX.

- Il vostro partner deve essere un partecipante TISAX.
- Dovete conoscere l'ID Partecipante del vostro partner.[31]
- È necessario pagare la tariffa prevista (se applicabile).

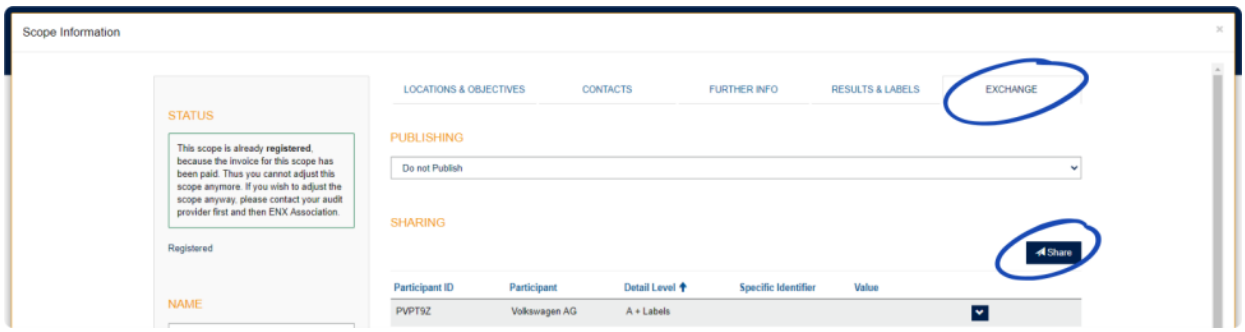
Nota importante:

È possibile condividere il risultato della valutazione solo se i prerequisiti generali descritti in Sezione 6.3, "Prerequisiti generali" sono soddisfatti.

6.7.2. Come creare un'autorizzazione di condivisione

Per condividere il risultato della valutazione con un altro partecipante TISAX, seguite questi passaggi:

1. Accedete al portale ENX.
2. Andate alla barra di navigazione principale e selezionate "MY TISAX" ("IL MIO TISAX").
3. Dal menu a discesa, selezionate "SCOPES AND ASSESSMENTS" ("AMBITI E VALUTAZIONI").
4. Andate alla tabella e cercate la riga con il vostro ambito di valutazione.
5. Verificate che l'ambito di valutazione abbia lo stato "Active" ("Attivo") (colonna "Scope Status" ("Stato dell'ambito")).
6. Andate alla fine della riga della tabella corrispondente al vostro ambito di valutazione e fate clic sul pulsante con la freccia verso il basso .
7. Selezionate "Scope Information" ("Informazioni sull'ambito").
8. Nella nuova finestra ("Scope Information" ("Informazioni sull'ambito")), selezionate la scheda "EXCHANGE" ("SCAMBIO").



9. Accedete alla sezione "SHARING" ("CONDIVISIONE") e fate clic sul pulsante "Share" ("Condividi").
10. Nella nuova finestra ("SHARE THIS SCOPE" ("CONDIVIDI QUESTO AMBITO")), inserite l'ID Partecipante del vostro partner (o selezionatelo dall'elenco dei partecipanti nella casella di ricerca adiacente).

11. Selezionate il livello di condivisione che preferite.
12. Fate clic sul pulsante “Next” (🇮🇹 “Avanti”).
13. Leggete attentamente le istruzioni relative alla durata dell’autorizzazione di condivisione.
14. Selezionate le due caselle di spunta “confirm” (🇮🇹 “conferma”).
15. Fate clic sul pulsante “Submit” (🇮🇹 “Invia”).

La piattaforma di scambio si occuperà di tutto il resto. Nel caso dei livelli di condivisione A e B, le informazioni sono disponibili nella piattaforma di scambio. Il vostro partner potrà quindi accedere al portale ENX e visualizzare il risultato della valutazione che avete condiviso[32].

Nel caso di livelli di condivisione più elevati (C-E), la piattaforma di scambio informa il vostro fornitore di audit, il quale invierà le informazioni (corrispondenti al livello di condivisione selezionato) al contatto principale del vostro partner partecipante.

6.8. Condivisione del risultato della valutazione al di fuori di TISAX

La regola[33] prevede che si possa usare la piattaforma di scambio TISAX per comunicare il proprio risultato della valutazione solo ad altri partecipanti TISAX.

6.8.1. Motivi alla base della rigorosa regolamentazione del meccanismo di scambio

TISAX offre un meccanismo di scambio standardizzato per i risultati della valutazione. Ciò rappresenta un valore aggiunto rispetto allo scambio dei risultati di altre certificazioni (ad esempio l’ISO), che avviene in vari modi e non sempre contiene tutte le informazioni necessarie per fornire un quadro completo.

Gli OEM, in particolare, apprezzano questa standardizzazione. Tuttavia anche altre aziende traggono vantaggio da procedure chiaramente definite.

6.8.2. Istruzioni su come pubblicare le informazioni sul processo TISAX

Sebbene non sia possibile mettere per iscritto pubblicamente il risultato della valutazione, potete comunque menzionare il lavoro fatto dalla vostra azienda nell’ambito di TISAX. Sul portale ENX forniamo consigli su come gestire le dichiarazioni pubbliche. Mettiamo inoltre a disposizione i loghi di TISAX che potete utilizzare.

Dopo aver effettuato l’accesso al portale ENX, le informazioni sono disponibili al seguente indirizzo:
🇬🇧 enx.com/en-US/myenxportal/marketing/
Download diretto della cartella ZIP (documenti e loghi):
🇬🇧 enx.com/en-US/myenxportal/marketing/TISAX-Trademark-and-Logos-Terms-and-

Conditions.zip

Se vi state chiedendo se è disponibile un certificato da poter appendere alla parete, ecco la risposta:
Visto il processo di scambio standardizzato menzionato sopra, non mettiamo a disposizione alcun certificato di questo tipo.

6.8.3. Condivisione con un partner che non è ancora un partecipante TISAX

Se volete condividere il risultato della valutazione TISAX con un partner specifico che a) non è ancora un partecipante TISAX e b) non ha ancora ricevuto etichette TISAX (attraverso il completamento del processo di valutazione), potete seguire questi passaggi:

1. Invitate il vostro partner a registrarsi come partecipante TISAX.
   È sufficiente che si registri come partecipante TISAX, non è necessario che proceda con la registrazione dell'ambito di valutazione.
2. Invitate il vostro partner a contattarci.
   Normalmente elaboriamo una nuova registrazione solo se l'azienda in questione registra anche un ambito di valutazione. Su richiesta del vostro partner, elaboreremo comunque la sua registrazione ed egli diventerà un partecipante TISAX. In questo modo potrà quindi ricevere il vostro risultato della valutazione TISAX attraverso il normale processo di scambio.

Lo scopo di questo approccio è assicurarci che il vostro partner accetti le "Condizioni generali di partecipazione a TISAX" che regolano lo scambio dei risultati delle valutazioni TISAX.

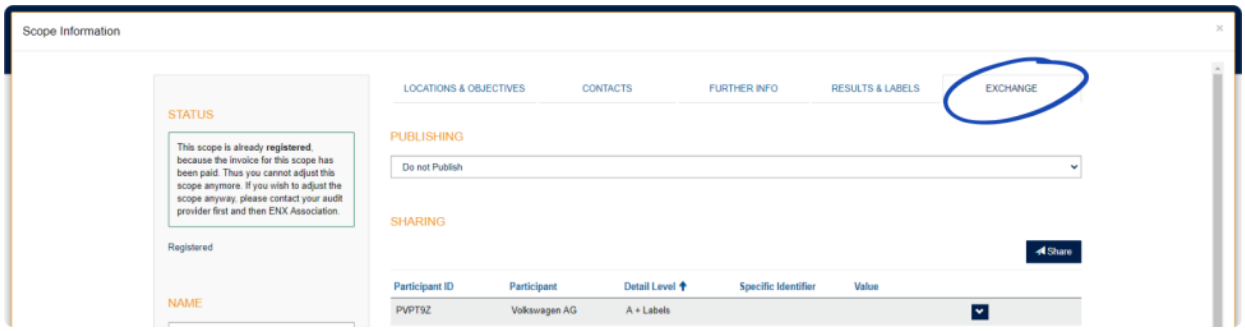
Solo la registrazione di un ambito di valutazione è a pagamento. Dal momento che la registrazione come partecipante TISAX è gratuita, il vostro partner riceverà il risultato della valutazione senza alcun costo. Tuttavia, in mancanza di un proprio risultato della valutazione, il vostro partner può ricevere un massimo di cinque risultati e non può vedere nessuna pubblicazione.

6.8.4. Condivisione con i dipendenti del vostro partner che non hanno accesso diretto al portale ENX

Solo i dipendenti del vostro partner che possiedono un account per il portale ENX possono vedere direttamente il risultato della vostra azienda. Se avete bisogno di dimostrare le vostre etichette TISAX a un dipendente del vostro partner che non ha accesso al portale, potete usare un apposito documento PDF. Per ottenere tale documento, seguite questi passaggi:

1. Condividete il risultato della valutazione con il partner in questione come descritto in Sezione 6.7, "Condivisione del risultato della valutazione con un partecipante specifico".
2. Accedete al portale ENX.
3. Andate alla barra di navigazione principale e selezionate "MY TISAX" ("IL MIO TISAX").

4. Dal menu a discesa, selezionate “SCOPES AND ASSESSMENTS” (🇮🇹 “AMBITI E VALUTAZIONI”).
5. Andate alla tabella e cercate la riga con il vostro ambito di valutazione.
6. Verificate che l’ambito di valutazione abbia lo stato “Active” (🇮🇹 “Attivo”) (colonna “Scope Status” (🇮🇹 “Stato dell’ambito”)).
7. Andate alla fine della riga della tabella corrispondente al vostro ambito di valutazione e fate clic sul pulsante con la freccia verso il basso .
8. Selezionate “Scope Information” (🇮🇹 “Informazioni sull’ambito”).
9. Nella nuova finestra (“Scope Information” (🇮🇹 “Informazioni sull’ambito”)), selezionate la scheda “EXCHANGE” (🇮🇹 “SCAMBIO”).



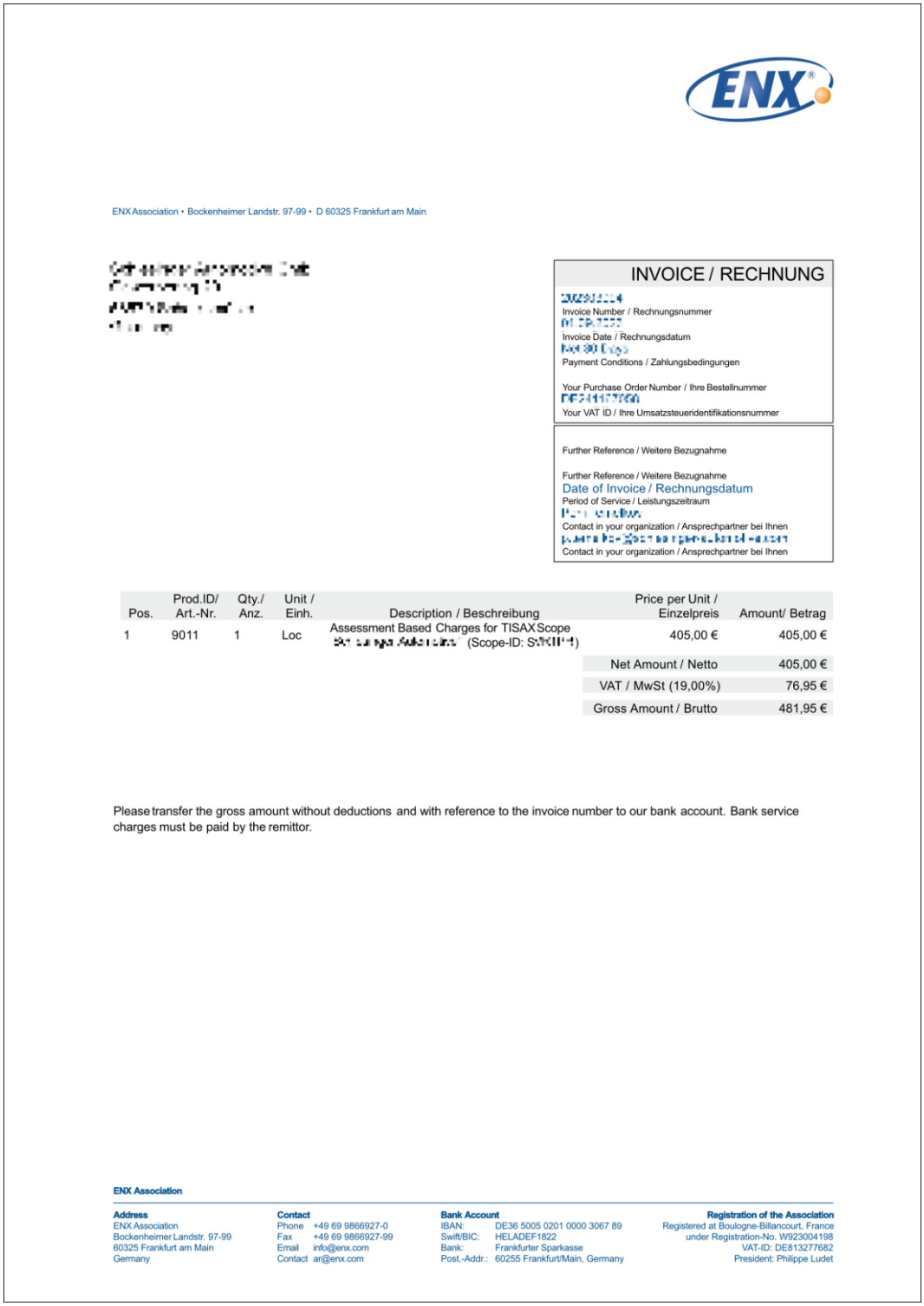
10. Accedete alla sezione “SHARING” (🇮🇹 “CONDIVISIONE”) e cercate la riga della tabella con l’autorizzazione di condivisione (creata al passaggio 1).
11. Andate alla fine della riga della tabella corrispondente all’autorizzazione di condivisione e fate clic sul pulsante con la freccia verso il basso .
12. Selezionate “Edit” (🇮🇹 “Modifica”)
13. Nella nuova finestra (“SHARE THIS SCOPE” (🇮🇹 “CONDIVIDI QUESTO AMBITO”)), scorrete verso il basso e selezionate “Request Shared Information as PDF” (🇮🇹 “Richiedi informazioni condivise come PDF”).
14. Attendete alcuni istanti fino a quando il documento non viene generato.
15. Scaricate il documento (“Copy of information shared with ACME.pdf (66.84 KB)” (🇮🇹 “Copia delle informazioni condivise con ACME.pdf (66,84 KB)”))

7. Allegati

7.1. Allegato: Esempio di fattura

Di seguito è riportato un esempio delle nostre fatture.

Per maggiori informazioni, si veda Sezione 4.3.4, “Tariffa”.



ENX Association • Bockenheimer Landstr. 97-99 • D 60325 Frankfurt am Main

[redacted]

INVOICE / RECHNUNG

[redacted]
Invoice Number / Rechnungsnummer
[redacted]
Invoice Date / Rechnungsdatum
[redacted]
Payment Conditions / Zahlungsbedingungen

Your Purchase Order Number / Ihre Bestellnummer
[redacted]
Your VAT ID / Ihre Umsatzsteueridentifikationsnummer

Further Reference / Weitere Bezugnahme

Further Reference / Weitere Bezugnahme
Date of Invoice / Rechnungsdatum
Period of Service / Leistungszeitraum
[redacted]
Contact in your organization / Ansprechpartner bei Ihnen
[redacted]
Contact in your organization / Ansprechpartner bei Ihnen

Pos.	Prod.ID/ Art.-Nr.	Qty./ Anz.	Unit / Einh.	Description / Beschreibung	Price per Unit / Einzelpreis	Amount/ Betrag
1	9011	1	Loc	Assessment Based Charges for TISAX Scope [redacted] (Scope-ID: [redacted])	405,00 €	405,00 €
					Net Amount / Netto	405,00 €
					VAT / MwSt (19,00%)	76,95 €
					Gross Amount / Brutto	481,95 €

Please transfer the gross amount without deductions and with reference to the invoice number to our bank account. Bank service charges must be paid by the remittor.

ENX Association

Address	Contact	Bank Account	Registration of the Association
ENX Association Bockenheimer Landstr. 97-99 60325 Frankfurt am Main Germany	Phone +49 69 9866927-0 Fax +49 69 9866927-99 Email info@enx.com Contact ar@enx.com	IBAN: DE36 5005 0201 0000 3067 89 Swift/BIC: HELADEF1822 Bank: Frankfurter Sparkasse Post.-Addr.: 60255 Frankfurt/Main, Germany	Registered at Boulogne-Billancourt, France under Registration-No. W923004198 VAT-ID: DE813277682 President: Philippe Ludet

7.2. Allegato: Esempio di e-mail di conferma

L’e-mail di conferma viene inviata dopo che avrete completato tutti i passaggi obbligatori della procedura di registrazione online.

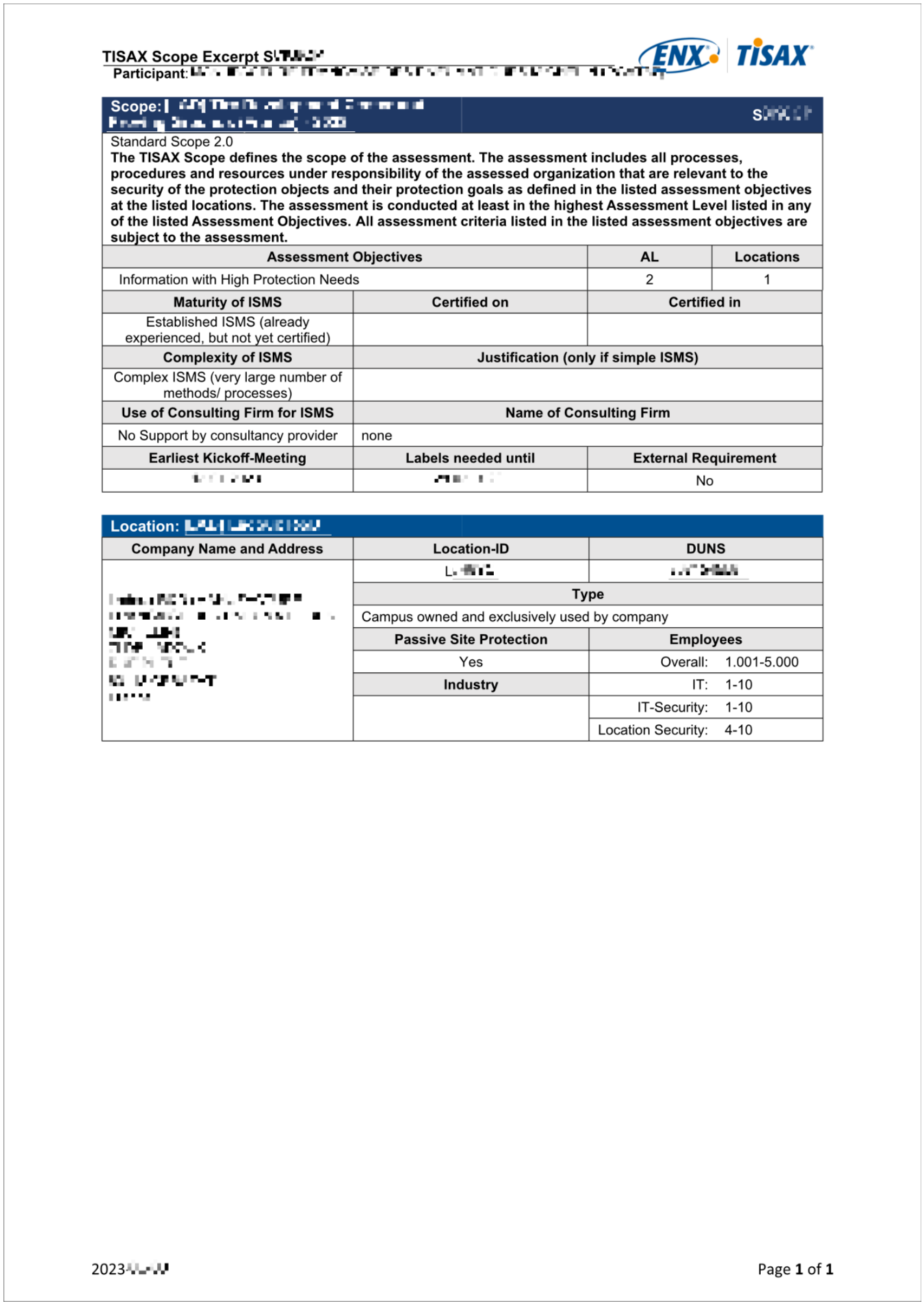
Per maggiori informazioni su quando inviamo questa e-mail di conferma, si veda Sezione 4.5.8, “E-mail di conferma”.

```
Oggetto: [TISAX] Ambito S3ZY5V approvato

Gentile John Doe,

la ringraziamo per aver registrato l□ambito di valutazione TISAX. Le confermiamo
che l□ambito è stato registrato e approvato. In allegato trova l□estratto
dell□ambito TISAX contenente tutte le informazioni sull□ambito e l□elenco attuale
dei fornitori di audit TISAX.

Qual è il prossimo passaggio?

Con l□estratto dell□ambito TISAX allegato ora può richiedere preventivi a tutti i
fornitori di audit TISAX per il suo ambito.

Ha bisogno di aiuto?

Nel caso in cui abbia altre domande su TISAX, la invitiamo a leggere le FAQ di
TISAX o il Manuale per i partecipanti TISAX. Se necessita di ulteriore supporto per
quanto riguarda TISAX, non esiti a contattare il servizio di assistenza TISAX
tramite e-mail (tisax@enx.com) o telefono (+49 69 986692-777).

Cordiali saluti,

Il Team TISAX
```

7.3. Allegato: Esempio dell’Estratto dell’ambito TISAX

Il “TISAX Scope Excerpt” (“Estratto dell’ambito TISAX”) è allegato all’e-mail di conferma.

Per maggiori informazioni, si veda Sezione 4.5.8, “E-mail di conferma”.



TISAX Scope Excerpt [illegible]
Participant: [illegible]

Scope: [illegible]

Standard Scope 2.0

The TISAX Scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations. The assessment is conducted at least in the highest Assessment Level listed in any of the listed Assessment Objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.

Assessment Objectives	AL	Locations
Information with High Protection Needs	2	1

Maturity of ISMS	Certified on	Certified in
Established ISMS (already experienced, but not yet certified)		

Complexity of ISMS	Justification (only if simple ISMS)
Complex ISMS (very large number of methods/ processes)	

Use of Consulting Firm for ISMS	Name of Consulting Firm
No Support by consultancy provider	none

Earliest Kickoff-Meeting	Labels needed until	External Requirement
[illegible]	[illegible]	No

Location: [illegible]

Company Name and Address	Location-ID	DUNS
[illegible]	[illegible]	[illegible]
	Type	
	Campus owned and exclusively used by company	
	Passive Site Protection	**Employees**
	Yes	Overall: 1.001-5.000
	Industry	IT: 1-10
		IT-Security: 1-10
		Location Security: 4-10

2023[illegible]

Page **1** of **1**

7.4. Allegato: Participant status (Stato del partecipante)

7.4.1. Panoramica: Participant status (Stato del partecipante)

Lo “stato del partecipante” indica l’avanzamento della vostra azienda nel processo TISAX.

Lo “stato del partecipante” può essere:

1. Incomplete (Incompleto)
2. Awaiting approval (In attesa di approvazione)
3. Preliminary (Preliminare)
4. Registered (Registrato)
5. Expired (Scaduto)

Le tabelle presenti nelle sezioni riportate qui sotto relative a ciascuno stato descrivono quanto segue:

- La situazione della vostra azienda
  (la situazione corrente quando ci si trova nello stato in questione)
- Il vostro passo successivo
  (cosa dovete fare per passare allo stato successivo, se applicabile)
- Il nostro passo successivo
  (cosa dobbiamo fare per far progredire il vostro stato, se applicabile)
- Lo stato successivo
  (se applicabile)

L’illustrazione seguente mostra le azioni che consentono di passare da uno stato a quello successivo:

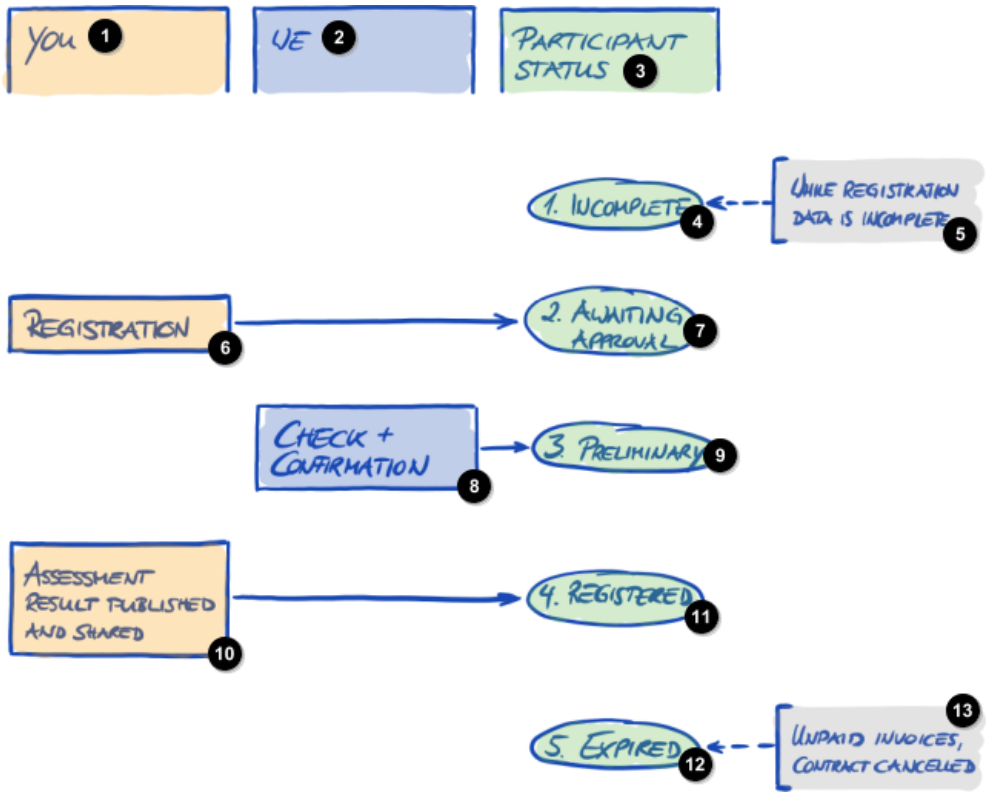


Figura 34. Panoramica sugli stati del partecipante

1. La vostra azienda
2. Noi
3. Stato del partecipante
4. 1. Incompleto
5. Fino a completamento dei dati di registrazione
6. Registrazione
7. 2. In attesa di approvazione
8. Verifica + conferma
9. 3. Preliminare
10. Risultato della valutazione pubblicato e condiviso
11. 4. Registrato
12. 5. Scaduto
13. Fatture insolute, contratto risolto

7.4.2. Participant status “Incomplete” (Stato del partecipante “Incompleto”)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
Incompleto	La registrazione a TISAX non è completa. Il motivo può essere che non avete accettato le condizioni generali. Oppure non avete specificato la sede principale del partecipante. Oppure non avete assegnato un contatto principale del partecipante. Oppure non avete inserito altre informazioni obbligatorie.	Proseguite all’indirizzo enx.com/en-US/SignIn	Vi invieremo un promemoria tramite e-mail (di solito entro pochi giorni).	In attesa di approvazione

7.4.3. Participant status “Awaiting approval” (Stato del partecipante “In attesa di approvazione”)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
In attesa di approvazione	La registrazione a TISAX è completa. Potreste aver già registrato un ambito di valutazione oppure non ancora.	Aspettate il passo successivo da parte nostra.	Verificheremo e generalmente approveremo la vostra domanda. Tuttavia, solitamente la verifica viene attivata anche registrando un ambito di valutazione. Assegneremo un ID Partecipante e l’ID (o gli ID) Ambito. Vi invieremo un’e-mail di conferma. Il “TISAX Scope Excerpt” (“Estratto dell’ambito TISAX”) in PDF allegato riassume le informazioni contenute nel nostro database.	Preliminare

7.4.4. Participant status “Preliminary” (Stato del partecipante “Preliminare”)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
Preliminare	Avete completato con successo il processo di registrazione a TISAX.	Provvedete a pagare la tariffa (se applicabile). Completate il processo di valutazione TISAX. Pubblicate e condividete il risultato della valutazione.	Nessuna	Registrato

7.4.5. Participant status “Registered” (Stato del partecipante “Registrato”)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
Registrato	Avete completato con successo il processo di valutazione TISAX e avete ricevuto le etichette TISAX. Avete pubblicato e condiviso il risultato della valutazione. Riceverete le etichette TISAX solo dopo aver superato con successo il processo di valutazione TISAX. Sul portale ENX, ciò si traduce nello stato dell’ambito di valutazione “Attivo”.	Nessuna	Nessuna	(Scaduto)

Attenzione:

Se volete accedere ai risultati della valutazione del/i vostro/i partner:

Per poter ricevere i risultati delle valutazioni di altri partecipanti è necessario uno dei seguenti prerequisiti teorici:

- La vostra azienda condivide il risultato della propria valutazione (in questo modo la vostra azienda “dimostra” di essere un partecipante TISAX serio e un membro del settore automotive).
- Confermiamo la vostra azienda sulla base della sua reputazione nel settore automotive (ad esempio OEM, fornitori di primo livello).
- La vostra azienda dimostra di avere un legittimo interesse nel ricevimento

dei risultati delle valutazioni da parte degli altri partecipanti. Ciò deve essere verificato da parte nostra durante un processo complesso per il quale può essere prevista una tariffa considerevole. Per ulteriori dettagli, contattateci.

7.4.6. Participant status “Expired” (Stato del partecipante “Scaduto”)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
Scaduto	Non avete provveduto a pagare la tariffa prevista. Oppure il contratto (le CG) è stato risolto dalla vostra azienda o da noi.	Nessuna	Nessuna	N/A

7.5. Allegato: Assessment scope status (Stato dell’ambito di valutazione)

7.5.1. Panoramica: Assessment scope status (Stato dell’ambito di valutazione)

Lo “stato dell’ambito di valutazione” definisce in che punto del suo ciclo di vita si trova il vostro ambito di valutazione.

Tenete presente che lo “stato dell’ambito di valutazione” è diverso dallo “stato della valutazione”. Per maggiori informazioni sullo “stato della valutazione”, si veda Sezione 7.6, “Allegato: Assessment status (Stato della valutazione)”.

Lo “stato dell’ambito di valutazione” della vostra azienda può essere:

1. Incomplete (Incompleto)
2. Awaiting your order (In attesa dell’ordine)
3. Awaiting ENX approval (In attesa dell’approvazione di ENX)
4. Awaiting your payment (In attesa del pagamento)
5. Registered (Registrato)
6. Active (Attivo)
7. Expired (Scaduto)

Le tabelle presenti nelle sezioni riportate qui sotto relative a ciascuno stato descrivono quanto segue:

- La situazione della vostra azienda
  (la situazione corrente quando ci si trova nello stato in questione)
- Il vostro passo successivo
  (cosa dovete fare per passare allo stato successivo, se applicabile)
- Il nostro passo successivo
  (cosa dobbiamo fare per far progredire il vostro stato, se applicabile)
- Lo stato successivo
  (se applicabile)

L'illustrazione seguente mostra le azioni che consentono di passare da uno stato a quello successivo:

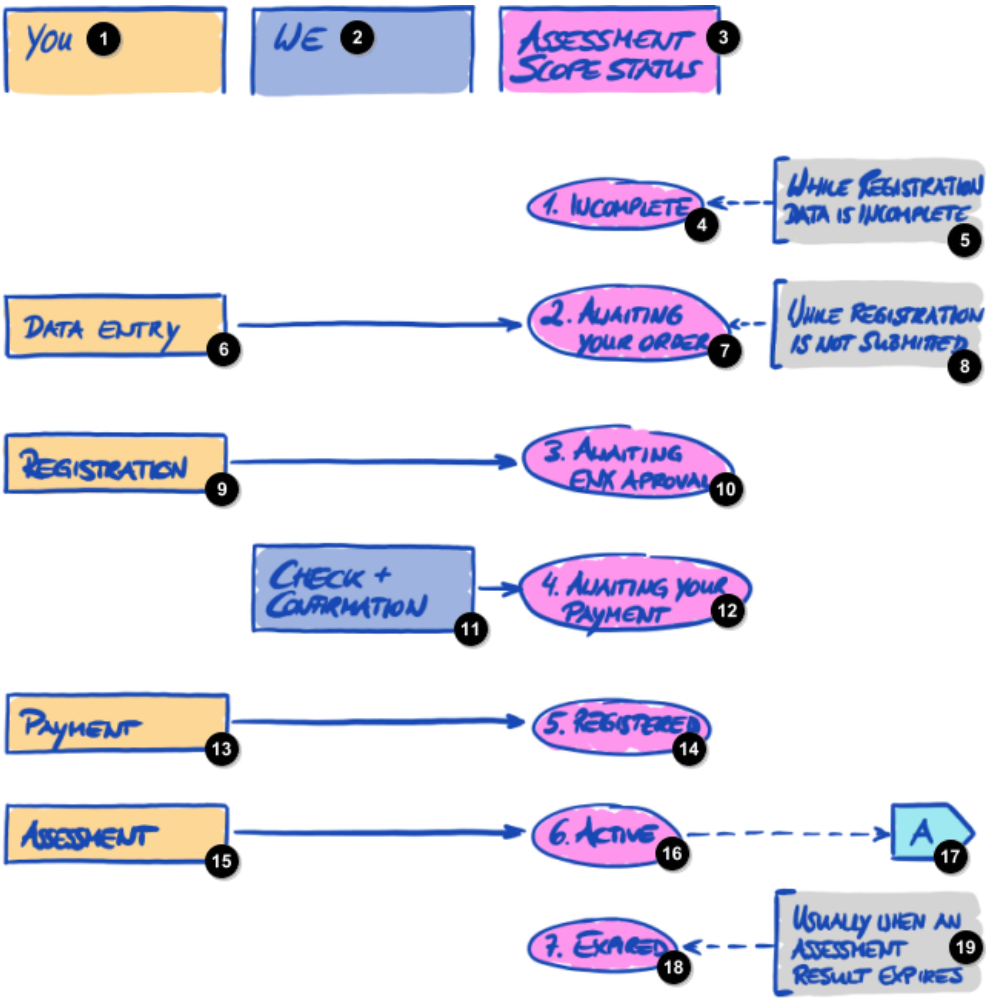


Figura 35. Panoramica dello stato dell'ambito di valutazione

1 La vostra azienda

2. Noi
3. Stato dell’ambito di valutazione
4. 1. Incompleto
5. Fino a completamento dei dati di registrazione
6. Inserimento dei dati
7. 2. In attesa dell’ordine
8. Fino a invio della registrazione
9. Registrazione
10. 3. In attesa dell’approvazione di ENX
11. Verifica + conferma
12. 4. In attesa del pagamento
13. Pagamento
14. 5. Registrato
15. Valutazione
16. 6. Attivo
17. A
18. 7. Scaduto
19. Solitamente quando scade il risultato della valutazione

Il riferimento esterno “A” nella figura riportata sopra collega lo stato dell’ambito di valutazione “Attivo” con lo “stato della valutazione”. Per maggiori informazioni sullo “stato della valutazione”, si veda Sezione 7.6, “Allegato: Assessment status (Stato della valutazione)”.

7.5.2. Assessment scope status “Incomplete” (Stato dell’ambito di valutazione “Incompleto”)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
Incompleto	Non avete completato la registrazione dell'ambito di valutazione. Oppure non avete inserito tutte le informazioni obbligatorie.	Proseguite all'indirizzo enx.com/en-US/SignIn	Vi invieremo un promemoria tramite e-mail (di solito entro pochi giorni).	In attesa dell'ordine

Per maggiori informazioni su dove questo stato svolga un ruolo, si veda Sezione 4.5.7, "Registrazione dell'ambito di valutazione".

7.5.3. Assessment scope status "Awaiting your order" (Stato dell'ambito di valutazione "In attesa dell'ordine")

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
In attesa dell'ordine	La registrazione dell'ambito non è stata completata.	Proseguite all'indirizzo enx.com/en-US/SignIn	Vi invieremo un promemoria tramite e-mail (di solito entro pochi giorni).	In attesa dell'approvazione di ENX

Per maggiori informazioni su dove questo stato svolga un ruolo, si veda Sezione 4.5.7, "Registrazione dell'ambito di valutazione".

7.5.4. Assessment scope status "Awaiting ENX approval" (Stato dell'ambito di valutazione "In attesa dell'approvazione di ENX")

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
In attesa dell'approvazione di ENX	La registrazione dell'ambito di valutazione è completa.	Aspettate il passo successivo da parte nostra.	Verificheremo e generalmente approveremo la vostra domanda. Assegneremo l'ID (o gli ID) Ambito. Vi invieremo un'e-mail di conferma. Il "TISAX Scope Excerpt" ("Estratto dell'ambito TISAX") in PDF allegato riassume le informazioni contenute nel nostro database.	In attesa del pagamento

Per maggiori informazioni su dove questo stato svolga un ruolo, si veda Sezione 4.5.7, "Registrazione dell'ambito di valutazione".

7.5.5. Assessment scope status “Awaiting your payment” (Stato dell’ambito di valutazione “In attesa del pagamento”)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
In attesa del pagamento	La registrazione dell’ambito di valutazione è completa e approvata. Avete ricevuto la nostra e-mail di conferma e il “TISAX Scope Excerpt” (“Estratto dell’ambito TISAX”).	Provvedete a pagare la tariffa (se applicabile). Richiedete offerte ai nostri fornitori di audit TISAX. Dallo stato “In attesa del pagamento” in poi potete: ▪ cominciare a condividere con il vostro partner alcune informazioni relative alla valutazione. [34] ▪ Pre-configurare la pubblicazione del risultato della valutazione (che diventerà effettiva solo quando il vostro stato dell’ambito di valutazione diventa “Attivo”).	Attendiamo il pagamento da parte vostra.	Registrato

Per maggiori informazioni su dove questo stato svolga un ruolo, si veda Sezione 4.5.8, “E-mail di conferma”.

7.5.6. Assessment scope status “Registered” (Stato dell’ambito di valutazione “Registrato”)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
Registrato	Il vostro ambito di valutazione è registrato. Abbiamo ricevuto il vostro pagamento completo o il vostro stato commerciale è di colore “verde” per via di altre circostanze.	Completate il processo di valutazione TISAX.	Nessuna	Attivo

7.5.7. Assessment scope status “Active” (Stato dell’ambito di valutazione “Attivo”)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
Attivo	Avete completato con successo il processo di valutazione TISAX e avete ricevuto le etichette TISAX.	Pubblicate e condividete il risultato della valutazione. Tutte le pubblicazioni e autorizzazioni di condivisione pre-configurate in uno stato inferiore ora assumono efficacia.	Nessuna	Scaduto

Per maggiori informazioni sulla pubblicazione e la condivisione, si veda Sezione 6, “Scambio (fase 3)”.

7.5.8. Assessment scope status “Expired” (Stato dell’ambito di valutazione “Scaduto”)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
Scaduto	Si è verificata una delle seguenti situazioni: ▪ non avete completato la registrazione dell’ambito di valutazione entro 90 giorni,	Avviate una nuova registrazione dell’ambito di valutazione .	Nessuna	Incompleto o In attesa dell’ordine o In attesa dell’approvazione di ENX
	• si è verificato un ritardo ingiustificato con il pagamento della tariffa da parte vostra,			
	• avete abbandonato il processo TISAX,			
	• la validità del risultato della vostra valutazione è scaduta (tre anni),			

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
	• avete apportato modifiche sostanziali all'ambito di valutazione (esempio: nessuna delle sedi di un ambito di valutazione fa più parte della vostra azienda).			

7.6. Allegato: Assessment status (Stato della valutazione)

7.6.1. Panoramica: Assessment status (Stato della valutazione)

Lo "stato della valutazione" indica l'avanzamento della vostra azienda nel processo di valutazione. Lo stato cambia man mano che si passa da una tipologia di valutazione all'altra (ad esempio da "valutazione iniziale" a "valutazione del piano d'azione correttivo").

Tenete presente che lo "stato della valutazione" è diverso dallo "stato dell'ambito di valutazione". Per maggiori informazioni sullo "stato dell'ambito di valutazione", si veda Sezione 7.5, "Allegato: Assessment scope status (Stato dell'ambito di valutazione)".

Lo "stato della valutazione" della vostra azienda può essere:

1. Initial assessment ordered (Valutazione iniziale richiesta)
2. Initial assessment ongoing (Valutazione iniziale in corso)
3. Waiting for corrective action plan assessment (In attesa della valutazione del piano d'azione correttivo)
4. Waiting for follow-up (In attesa del follow-up)
5. Finished (Terminata)

Le tabelle presenti nelle sezioni riportate qui sotto relative a ciascuno stato descrivono quanto segue:

- La situazione della vostra azienda
  (la situazione corrente quando ci si trova nello stato in questione)
- Il vostro passo successivo
  (cosa dovete fare per passare allo stato successivo, se applicabile)
- Il nostro passo successivo
  (cosa dobbiamo fare per far progredire il vostro stato, se applicabile)
- Lo stato successivo
  (se applicabile)

L'illustrazione seguente mostra le azioni che consentono di passare da uno stato a quello successivo:

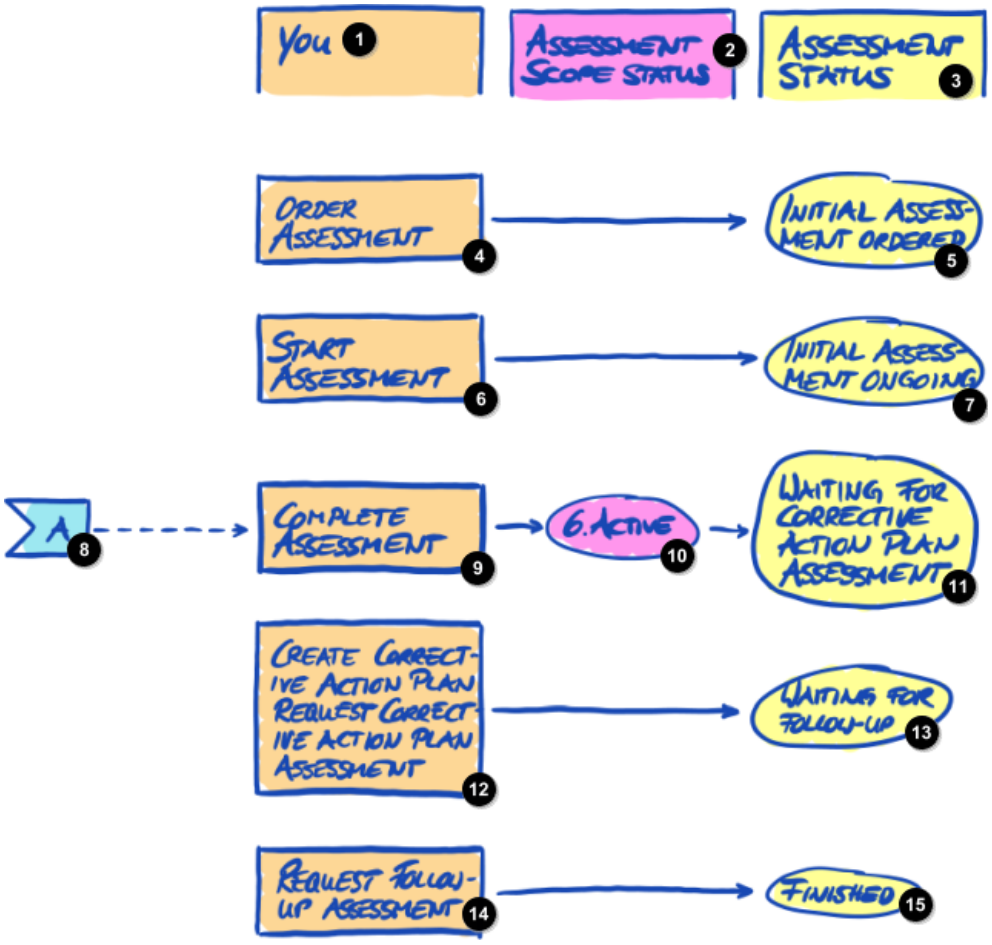


Figura 36. Panoramica dello stato della valutazione

1. La vostra azienda
2. Stato dell'ambito di valutazione
3. Stato della valutazione
4. Richiedere valutazione

5. Valutazione iniziale richiesta
6. Iniziare valutazione
7. Valutazione iniziale in corso
8. A
9. Completare valutazione
10. 6. Attivo
11. In attesa della valutazione del piano d'azione correttivo
12. Creare piano d'azione correttivo
    Richiedere valutazione del piano d'azione correttivo
13. In attesa del follow-up
14. Richiedere valutazione di follow-up
15. Terminata

Il riferimento esterno "A" nella figura riportata sopra collega lo stato dell'ambito di valutazione "Attivo" con lo stato della valutazione "In attesa della valutazione del piano d'azione correttivo". Per maggiori informazioni sullo "stato dell'ambito di valutazione", si veda Sezione 7.5, "Allegato: Assessment scope status (Stato dell'ambito di valutazione)".

7.6.2. Assessment status "Initial assessment ordered" (Stato della valutazione "Valutazione iniziale richiesta")

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
Valutazione iniziale richiesta	Avete selezionato uno dei nostri fornitori di audit TISAX e richiesto una valutazione iniziale.	Proseguite con il processo di valutazione TISAX.	Nessuna	Valutazione iniziale in corso

7.6.3. Assessment status "Initial assessment ongoing" (Stato della valutazione "Valutazione iniziale in corso")

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
Valutazione iniziale in corso	La valutazione iniziale della vostra azienda: ▪ è stata avviata ▪ o è stata completata, ma il vostro fornitore di audit non ha ancora inviato la relazione della valutazione TISAX.	Nessuna	Nessuna	In attesa della valutazione del piano d'azione correttivo (se applicabile)

7.6.4. Assessment status "Waiting for corrective action plan assessment" (Stato della valutazione "In attesa della valutazione del piano d'azione correttivo)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
In attesa della valutazione del piano d'azione correttivo	Il vostro fornitore di audit ha condotto una valutazione iniziale. Il vostro fornitore di audit ci ha inviato la relazione della valutazione TISAX. Il risultato della valutazione è non conforme (di livello grave/minore).	Create un piano d'azione correttivo. Mettete in atto le azioni correttive. Richiedete una valutazione del piano d'azione correttivo.	Nessuna	In attesa del follow-up (se applicabile)

Lo stato della valutazione “In attesa della valutazione del piano d’azione correttivo” ha una durata massima di nove mesi. Per maggiori informazioni, si veda Sezione 5.4.9.3, “Requisiti del piano d’azione correttivo”.

7.6.5. Assessment status “Waiting for follow-up” (Stato della valutazione “In attesa del follow-up”)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
In attesa del follow-up	Il vostro fornitore di audit ha approvato il piano d’azione correttivo della vostra azienda. Avete implementato le azioni correttive.	Richiedete una valutazione di follow-up.	Nessuna	Terminata

Lo stato della valutazione “In attesa del follow-up” ha una durata massima di nove mesi. Per maggiori informazioni, si veda Sezione 5.4.9.3, “Requisiti del piano d’azione correttivo”.

7.6.6. Assessment status “Finished” (Stato della valutazione “Terminata”)

Stato	Situazione	Il vostro passo successivo	Il nostro passo successivo	Lo stato successivo
Terminata	Il vostro fornitore di audit ha condotto una valutazione di follow-up. Il risultato della valutazione non presenta alcuna non conformità. Il vostro fornitore di audit ci ha inviato la relazione della valutazione TISAX.	Pubblicate e condividete il risultato della valutazione.	Nessuna	N/A

7.7. Allegato: Motivazioni a sfavore delle “valutazioni preliminari” e delle “analisi dei divari”

Generalmente si sconsiglia di richiedere a un fornitore di audit di condurre una “valutazione preliminare” o una “analisi dei divari”. Nella maggior parte dei casi ha più senso cominciare subito il processo di valutazione TISAX.

In questa sezione parleremo delle preoccupazioni più comuni.

Avete preso in considerazione una valutazione preliminare perché:

1. Siete preoccupati che il vostro cliente possa vedere un risultato della valutazione potenzialmente sfavorevole?

   Avete il pieno controllo su chi può vedere i risultati della vostra valutazione. Spetta a voi decidere se il fornitore di audit può caricare qualsiasi informazione sul portale ENX. Se non volete farle vedere a nessuno, nessuno le vedrà (tranne l’auditor, ovviamente).

   Inoltre, il fornitore di audit carica sempre solo le prime due sezioni della relazione della valutazione TISAX e in ogni caso non carica *mai* i risultati della valutazione in dettaglio.

2. Pensate che una valutazione preliminare possa farvi risparmiare denaro?
   - Nel caso di una valutazione preliminare:
     - dovrete provvedere al pagamento della valutazione preliminare
     - potreste incorrere in costi interni per la risoluzione di eventuali non conformità
     - dovrete provvedere al pagamento della valutazione TISAX completa (“valutazione iniziale”)

     Anche nel caso in cui *non* emergano rilievi, dovrete comunque pagare *due* valutazioni complete.

   - Se iniziate con una valutazione TISAX:
     - dovrete provvedere al pagamento della “valutazione iniziale”
     - potreste incorrere in costi interni per la risoluzione di eventuali rilievi
     - potreste dover pagare molto meno (rispetto alla valutazione iniziale) per la cosiddetta “valutazione di follow-up”, durante la quale l’auditor verifica solo che abbiate risolto le non conformità risultanti dalla valutazione iniziale

     Anche nel caso in cui *emergano* rilievi, pagherete solo la valutazione completa più la breve valutazione di follow-up.

3. Pensate che non supererete la valutazione con conseguenze permanenti?

Il mancato superamento della valutazione non può essere permanente, perché potete sottoporre la vostra azienda a tutte le valutazioni che volete. Se il risultato della valutazione non rispecchia le vostre aspettative o se non riuscite a risolvere le non conformità attraverso azioni correttive entro il periodo di tempo obbligatorio di nove mesi, potrete semplicemente considerare questo tentativo fallito come una valutazione preliminare e cominciarne una nuova. Inoltre nessuno deve per forza vedere i risultati del vostro primo tentativo, potrete condividere semplicemente il risultato della valutazione superata con successo.

Ulteriori considerazioni:

- Se il risultato della valutazione è migliore di quanto vi aspettavate, potreste ricevere etichette TISAX temporanee. che potete condividere direttamente con il vostro partner. Ciò non è possibile con una valutazione preliminare.
- Se il fornitore di audit che effettua la valutazione preliminare è anche incaricato di condurre la valutazione TISAX, non può fornirvi servizi di consulenza. Diversamente, dovrete scegliere un altro fornitore di audit per la valutazione TISAX.

Sebbene la maggior parte delle aziende che si sottopongono all'audit non traggono alcun beneficio da una valutazione preliminare, vogliamo comunque menzionare i seguenti vantaggi.

L'auditor:

- può concentrarsi sugli aspetti critici dell'ISMS della vostra azienda sui quali non siete sufficientemente sicuri
- può impiegare più tempo rispetto al solito e intensificare gli approfondimenti
- può documentare i rilievi in maniera differente

Dopo aver letto le sezioni sul processo di valutazione TISAX, sarà ancora più semplice comprendere le nostre motivazioni.

7.8. Allegato: Ambiti personalizzati

La maggior parte dei partecipanti TISAX sceglie l'ambito standard. Tuttavia, in determinati e *rari* casi potrebbe essere necessario scegliere un ambito personalizzato.

Esistono due tipi di ambiti personalizzati:

7.8.1. Ambito personalizzato esteso

È possibile estendere l'ambito. Un ambito personalizzato esteso ha portata MAGGIORE rispetto all'ambito standard. Il fornitore di audit eseguirà più verifiche.

Finalità: un ambito personalizzato esteso può essere utile se volete utilizzare la valutazione TISAX per finalità interne o al di fuori del settore automotive.

Etichette TISAX e condivisione dei risultati: un ambito personalizzato esteso include sempre l'ambito standard. Pertanto un ambito personalizzato esteso riceverà le etichette TISAX[35]. Gli altri partecipanti TISAX accetteranno comunque il risultato della valutazione.

Descrizione: mentre l'ambito standard è provvisto di una descrizione predefinita, se avete bisogno di un ambito personalizzato esteso dovrete scrivere autonomamente la relativa descrizione.

7.8.2. Ambito personalizzato completo

È possibile definire completamente il proprio ambito.

Finalità: se la vostra azienda possiede sedi che rientrano in ambiti di valutazione diversi e che si avvalgono di servizi presso un determinato sito (ad esempio un data center), potreste usare un ambito personalizzato completo per tali servizi. In questo modo, un fornitore di audit TISAX può facilmente riutilizzare il risultato della valutazione dell'ambito personalizzato completo per il servizio.

Esempio: la vostra azienda possiede molte sedi (che rientrano eventualmente in ambiti diversi) e presso una di esse si trova il reparto IT centrale. La definizione di un ambito personalizzato completo solo per il reparto IT potrebbe rendere più semplice riutilizzare il relativo risultato della valutazione per altri ambiti.

Etichette TISAX e condivisione dei risultati: gli ambiti personalizzati completi non ricevono etichette TISAX. Il risultato della valutazione viene registrato nel portale ENX insieme alla data, al periodo di validità e all'indicazione se il risultato complessivo della valutazione è conforme o non conforme. Potete condividere tale risultato della valutazione, ma, per la maggior parte dei destinatari, la condivisione di un risultato della valutazione senza etichette TISAX apparirà come una valutazione "non superata". Gli altri partecipanti TISAX generalmente non accettano risultati delle valutazioni di ambiti personalizzati completi.

Descrizione: come per l'ambito personalizzato esteso, se avete bisogno di un ambito personalizzato completo dovrete scrivere autonomamente la relativa descrizione.

Nota importante:

Per farvi capire quanto sia raro usare ambiti personalizzati completi, precisiamo che nel 98% dei casi il fornitore di audit trasformerà il vostro ambito personalizzato completo in un ambito standard. Non accade *mai* che un partecipante scelga con successo un ambito personalizzato completo senza una consulenza da parte del suo fornitore di audit.

Una valutazione con ambito personalizzato completo non riceverà etichette TISAX. Solitamente sconsigliamo di scegliere un ambito personalizzato completo, principalmente perché gli altri partecipanti in genere

> non accettano risultati delle valutazioni con ambiti personalizzati completi. Non scegliete un ambito personalizzato completo se il vostro partner non vi ha esplicitamente confermato che accetterà il risultato e che è d'accordo con la vostra specifica descrizione dell'ambito.

7.9. Allegato: Gestione del ciclo di vita dei dati del partecipante

Nelle sezioni seguenti viene spiegato cosa dovete fare se i dati di partecipante della vostra azienda cambiano.

7.9.1. Perdita dell'accesso ai dati del partecipante (portale ENX)

Se all'interno della vostra azienda non c'è più nessuno che aveva accesso al portale ENX e quindi ai vostri dati di partecipante, contattateci. Cercheremo di aiutarvi a riottenere l'accesso ai dati di partecipante della vostra azienda.

7.9.2. Gestione dei contatti

I contatti principali della vostra azienda partecipante e tutti gli altri "contatti di gestione" che possiedono account per il portale possono sempre accedere al portale ENX e:

- aggiungere nuovi contatti
- eliminare i contatti esistenti
- modificare i dati di contatto dei contatti esistenti

7.9.2.1. Come aggiungere un nuovo contatto

Per aggiungere un nuovo contatto, seguite questi passaggi:

1. Accedete al portale ENX.
2. Andate alla barra di navigazione principale e selezionate "MY TISAX" ("IL MIO TISAX").
3. Dal menu a discesa, selezionate "ADMINISTRATORS" ("AMMINISTRATORI").
4. Fate clic sul pulsante "Create new TISAX Administrator" ("Crea nuovo amministratore TISAX").
5. Inserite i dati del contatto in questione.
6. Fate clic sul pulsante "Save Contact" ("Salva contatto").
7. Andate alla tabella e cercate la riga con il contatto in questione.
8. Andate alla fine della riga della tabella corrispondente al contatto in questione e fate clic sul pulsante con la freccia verso il basso .
9. Selezionate "Edit TISAX Administrator" ("Modifica amministratore TISAX").

10. Nella nuova finestra (“Edit TISAX Contact” (“Modifica contatto TISAX”)), scorrete verso il basso fino alla sezione “ENX PORTAL ACCESS” (“ACCESSO AL PORTALE ENX”).
11. Selezionate “Yes” (“Sì”).
12. Nella sezione che appare “WEB ROLES” (“RUOLI WEB”), fate clic sul pulsante “Add Role” (“Aggiungi ruolo”).
13. Selezionate il ruolo che volete assegnare (es. “TISAX Administrator” (“Amministratore TISAX”)).
14. Fate clic sul pulsante “Add Role” (“Aggiungi ruolo”).
15. Fate clic sul pulsante “Save Contact” (“Salva contatto”).

7.9.2.2. Come eliminare un contatto esistente

Per eliminare un contatto esistente, seguite questi passaggi:

1. Accedete al portale ENX.
2. Andate alla barra di navigazione principale e selezionate “MY TISAX” (“IL MIO TISAX”).
3. Dal menu a discesa, selezionate “ADMINISTRATORS” (“AMMINISTRATORI”).
4. Andate alla tabella e cercate la riga con il contatto in questione.
5. Andate alla fine della riga della tabella corrispondente al contatto in questione e fate clic sul pulsante con la freccia verso il basso .
6. Selezionate “Delete TISAX Administrator” (“Elimina amministratore TISAX”).
7. Nella richiesta di conferma che compare, fate clic sul pulsante “Delete” (“Elimina”).

7.9.2.3. Come aggiornare i dati di un contatto esistente

Per aggiornare i dati di un contatto esistente, seguite questi passaggi:

1. Accedete al portale ENX.
2. Andate alla barra di navigazione principale e selezionate “MY TISAX” (“IL MIO TISAX”).
3. Dal menu a discesa, selezionate “ADMINISTRATORS” (“AMMINISTRATORI”).
4. Andate alla tabella e cercate la riga con il contatto in questione.
5. Andate alla fine della riga della tabella corrispondente al contatto in questione e fate clic sul pulsante con la freccia verso il basso .
6. Selezionate “Edit TISAX Administrator” (“Modifica amministratore TISAX”).
7. Aggiornate i dati.
8. Fate clic sul pulsante “Save Contact” (“Salva contatto”).

7.9.3. Gestione delle sedi

I contatti principali della vostra azienda partecipante e tutti gli altri “contatti di gestione” che possiedono account per il portale possono sempre accedere al portale ENX e richiedere:

- la modifica della denominazione dell’azienda
- la modifica di una sede (trasferimento/cambio di sede)
- la modifica del nome di una via
- l’aggiunta di una nuova sede

I passaggi da seguire sono descritti nelle sezioni seguenti.

Attenzione:

- Nell’ambito di TISAX, la combinazione di una denominazione aziendale e di un indirizzo indica una “sede”.
- Ciascuna sede è dotata di un “ID Sede” (gli ID Sede cominciano sempre con una “L” e sono composti da sei caratteri; esempio: L1L3XY).
- Se l’indirizzo della vostra azienda cambia, la vecchia sede non sarà più valida.

Nota importante:

Una volta che avete fatto clic sul pulsante “Save Location” (“Salva sede”) nel portale ENX, non potete più apportarvi modifiche autonomamente. Potete richiedere modifiche nei casi descritti di seguito.

7.9.3.1. Come richiedere la modifica della denominazione della propria azienda

Situazione:	La denominazione della vostra azienda è cambiata.
Esempio:	La vecchia denominazione era “ACME Tires Corporation”. La nuova denominazione è “ACME Corporation”.

Per richiedere la modifica della denominazione della vostra azienda, seguite questi passaggi:

1. Accedete al portale ENX.
2. Andate alla barra di navigazione principale e selezionate “MY TISAX” (“IL MIO TISAX”).
3. Dal menu a discesa, selezionate “LOCATIONS” (“SEDI”).
4. Andate alla tabella e cercate la riga con la vostra sede.
5. Andate alla fine della riga della tabella corrispondente alla vostra sede e fate clic sul pulsante con la freccia verso il basso .

6. Selezionate “Request Change” (🇮🇹 “Richiedi modifica”).
7. Nella nuova finestra (“Request Change” (🇮🇹 “Richiedi modifica”)), andate al campo del modulo “Subject of the change” (🇮🇹 “Oggetto della modifica”), aprite il menu a discesa e selezionate “Company Name” (🇮🇹 “Denominazione aziendale”).
8. Proseguite con la compilazione del modulo.
9. Inviate il modulo.

Controlleremo la vostra richiesta di modifica della denominazione aziendale, la quale verrà eventualmente approvata, e vi informeremo una volta apportata la modifica.

7.9.3.2. Come richiedere la modifica di una sede

Situazione:	La vostra azienda si è trasferita in una nuova sede.
Esempio:	La vecchia sede era “ACME Corporation, Bockenheimer Landstraße 97-99, 60325 Francoforte, Germania”. La nuova sede è “ACME Corporation, Behrenstraße 35, 10117 Berlino, Germania”.

Nota importante:

Se un ente ufficiale ha rinominato la via della vostra sede, fate riferimento alla Sezione 7.9.3.3, “Come richiedere la modifica del nome di una via” per maggiori informazioni.

Se una delle vostre sedi si è trasferita a un nuovo indirizzo, seguite questi passaggi:

1. Create una nuova sede:
   a. Accedete al portale ENX.
   b. Andate alla barra di navigazione principale e selezionate “MY TISAX” (🇮🇹 “IL MIO TISAX”).
   c. Dal menu a discesa, selezionate “Locations” (🇮🇹 “Sedi”).
   d. Fate clic sul pulsante “Create TISAX Location” (🇮🇹 “Crea sede TISAX”).
   e. Nella nuova finestra (“CREATE TISAX LOCATION” (🇮🇹 “CREA SEDE TISAX”)), compila il modulo con i dati della nuova sede.
   f. Fate clic sul pulsante “Save Location” (🇮🇹 “Salva sede”).
2. Prendete nota del “Location ID” (🇮🇹 “ID Sede”) della sede appena creata. L’“ID Sede” è indicato nella prima colonna della tabella “MY LOCATIONS” (🇮🇹 “LE MIE SEDI”). Il fornitore di audit ha bisogno dell’“ID Sede” per aggiornare il vostro ambito di valutazione nel portale ENX.

3. Informate il vostro fornitore di audit del cambio di sede (fornitegli l'"ID Sede" della vecchia sede e quello della nuova sede).
   Avete già completato la valutazione?
   a. Se la risposta è NO, non dovete fare nient'altro per quanto riguarda il cambio di sede.
   b. Se la risposta è SÌ, dovete richiedere una "valutazione di estensione dell'ambito" ("scope extension assessment") al vostro fornitore di audit. Per maggiori informazioni, si veda Sezione 7.10, "Allegato: Valutazione di estensione dell'ambito".

Il fornitore di audit controllerà la vostra richiesta e aggiornerà il vostro ambito di valutazione nel portale ENX.

Attenzione:

Un fornitore di audit può aggiornare il vostro ambito di valutazione solo se avete già richiesto la valutazione da tale fornitore di audit.

7.9.3.3. Come richiedere la modifica del nome di una via

Situazione:	Il nome della via della vostra sede è cambiato, ma l'ubicazione fisica della vostra azienda è sempre la stessa.
Esempio:	La vecchia sede era "ACME Corporation, Bockenheimer Landstraße 97-99, 60325 Francoforte, Germania". La nuova sede è "ACME Corporation, Behrenstraße 97-99, 60325 Francoforte, Germania".

Se un ente ufficiale ha rinominato la via della vostra sede, seguite questi passaggi:

1. Accedete al portale ENX.
2. Andate alla barra di navigazione principale e selezionate "MY TISAX" ("IL MIO TISAX").
3. Dal menu a discesa, selezionate "Locations" ("Sedi").
4. Andate alla tabella e cercate la riga con la vostra sede.
5. Andate alla fine della riga della tabella corrispondente alla vostra sede e fate clic sul pulsante con la freccia verso il basso .
6. Selezionate "Request Change" ("Richiedi modifica").
7. Nella nuova finestra ("Request Change" ("Richiedi modifica")), andate al campo del modulo "Subject of the change" ("Oggetto della modifica"), aprite il menu a discesa e selezionate "Address" ("Indirizzo").
8. Proseguite con la compilazione del modulo.
9. Inviate il modulo.

Controlleremo la vostra richiesta di modifica del nome della via, la quale verrà eventualmente approvata, e vi informeremo una volta apportata la modifica.

Nota importante:

Questi passaggi si applicano solo nel caso in cui l'ubicazione fisica della vostra azienda non cambi, ma il nome della via è stato modificato da un ente ufficiale. Se vi trasferite in una nuova sede, consultate la Sezione 7.9.3.2, "Come richiedere la modifica di una sede" per maggiori informazioni.

7.9.3.4. Come aggiungere un'ulteriore sede

Se aprite un'ulteriore sede durante il periodo di validità delle vostre etichette TISAX esistenti, potete richiedere una "valutazione di estensione dell'ambito" (🇬🇧 "scope extension assessment") al vostro fornitore di audit.

Per maggiori informazioni, si veda Sezione 7.10, "Allegato: Valutazione di estensione dell'ambito".

7.10. Allegato: Valutazione di estensione dell'ambito

Oltre alle tipologie di valutazione standard descritte nella Sezione 5.4.3, "Tipologie di valutazione TISAX", è prevista un'altra tipologia di valutazione speciale: la "valutazione di estensione dell'ambito" (🇬🇧 "scope extension assessment").

Potete estendere un ambito di valutazione TISAX esistente se volete aggiungere uno/a o più:

- obiettivi di valutazione, o
- sedi.

Non potete scegliere un altro fornitore di audit per condurre una "valutazione di estensione dell'ambito". La valutazione è simile alle tipologie di valutazione standard, tuttavia molto probabilmente il vostro fornitore di audit sceglierà di riutilizzare i risultati applicabili provenienti dalle valutazioni precedenti.

Una volta che la valutazione di estensione dell'ambito sarà conclusa senza non conformità, il vostro fornitore di audit:

- aggiornerà il vostro ambito di valutazione nel portale ENX.
- emetterà la relazione della valutazione di estensione dell'ambito.

Una valutazione di estensione dell'ambito non estende il periodo di validità originale delle vostre etichette TISAX esistenti.

Attenzione:

> Se il motivo della valutazione di estensione dell'ambito è un cambio di sede o l'aggiunta di una sede, dovrete creare la nuova sede nel portale ENX. Fornite al vostro fornitore di audit l'"Estratto Sede" o almeno l'"ID Sede".
> Ciascuna sede è dotata di un "ID Sede" (gli ID Sede cominciano sempre con una "L" e sono composti da sei caratteri; esempio: L1L3XY). Il fornitore di audit ha bisogno dell'ID Sede per aggiornare il vostro risultato di valutazione nel portale ENX.

7.11. Allegato: Gestione del ciclo di vita dell'ISA

Un gruppo di lavoro di ENX si occupa della gestione dell'ISA.

Le informazioni riportate di seguito potrebbero essere di vostro interesse:

- La VDA pubblica ufficialmente nuove versioni.
- Il fornitore di audit utilizzerà la versione dell'ISA valida al momento della vostra *richiesta* di una valutazione iniziale.
- Di comune accordo, è possibile utilizzare una versione dell'ISA più recente se ne viene pubblicata una nel periodo che intercorre tra il momento in cui avete fatto la richiesta e l'inizio della valutazione iniziale.
- La data di pubblicazione di una determinata versione dell'ISA è disponibile nel foglio Excel "Copertina".
  - Esempio:
    Versione: 5.0 | Revisione 4 | 2021-04-16

7.12. Allegato: Documenti utili

In questa sezione sono elencati documenti che consideriamo utili.

- White Paper "Harmonization of classification levels" ("Armonizzazione dei livelli di classificazione")

  "Questo White Paper descrive la proposta del gruppo di lavoro sulla sicurezza delle informazioni per l'elaborazione di uno schema incentrato sull'obiettivo di protezione della riservatezza; ciò significa che le informazioni non vengono rese accessibili a persone, organizzazioni o processi non autorizzati. Inoltre, questo White Paper non si concentra sugli obiettivi di protezione come la disponibilità, l'integrità e l'affidabilità".

  Editore: Verband der Automobilindustrie e.V. ("Associazione tedesca dell'industria automobilistica")

  Lingue disponibili: inglese, tedesco

https://www.vda.de/en/news/publications/publication/harmonization-of-classification-levels
https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--harmonisierung-der-klassifizierungsstufen-

- White Paper “Information Security Risk Management” (“Gestione dei rischi per la sicurezza delle informazioni”)

  “L’obiettivo di questo White Paper è quello di informare le aziende del settore automobilistico in merito alla gestione della sicurezza delle informazioni orientata al rischio e di metterle in grado di definire una gestione efficace dei rischi per la sicurezza delle informazioni. Il suo scopo è quello di supportare le organizzazioni nella preparazione o nell’esecuzione di una valutazione TISAX per soddisfare i requisiti della domanda di controllo 1.4.1 dell’ISA di VDA. Il suo contenuto deve essere considerato alla stregua di consigli di implementazione, non di requisiti obbligatori”.

  Editore: Verband der Automobilindustrie e.V. (“Associazione tedesca dell’industria automobilistica”)

  Lingue disponibili: inglese, tedesco

  https://www.vda.de/en/news/publications/publication/white-paper--information-security-risk-management-
  https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--risikomanagement-in-der-informationssicherheit-

7.13. Allegato: Gestione dei reclami

7.13.1. Cause dei reclami

La nostra gestione dei reclami fa una distinzione tra queste due aree:

1. ENX Association: l’organizzazione che regolamenta TISAX
2. Fornitori di audit: le organizzazioni che conducono le valutazioni TISAX

7.13.1.1. Reclami relativi a ENX Association

In caso di reclami relativi a ENX Association, contattate il nostro “responsabile TISAX competente” (si vedano i dati di contatto riportati di seguito).

7.13.1.2. Reclami relativi ai fornitori di audit

Cercate innanzitutto di risolvere il problema direttamente con l’auditor in questione.

Il passo successivo è quello di rivolgersi al soggetto responsabile di TISAX presso il fornitore di audit.

Il referente successivo da contattare è il responsabile della gestione della qualità del fornitore di audit.

Nel caso in cui non siate ancora riusciti a risolvere il problema, contattate il nostro “responsabile TISAX competente” (si vedano i dati di contatto riportati di seguito).

Vi sono inoltre referenti di livello superiore rispetto al “responsabile TISAX competente”. In tali casi vi dovrete rivolgere al direttore generale di ENX Association.

La VDA non ricopre alcun ruolo nella gestione dei reclami.

Attenzione:

Il fornitore di audit è tenuto a informarvi del vostro diritto a presentare un reclamo durante la riunione iniziale. Qualora non lo faccia, questo sarebbe già un motivo di reclamo.

7.13.1.3. Requisiti per i reclami

Se volete coinvolgerci in questo processo, abbiamo bisogno delle seguenti informazioni:

- Chi presenta il reclamo?
  - Denominazione dell’azienda
  - ID Partecipante TISAX
  - Contatti (nome, indirizzo e-mail, numero di telefono)
- Quale valutazione è coinvolta?
  - ID Valutazione
  - Se la valutazione non è ancora registrata nel portale ENX: ID Ambito
- Chi è il fornitore di audit?
  - Nome dell’azienda del fornitore di audit
  - Nome dell’auditor (o degli auditor)
- Qual è l’oggetto del reclamo?
  1. Reclamo generale relativo ai servizi del fornitore di audit
  2. Reclamo relativo all’approccio dell’auditor
  3. Reclamo relativo alla valutazione in termini di contenuto
- Nel caso di reclami relativi alla valutazione in termini di contenuto: Quale rilievo viene contestato?
  - Controllo (es. 1.6.1 "In quale misura vengono elaborati gli eventi relativi alla sicurezza delle informazioni?")

- Rilievo (testo completo)
- Contestazione relativa a:
  - Interpretazione del controllo
  - Accertamento rispetto al contenuto (le prove disponibili non sono valutate correttamente)
  - Valutazione dei rischi (adeguatezza non considerata)
- Motivazione per cui valutate la situazione in maniera diversa

7.13.2. Contatto per i reclami

Contattate il “responsabile TISAX competente”:

Potete inviargli un’e-mail all’indirizzo:	tisax-complaints@enx.com
Oppure contattarlo telefonicamente al numero:	+49 69 9866927-79

Il responsabile è raggiungibile durante il normale orario di lavoro in Germania (UTC+01:00).

Il responsabile parla inglese e tedesco.

8. Cronologia dei documenti

Versione 2.7

- Altre quattro lingue aggiunte (giapponese, portoghese del Brasile, italiano, coreano)
- Commutatore di lingua per versioni HTML aggiunte (nell'angolo in alto a destra)
- Layout delle versioni PDF perfezionato
- Diverse sezioni aggiornate con i due nuovi obiettivi di valutazione della riservatezza
- Sezione "Lista degli obiettivi di valutazione" aggiornata (formulazione dell'obiettivo di valutazione "Special data" corretto; aggiunta nota relativa alla transizione dell'etichetta)
- Errori di battitura corretti

Versione 2.6

- Nota generale sugli obiettivi di valutazione e sulle etichette che abbiamo aggiunto in questa versione: nelle versioni precedenti, gli obiettivi di valutazione e le etichette avevano un "nome ufficiale" lungo e un "nome abbreviato" (esempio: "Gestione delle informazioni con esigenze di protezione elevate" e "Info high"). Dal momento che la maggior parte delle persone usava solo il nome abbreviato questo è ora diventato il "nome ufficiale". Il vecchio nome lungo viene ora definito "Descrizione". Inoltre, usiamo *solo* il nome ufficiale inglese nel portale ENX e in tutte le traduzioni del Manuale per i partecipanti TISAX.
- Sezione "Elenco degli obiettivi di valutazione" aggiornata con i due obiettivi di valutazione "High availability" e "Very high availability" e "Figura 6. Obiettivi di valutazione TISAX (raffigurazione tabellare, forme lunghe e brevi)" rimossa.
- Sezione "Obiettivi di valutazione e ISA" aggiornata per riflettere il fatto che solo un sottoinsieme del catalogo di criteri Sicurezza delle informazioni si applica ai due obiettivi di valutazione "High availability" e "Very high availability"
- Sezione "Obiettivi di valutazione e relative dipendenze" rimossa
- Sezione "Selezione degli obiettivi di valutazione" aggiornata con i due obiettivi di valutazione "High availability" e "Very high availability"
- Sezione "Esigenze di protezione ed obiettivi di valutazione" aggiornata con i due obiettivi di valutazione "High availability" e "Very high availability" e "Tabella 5. Corrispondenza dei cataloghi di criteri dell'ISA e delle esigenze di protezione con gli obiettivi di valutazione TISAX" rimossa
- Sezione "Cataloghi di criteri" aggiornata con i due obiettivi di valutazione "High availability" e "Very high availability"
- Sezione "Requisiti" aggiornata per riflettere il fatto che solo un sottoinsieme del catalogo di criteri Sicurezza delle informazioni si applica ai due obiettivi di valutazione "High

availability” e “Very high availability”

- Sezione “Gerarchia delle etichette TISAX” aggiornata per riflettere il fatto che ormai una gerarchia esiste solo in pochi casi e “Figura 36. Obiettivi di valutazione e le etichette TISAX (dipendenze e gerarchia)” rimossa.
- Sezione “Allegato: Documenti utili” aggiornata per riflettere le modifiche ai link
- Chiarimenti minori e piccole correzioni di vario tipo
- Errori di battitura corretti

Versione 2.5.1

- Link non funzionanti corretti

Versione 2.5

- Sezione “Gestione delle sedi” aggiunta
- Sezione “Allegato: Documenti utili” aggiornata per riflettere le modifiche ai link

Versione 2.4

- Dichiarazione errata sulla durata massima del processo di valutazione TISAX rimossa dalla Sezione 3.1, “Panoramica”
- “Relazione TISAX” rinominata “Relazione della valutazione TISAX”
- Nota relativa alle differenze tra ISO 27001 e TISAX aggiornata
- Sezione “Descrizione dell’ambito” aggiornata; sezione relativa all’ambito personalizzato spostata nell’allegato
- “Descrizione dell’ambito standard” aggiornata alla versione 2.0
- Sezione “Pubblicazione e condivisione” aggiornata con nota relativa alla condivisione dello stato della valutazione
- Sezione “Esigenze di protezione e livelli di valutazione” aggiornata con contenuti sul “livello di valutazione 2.5”, sul “metodo di valutazione a distanza con supporto video”, sulle differenze tra AL 2 e AL 3, sul controllo di attendibilità vs verifica
- Link per l’avvio della procedura di registrazione aggiornato
- Sezione “Account sul portale” aggiornata per riflettere il processo di invito modificato
- Link per il download del documento ISA modificati (ora disponibili anche su enx.com)
- Sezione “Valutazione delle offerte” aggiornata con una base per le stime dei costi
- Sezione “Riunione iniziale” aggiunta (contenuti spostati qui dalla sezione “La prima riunione

formale di apertura”)

- Sezione “Informazioni sulla conformità” aggiornata con una nuova tabella sui quattro tipi di rilievi
- Sezione “Valutazione iniziale” aggiornata con nota relativa ai vincoli temporali
- Sezione “Relazione della valutazione TISAX” aggiornata con nota relativa a un piano d’azione correttivo proattivo
- Sezione “Preparazione del piano d’azione correttivo” aggiornata con i requisiti “rilievo” e “causa principale” e nota relativa ai modelli per il piano d’azione correttivo
- Sezione “Valutazione del piano d’azione correttivo” aggiornata con un’osservazione relativa all’utilizzo dell’e-mail come sola modalità di comunicazione
- Sezione “Prerequisiti per una valutazione del piano d’azione correttivo” rinominata “Motivazioni alla base di una valutazione del piano d’azione correttivo” e due motivazioni aggiunte
- Sezione “Etichette TISAX temporanee” aggiornata con esempi e chiarimenti relativamente al periodo di validità
- Sezione “Relazione TISAX” rinominata “Relazione della valutazione TISAX”
- Sezione “Rinnovo delle etichette TISAX” aggiornata con una nota relativa al riutilizzo dei dati delle sedi nel portale ENX
- Sezione “Allegato: Motivazioni a sfavore delle “valutazioni preliminari” e delle “analisi dei divari”” aggiunta
- Sezione “Allegato: Ambiti personalizzati” aggiunta (“Ambito esteso” e “Ambito ristretto” sostituiti da “Ambito personalizzato esteso” e “Ambito personalizzato completo”)
- Sezione “Allegato: Valutazione di estensione dell’ambito” aggiornata con motivazioni e una nota relativa all’aggiunta dei dati delle sedi all’account del partecipante sul portale ENX
- Sezione “Allegato: Gestione del ciclo di vita dell’ISA” aggiornata per riflettere la situazione attuale
- Sezione “Allegato: Documenti utili” aggiornata per riflettere le modifiche ai link
- Sezione “Allegato: Gestione dei reclami” aggiunta
- È ora possibile fare clic sui numeri di telefono
- Chiarimenti minori e piccole correzioni di vario tipo
- Errori di battitura corretti
- Nota per i fornitori di audit TISAX: questo aggiornamento si basa sul documento ENX ID 612 versione 2.1

Versione 2.3

- Didascalie riformulate
- Passaggio da Word/PDF a HTML come formato principale del manuale
- Ulteriori traduzioni disponibili (cinese e francese, si veda punto successivo)
- Sezione “Il Manuale per i partecipanti TISAX in altre lingue e altri formati aggiunta
- Tutti i link alla home page di ENX modificati da "https://portal.enx.com" a "https://enx.com" (i vecchi link sono ancora funzionanti)
- “ISA di VDA” diventa “ISA”
- Sezione Sezione 5.2, “Autovalutazione basata sull’ISA” aggiornata per riflettere le modifiche introdotte con la versione 5 dell’ISA
- Righe di tutte le tabelle riportanti gli obiettivi di valutazione riordinate per allinearsi all’ordine modificato dei cataloghi di criteri nell’ISA 5
- Figure riportanti gli obiettivi di valutazione aggiornate per allinearsi all’ordine modificato dei cataloghi di criteri nell’ISA 5
- Sezione “Personalizzazione dell’ambito” aggiornata (figura 6, errore di battitura corretto, obiettivi di valutazione aggiornati)
- Sezione “Tariffa” aggiornata con informazioni sui pagamenti con carta di credito
- Sezione “Grafico del processo di valutazione TISAX” aggiornata (figura 34, riferimento al fornitore di servizi gestiti rimosso)
- Sezione “Allegato: Documenti utili” aggiornata (White Paper “Information Security Risk Management” (Gestione dei rischi per la sicurezza delle informazioni) aggiunto)

Versione 2.2.1

- Errori di battitura corretti

Versione 2.2

- Errore di stampa nella copertina risolto
- Tutti i link alla nostra home page e per i download modificati
- Ora parliamo anche italiano
- Sezione “Ambito personalizzato” estesa
- Sezione “Sedi dell’ambito” aggiornata
- Obiettivo di valutazione “Collegamento con terze parti” rimosso; figure 7, 9, e 38 aggiornate; tabelle 4, 5, 6 e 8 aggiornate
- Formulazione “*con* livello di valutazione” modificata con “*nel* livello di valutazione”

- Riferimento alla “lista di attivazione TISAX” nella sezione “Esigenze di protezione e livelli di valutazione” rimosso
  (non più applicabile)
- Sezione “Obiettivi di valutazione e fornitori della vostra azienda” aggiunta
- Sezione “Contatto del partecipante” aggiornata con informazioni relative agli indirizzi e-mail di gruppo e agli inviti ai contatti per consentire loro di gestire i dati del partecipante nel portale ENX
- Sezione “Registrazione dell’ambito di valutazione” aggiornata con informazioni sulle modifiche all’ambito di valutazione
- Sezione “Informazioni sullo stato” aggiornata (figura 12)
- Sezione “Gestione del risultato dell’autovalutazione” aggiornata con informazioni relative all’assistenza esterna di terze parti
- Sezione “Copertura” aggiornata con link alla matrice di copertura dei fornitori di audit
- Sezione “Richiesta di offerte” aggiornata
- Sezione “Valutazione delle offerte” aggiornata con informazioni relative alle “valutazioni preliminari”
- Sezione “Rinnovo delle etichette TISAX” aggiornate con informazioni relative alla necessità di registrare un nuovo ambito
- Diverse sotto-sezioni della sezione “Scambio (fase 3)” aggiornate per riflettere le modifiche dell’interfaccia nel portale ENX
- Sezione “Condivisione del risultato della valutazione con un partecipante specifico” aggiornata con consigli relativi al livello di condivisione e con una nota relativa all’elaborazione automatica dei risultati della valutazione condivisi
- Sezione “Condivisione del risultato della valutazione al di fuori di TISAX aggiunta
- Sezione “Gestione del ciclo di vita dell’ISA” aggiunta
- Sezione “Allegato: Stato dell’ambito di valutazione” aggiornata (nuovo stato “In attesa dell’ordine”, stato “In attesa di approvazione” rinominato “In attesa dell’approvazione di ENX”, stato “Approvato” rinominato “In attesa del pagamento”, figura 40)
- Sezione “Allegato: Esempio di e-mail di conferma” aggiornata
- Sezione “Allegato: Esempio dell’Estratto dell’ambito TISAX” aggiornata
- Sezione “Allegato: Stato della valutazione” aggiornata (nuovo stato “Valutazione iniziale in corso”, stato “In attesa della valutazione di follow-up” rinominato “In attesa del follow-up”, figura 41)
- Sezione “Allegato: Valutazioni sull’eredità di Volkswagen” (e relativi riferimenti) rimossa (non più pertinente)

Versione 2.1.2

- Limite formale della “distanza” tra il “punteggio della vostra azienda” e il “punteggio massimo” corretto da 25% a 30%

Versione 2.1.1

- Errori di battitura corretti

Versione 2.1

- Sezione “Fornitori di servizi gestiti” rimossa
- Nuovi/e obiettivi di valutazione/etichette TISAX (etichette per la protezione dei dati sulla base del GDPR; quattro etichette per i prototipi invece che due; riformulazione: esigenze di protezione al posto di livelli di protezione; consigli per la selezione aggiornati)
- Aggiornamenti dovuti a modifiche dell’ISA (da versione 4.0 a 4.1)
- Riferimento al nuovo documento “Valutazione di gruppo semplificata TISAX” (aggiunta al presente manuale)
- Suggerimenti per l’assegnazione dei nomi delle sedi e dei nomi degli ambiti aggiunti
- “Tariffa di registrazione” rinominata “tariffa”
- Consiglio sui sostituti dei contatti aggiunto
- Selezione del modello di addebito rimossa

Torna all’inizio.

[1] Potreste prendere in considerazione l’idea di completare il processo TISAX come azione preventiva. Alcune aziende prendono questa decisione per essere più preparate, poiché avere già conseguito una valutazione TISAX potrebbe significare un periodo di onboarding molto più breve e darvi quindi un vantaggio rispetto ai concorrenti che non si sono ancora sottoposti a una valutazione TISAX.

[2] Le “etichette TISAX” sintetizzano il risultato della valutazione e rappresentano l’elemento a valle del processo TISAX. Si veda Sezione 5.4.14, “Etichette TISAX” per maggiori dettagli.

[3] La maggior parte delle operazioni di registrazione deve essere eseguita una sola volta quando si diventa partecipanti TISAX. Quando si decide di rinnovare il risultato della valutazione, è sufficiente aggiornare e confermare i dati di registrazione.

[4] Le modifiche alle nostre CG verranno pubblicate sul portale ENX e comunicate ai contatti registrati.

[5] Ciò vale anche per tutti gli altri accordi aggiuntivi (ad esempio, i codici di condotta).

[6] Si precisa che al momento il partner non viene automaticamente informato sulle nuove autorizzazioni. Si consiglia di informare il partner una volta che il risultato della valutazione è disponibile.

[7] Se desiderate includere la vostra azienda in questo elenco, contattateci.

[8] Con prove si intendono tutti gli elementi a supporto del fatto che la vostra azienda soddisfi un determinato requisito. Si tratta per lo più di documenti, vi avvarrete quindi sicuramente di documentazione interna come prova.

[9] I colloqui per le valutazioni nel livello di valutazione 2 vengono generalmente condotti tramite videoconferenza. Su richiesta dell'azienda i colloqui possono essere effettuati in sede.

[10] Il numero minimo di sedi previsto per le valutazioni di gruppo semplificate è di tre.

[11] Se sapete già di dover migliorare il sistema di gestione della sicurezza delle informazioni della vostra azienda, il numero minimo consigliato è di almeno dodici sedi.

[12] Al fine di evitare confusione tra numeri e lettere (come 8 e B), alcune lettere non sono consentite negli ID Partecipante. Tuttavia alcuni ID Partecipante più vecchi potrebbero contenere la lettera "G".

[13] L'ISA si riferisce ai cataloghi di criteri anche come "moduli".

[14] La funzione di Excel sottostante si trova nella barra multifunzione "Dati", sezione "Struttura".

[15] Se conoscete fornitori di audit che svolgono valutazioni simili (come la ISO 27001) per la vostra azienda e che sono interessati a condurre anche la valutazione TISAX, condividete con loro questo manuale e dite loro di contattarci per scoprire come diventare fornitori di audit TISAX

[16] I fornitori di audit non compresi nel nostro elenco non sono autorizzati a condurre valutazioni TISAX.

[17] Se si interrompe il processo di valutazione, non si riceveranno le etichette TISAX.

[18] In realtà esiste una quarta tipologia: la "valutazione di estensione dell'ambito". Trattandosi di una casistica particolare, viene descritta in dettaglio nell'allegato in Sezione 7.10, "Allegato: Valutazione di estensione dell'ambito".

[19] La riunione formale *di apertura* sarà descritta nel dettaglio solo per la valutazione iniziale. Per le altre valutazioni TISAX sarà il vostro fornitore di audit a programmare e organizzare queste riunioni.

[20] Alcuni fornitori di audit potrebbero usare il termine "riunione iniziale" come sinonimo di "riunione formale di apertura".

[21] La riunione formale *di chiusura* sarà descritta nel dettaglio solo per la valutazione iniziale. Per le altre valutazioni TISAX sarà il vostro fornitore di audit a programmare e organizzare queste riunioni.

[22] Qualora non si riuscisse a risolvere una contestazione, è possibile procedere con un'escalation del problema. Per altre informazioni, si veda Sezione 7.13, "Allegato: Gestione dei reclami" per maggiori dettagli.

[23] Per maggiori informazioni sui metodi di audit e intensità, si veda Sezione 4.3.3.5, "Esigenze di protezione e livelli di valutazione".

[24] Qualora non si riuscisse a risolvere una contestazione, è possibile procedere con un'escalation del problema. Contattateci per ulteriori dettagli.

[25] Si precisa che il risultato complessivo della valutazione può comunque essere "non conforme di livello grave" anche se avete stabilito azioni correttive adeguate. Ciò si verifica se le misure adottate non hanno/possono avere effetto immediato.

[26] Ciò vale ovviamente solo nel caso di una valutazione iniziale durante la quale sono emerse non conformità. La valutazione di follow-up non è necessaria nel caso di una valutazione iniziale con risultato "conforme".

[27] In teoria, tale termine può essere nove mesi dopo la conclusione della valutazione iniziale.

[28] In realtà esiste una quarta tipologia: la "relazione della valutazione di estensione dell'ambito". Trattandosi di una casistica particolare, viene descritta in dettaglio in Sezione 7.10, "Allegato: Valutazione di estensione dell'ambito".

[29] La "relazione della valutazione TISAX" si basa su un modello che tutti i fornitori di audit TISAX sono obbligati a usare.

[30] Il termine "rinnovo" potrebbe essere fuorviante. Per mantenere un'etichetta X per più di tre anni, è necessario ripetere il processo TISAX, a partire dalla registrazione di un nuovo ambito di valutazione.

[31] Non redigiamo un elenco "TISAX pubblico" degli ID Partecipante per evitare una condivisione accidentale dovuta a nomi di società simili o altri "errori umani". Pertanto, dovrete sempre chiedere l'ID Partecipante direttamente al vostro partner.

[32] Il vostro partner deve accedere al portale e cercare attivamente il risultato della valutazione che avete condiviso. I partner non ricevono infatti una notifica automatica relativa ai nuovi risultati delle valutazioni condivisi.

[33] La regola è stabilita nelle "Condizioni generali di partecipazione a TISAX" (https://enx.com/tisaxgtcen.pdf).

[34] Quando lo stato dell'ambito di valutazione è "In attesa del pagamento" o "Registrato", "Informazioni relative alla valutazione" include la/le sede/i dell'ambito di valutazione, lo stato dell'ambito di valutazione e l'obiettivo (o gli obiettivi) di valutazione, ma non include i risultati della valutazione o le etichette TISAX.

[35] Le “etichette TISAX” sintetizzano il risultato della valutazione e rappresentano l’elemento a valle del processo TISAX. Si veda Sezione 5.4.14, “Etichette TISAX” per maggiori dettagli.