Manual do participante de TISAX

Passe pelo processo de avaliação TISAX e compartilhe o resultado da avaliação com seu parceiro

Publicado por

ENX Association
uma Associação de acordo com a Lei Francesa de 1901,
registrada sob o número w923004198 na Sous-préfecture de Boulogne-Billancourt, França

Endereços
20 rue Barthélémy Danjou, 92100 Boulogne-Billancourt, França
Bockenheimer Landstraße 97-99, 60325 Frankfurt am Main, Alemanha

Autor

Florian Gleich

Contato

tisax@enx.com
+49 69 9866927-77

Versão

Data:	2023-12-07
Versão:	2.7
Classificação:	Public
ENX doc ID:	602-PT-BR

Aviso sobre direitos autorais

Todos os direitos reservados à ENX Association.
ENX, TISAX e seus respectivos logotipos são marcas registradas da ENX Association.
As marcas registradas de terceiros mencionadas são propriedade de seus respectivos proprietários.

Índice

1. Visão geral . . . 8
1.1. Finalidade . . . 8
1.2. Escopo . . . 8
1.3. Público . . . 9
1.4. Estrutura . . . 9
1.5. Como usar este documento . . . 9
1.6. Entre em contato conosco . . . 10
1.7. Observe o Manual do participante TISAX em outros idiomas e formatos . . . 10
1.7.1. Sobre a tradução para Português do Brasil . . . 13
1.7.2. Sobre o formato on-line . . . 13
1.7.3. Sobre o formato off-line . . . 13
1.7.4. Sobre o formato PDF . . . 14
2. Introdução . . . 15
2.1. Por que o TISAX? . . . 15
2.2. Quem define o que significa "seguro"? . . . 15
2.3. O jeito automotivo . . . 16
2.4. Como comprovar a segurança de forma eficiente? . . . 16
3. O processo TISAX . . . 18
3.1. Visão geral . . . 18
3.2. Cadastro . . . 19
3.3. Avaliação . . . 19
3.4. Compartilhamento . . . 20
4. Cadastro (Etapa 1) . . . 21
4.1. Visão geral . . . 21
4.2. Você é um participante TISAX . . . 21
4.3. Preparação do cadastro . . . 24
4.3.1. A base jurídica . . . 24
4.3.2. O escopo da avaliação TISAX . . . 25
4.3.2.1. Descrição do escopo . . . 26
4.3.2.2. Escopo padrão . . . 26
4.3.2.3. Definição do escopo . . . 27
4.3.2.4. Adaptação do escopo . . . 28
4.3.2.5. Localizações do escopo . . . 30
4.3.2.6. Nome do escopo . . . 33
4.3.2.7. Contatos . . . 34

4.3.2.8. Publicação e compartilhamento . . . 35
4.3.3. Objetivos da avaliação . . . 37
4.3.3.1. Lista dos objetivos da avaliação . . . 38
4.3.3.2. Objetivos da avaliação e a ISA . . . 40
4.3.3.3. Objetivos da avaliação e selos TISAX . . . 40
4.3.3.4. Seleção do objetivo da avaliação . . . 41
4.3.3.5. Necessidades de proteção e os níveis de avaliação . . . 45
4.3.3.6. Objetivos da avaliação e seus próprios fornecedores . . . 50
4.3.4. Taxa . . . 50
4.4. Portal ENX . . . 53
4.5. Processo de cadastro on-line . . . 53
4.5.1. Tempo necessário . . . 53
4.5.2. Comece aqui . . . 53
4.5.3. Conta do portal . . . 53
4.5.4. Cadastro do participante . . . 54
4.5.5. Contato do participante . . . 54
4.5.6. Termos e condições gerais . . . 55
4.5.7. Cadastro do escopo da avaliação . . . 56
4.5.8. E-mail de confirmação . . . 59
4.5.8.1. Participant ID (ID de participante) . . . 60
4.5.8.2. Scope ID (ID do escopo) . . . 61
4.5.9. Informações do status . . . 62
4.5.10. Alterações nas suas informações de cadastro . . . 65
5. Avaliação (Etapa 2) . . . 66
5.1. Visão geral . . . 66
5.2. Autoavaliação baseada na ISA . . . 66
5.2.1. Baixe o documento da ISA . . . 67
5.2.2. Entenda o documento da ISA . . . 67
5.2.2.1. Lista de critérios . . . 67
5.2.2.2. Capítulos . . . 76
5.2.2.3. Perguntas de controle . . . 77
5.2.2.4. Campos do formulário de autoavaliação . . . 77
5.2.2.5. Objetivo . . . 78
5.2.2.6. Requisitos . . . 79
5.2.2.7. Níveis de maturidade . . . 80
5.2.3. Faça a autoavaliação . . . 81
5.2.4. Interprete o resultado da autoavaliação . . . 82

5.2.4.1. Análise . . . 82
5.2.4.2. O nível de maturidade desejado (na pergunta) . . . 86
5.2.4.3. Seu resultado (na pergunta) . . . 86
5.2.4.4. A meta (no nível da pontuação) . . . 89
5.2.4.5. Seu resultado (no nível da pontuação) . . . 91
5.2.4.6. Você está pronto? . . . 92
5.2.5. Abordar o resultado da autoavaliação . . . 94
5.3. Seleção do provedor de auditoria . . . 95
5.3.1. Informações de contato . . . 96
5.3.2. Abrangência . . . 96
5.3.3. Solicitação de propostas . . . 96
5.3.4. Avaliação de propostas . . . 97
5.4. Processo de avaliação TISAX . . . 99
5.4.1. Visão geral . . . 99
5.4.2. Reunião inicial . . . 99
5.4.3. Tipos de avaliação TISAX . . . 100
5.4.4. Elementos da avaliação TISAX . . . 101
5.4.5. Sobre a conformidade . . . 101
5.4.6. Sua preparação para o processo de avaliação TISAX . . . 104
5.4.7. Avaliação inicial . . . 104
5.4.7.1. A primeira reunião formal de abertura . . . 105
5.4.7.2. Procedimento de avaliação . . . 105
5.4.7.3. Reunião de encerramento . . . 105
5.4.7.4. Relatório de avaliação TISAX . . . 105
5.4.8. Preparação do plano de ação corretiva . . . 106
5.4.9. Avaliação do plano de ação corretiva . . . 108
5.4.9.1. Motivos para uma avaliação do plano de ação corretiva . . . 108
5.4.9.2. Combinação com avaliação inicial . . . 108
5.4.9.3. Requisitos do plano de ação corretiva . . . 108
5.4.9.4. Selos TISAX temporários . . . 109
5.4.10. Avaliação de acompanhamento . . . 110
5.4.10.1. Cronograma . . . 110
5.4.10.2. Pré-requisitos . . . 110
5.4.10.3. Vencimento dos selos TISAX temporários . . . 110
5.4.11. Diagrama do processo de avaliação TISAX . . . 111
5.4.12. Assessment ID (ID da avaliação) . . . 114
5.4.13. Relatório de avaliação TISAX . . . 115

5.4.14. Selos TISAX . . . 116
5.4.14.1. Hierarquia dos selos TISAX . . . 117
5.4.14.2. Período de validade dos selos TISAX . . . 118
5.4.14.3. Renovação dos selos TISAX . . . 118
6. Compartilhamento (Etapa 3) . . . 120
6.1. Premissa . . . 120
6.2. A plataforma de compartilhamento . . . 120
6.3. Pré-requisitos gerais . . . 120
6.4. Permanência dos resultados compartilhados . . . 121
6.5. Níveis de compartilhamento . . . 121
6.6. Publique o resultado da sua avaliação na plataforma de compartilhamento . . . 122
6.7. Compartilhar o resultado da sua avaliação com um participante específico . . . 123
6.7.1. Pré-requisitos . . . 124
6.7.2. Como criar uma permissão de compartilhamento . . . 125
6.8. Compartilhamento do resultado da sua avaliação fora do TISAX . . . 126
6.8.1. Os motivos para a regulamentação estrita do mecanismo de compartilhamento . . . 126
6.8.2. Um guia para escrever sobre o TISAX em público . . . 126
6.8.3. Compartilhamento com um parceiro que ainda não é participante TISAX . . . 127
6.8.4. Compartilhamento com funcionários do seu parceiro que não têm acesso direto ao portal ENX . . . 127
7. Anexos . . . 129
7.1. Anexo: Exemplo de nota fiscal . . . 129
7.2. Anexo: Exemplo de e-mail de confirmação . . . 130
7.3. Anexo: Exemplo do extrato do escopo TISAX . . . 131
7.4. Anexo: Participant status (Status do participante) . . . 132
7.4.1. Visão geral: Participant status (Status do participante) . . . 132
7.4.2. Participant status “Incomplete” (Status do participante “Incomplete” (Incompleto)) . . . 134
7.4.3. Participant status “Awaiting approval” (Status do participante “Awaiting approval” (Aguardando aprovação)) . . . 135
7.4.4. Participant status “Preliminary” (Status do participante “Preliminary” (Preliminar) . . . 135
7.4.5. Participant status “Registered” (Status do participante: “Cadastrado”) . . . 137
7.4.6. Participant status “Expired” (Status do participante “Expired” (Vencido)) . . . 138
7.5. Anexo: Assessment scope status (Status do escopo da avaliação) . . . 138
7.5.1. Visão geral: Assessment scope status (Status do escopo da avaliação) . . . 138
7.5.2. Assessment scope status “Incomplete” (Status do escopo da avaliação

"Incomplete" (Incompleto) . . . 140
7.5.3. Assessment scope status "Awaiting your order" (Status do escopo da avaliação "Awaiting your order" (Aguardando seu pedido)) . . . 141
7.5.4. Assessment scope status "Awaiting ENX approval" (Status do escopo da avaliação "Awaiting ENX approval" (Aguardando aprovação da ENX)) . . . 141
7.5.5. Assessment scope status "Awaiting your payment" (Status do escopo da avaliação "Awaiting your payment" (Aguardando seu pagamento)) . . . 142
7.5.6. Assessment scope status "Registered" (Status do escopo de avaliação "Registered" (Cadastrado) . . . 143
7.5.7. Assessment scope status "Active" (Status do escopo da avaliação "Active" (Ativo)) . . . 143
7.5.8. Assessment scope status "Expired" (Status do escopo da avaliação "Expired" (Vencido)) . . . 144
7.6. Anexo: Assessment status (Status da avaliação) . . . 145
7.6.1. Visão geral: Assessment status (Status da avaliação) . . . 145
7.6.2. Assessment status "Initial assessment ordered" (Status da avaliação "Initial assessment ordered" (Avaliação inicial solicitada)) . . . 147
7.6.3. Assessment status "Initial assessment ongoing" (Status da avaliação "Initial assessment ongoing" (Avaliação inicial em andamento)) . . . 147
7.6.4. Assessment status "Waiting for corrective action plan assessment" (Status da avaliação "Waiting for corrective action plan assessment" (Aguardando avaliação do plano de ação corretiva)) . . . 148
7.6.5. Assessment status "Waiting for follow-up" (Status da avaliação "Waiting for follow-up" (Aguardando acompanhamento)) . . . 148
7.6.6. Assessment status "Finished" (Status da avaliação "Finished" (Concluído)) . . . 149
7.7. Anexo: A lógica contra "avaliações prévias" e "análises de lacunas" . . . 149
7.8. Anexo: Escopos personalizados . . . 151
7.8.1. Escopo ampliado personalizado . . . 151
7.8.2. Escopo personalizado completo . . . 151
7.9. Anexo: Gerenciamento do ciclo de vida dos dados do participante . . . 152
7.9.1. Perda de acesso aos dados dos participantes (portal ENX) . . . 152
7.9.2. Administração dos contatos . . . 152
7.9.2.1. Como adicionar um novo contato . . . 152
7.9.2.2. Como excluir os dados de um contato existente . . . 153
7.9.2.3. Como atualizar os dados de um contato existente . . . 154
7.9.3. Administração das localizações . . . 154
7.9.3.1. Como solicitar a mudança do nome da sua empresa . . . 155

7.9.3.2. Como solicitar a mudança de uma localização) . . . 155
7.9.3.3. Como solicitar a mudança do nome da rua . . . 156
7.9.3.4. Como adicionar uma outra localização . . . 157
7.10. Anexo: Avaliação da ampliação do escopo . . . 157
7.11. Anexo: Gerenciamento do ciclo de vida da ISA . . . 158
7.12. Anexo: Documentos úteis . . . 159
7.13. Anexo: Gerenciamento de reclamações . . . 160
7.13.1. Causas para reclamação . . . 160
7.13.1.1. Reclamações sobre a ENX Association . . . 160
7.13.1.2. Reclamações sobre provedores de auditoria . . . 160
7.13.1.3. Requisitos para reclamações . . . 160
7.13.2. Contato para reclamações . . . 161
8. Histórico do documento . . . 162

1. Visão geral

1.1. Finalidade

Bem-vindo ao TISAX, o Trusted Information Security Assessment Exchange.

Um dos seus parceiros solicitou que você comprovasse que o gerenciamento de segurança das suas informações atende a um nível definido de acordo com os requisitos da “Avaliação de Segurança da Informação” (ISA). E agora você deseja saber como atender a esse pedido.

A finalidade desse manual é permitir que você atenda à solicitação do seu parceiro — ou tenha uma vantagem antecipando-a antes que um parceiro a solicite.

Esse manual descreve as etapas que você precisa seguir para passar na avaliação TISAX e para compartilhar o resultado da sua avaliação com seu parceiro.

Estabelecer e manter um sistema de gerenciamento de segurança da informação (SGSI) já é uma tarefa complexa. Provar ao seu parceiro que a gerenciamento de segurança da informação está adequada acrescenta ainda mais complexidade. Esse manual não vai ajudar a gerenciar a segurança da informação. No entanto, o objetivo é facilitar ao máximo o processo de comprovar seus esforços para o parceiro.

1.2. Escopo

Esse manual se aplica a todos os processos TISAX dos quais você possa fazer parte.

Ele contém tudo que você precisa saber para concluir o processo TISAX.

O manual dá alguns conselhos sobre como lidar com os requisitos de segurança da informação no centro da avaliação. Mas não tem como objetivo oferecer uma formação abrangente sobre o que você precisa fazer para ser aprovado na avaliação de segurança da informação.

1.3. Público

O público principal desse manual são as empresas que necessitam ou desejam comprovar um nível definido de gerenciamento de segurança da informação de acordo com os requisitos da “Avaliação de Segurança da Informação” (ISA).

Assim que estiver ativamente envolvido nos processos TISAX, você aproveitará as informações fornecidas nesse manual.

As empresas que solicitam aos seus fornecedores que comprovem níveis definidos de gerenciamento de segurança da informação também serão beneficiadas. Esse manual permite entender o que os seus fornecedores são obrigados a fazer para atender ao seu pedido.

1.4. Estrutura

Começamos com uma breve introdução ao TISAX e depois seguimos imediatamente com instruções sobre COMO fazer as coisas. Você vai encontrar tudo o que precisa para concluir o processo — na ordem em que precisa saber.

O tempo estimado de leitura do documento é de 75 a 90 minutos.

1.5. Como usar este documento

Mais cedo ou mais tarde, você provavelmente vai desejar entender a maior parte do que está descrito neste documento. Para estar devidamente preparado, recomendamos a leitura de todo o manual.

Estruturamos o manual de acordo com as três etapas principais do processo TISAX, para que você possa ir para a seção necessária e ler o restante mais tarde.

O manual usa ilustrações para ajudar a melhorar seu entendimento. As cores nas ilustrações geralmente têm um significado adicional. Portanto, recomendamos a leitura do documento na tela do computador ou em cópia impressa colorida.

Agradecemos seu feedback. Se você achar que algo está faltando nesse manual ou não está fácil de entender, não deixe de em nos informar. Nós e todos os futuros leitores desse manual ficaremos agradecidos pelo seu feedback.

Se você já usou uma versão anterior do manual do participante do TISAX, poderá encontrar algumas observações úteis no final do documento Seção 8, “Histórico do documento”.

1.6. Entre em contato conosco

Estamos aqui para orientar você sobre o processo TISAX e para responder a quaisquer perguntas que você possa ter.

Envie-nos um e-mail para:	tisax@enx.com
Ou ligue para:	+49 69 9866927-77

Você pode entrar em contato conosco durante o horário comercial normal na Alemanha (UTC+01:00).

Todos falamos inglês e alemão. Um dos nossos colegas é um falante nativo de italiano.

Observe Seção 7.13, “Anexo: Gerenciamento de reclamações”.

1.7. Observe o Manual do participante TISAX em outros idiomas e formatos

O manual do participante TISAX está disponível nos seguintes idiomas e formatos:

Idioma	Versão	Formato	Link
Inglês	2.7	On-line	https://www.enx.com/handbook/tisax-participant-handbook.html
		Off-line	https://www.enx.com/handbook/tisax-participant-handbook-offline.html
		PDF	https://www.enx.com/handbook/TISAX%20Participant%20Handbook.pdf

Idioma	Versão	Formato	Link
Alemão	2.7	On-line	https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html
		Off-line	https://www.enx.com/handbook/tisax-teilnehmerhandbuch-offline.html
		PDF	https://www.enx.com/handbook/TISAX-Teilnehmerhandbuch.pdf
Francês	2.7	On-line	https://www.enx.com/handbook/tph-fr.html
		Off-line	https://www.enx.com/handbook/tph-fr-offline.html
		PDF	https://www.enx.com/handbook/tph-fr.pdf
Chinês	2.7	On-line	https://www.enx.com/handbook/tph-cn.html
		Off-line	https://www.enx.com/handbook/tph-cn-offline.html
		PDF	https://www.enx.com/handbook/tph-cn.pdf
Espanhol	2.7	On-line	https://www.enx.com/handbook/tph-es.html
		Off-line	https://www.enx.com/handbook/tph-es-offline.html
		PDF	https://www.enx.com/handbook/tph-es.pdf
Japonês	2.7	On-line	https://www.enx.com/handbook/tph-jp.html
		Off-line	https://www.enx.com/handbook/tph-jp-offline.html
		PDF	https://www.enx.com/handbook/tph-jp.pdf
Português do Brasil	2.7	On-line	https://www.enx.com/handbook/tph-pt.html
		Off-line	https://www.enx.com/handbook/tph-pt-offline.html
		PDF	https://www.enx.com/handbook/tph-pt.pdf
Italiano	2.7	On-line	https://www.enx.com/handbook/tph-it.html
		Off-line	https://www.enx.com/handbook/tph-it-offline.html
		PDF	https://www.enx.com/handbook/tph-it.pdf

Idioma	Versão	Formato	Link
Coreano	2.7	On-line	https://www.enx.com/handbook/tph-kr.html
		Off-line	https://www.enx.com/handbook/tph-kr-offline.html
		PDF	https://www.enx.com/handbook/tph-kr.pdf

Observação importante:

A versão em inglês é a versão principal.
Todos os outros idiomas são traduções da versão em inglês.
Em caso de dúvida, a versão em inglês é a válida.

1.7.1. Sobre a tradução para Português do Brasil

Este Manual do Participante TISAX é uma tradução da versão em inglês.

Todos os documentos relacionados ao TISAX foram elaborados em inglês (por exemplo, todos os contratos e requisitos para provedores de serviços de auditoria do TISAX). Como resultado, seu parceiro ou provedor de auditoria poderá usar alguns dos termos específicos do TISAX em inglês.

Para permitir que você faça um mapeamento, mantivemos o termo TISAX original em inglês na tradução do Manual do Participante TISAX ou o indicamos entre colchetes logo após a tradução.

1.7.2. Sobre o formato on-line

Cada seção tem um ID exclusivo (formato: ID1234).
Um ID se refere a uma seção específica, independentemente do idioma.

Se desejar criar um link para uma seção específica, você poderá:

- clicar com o botão direito no título da seção e copiar o link, ou
- clicar no título da seção e copiar o link da barra de endereço do seu navegador.

A maioria das figuras está disponível em tamanho maior do que o exibido aqui por padrão. Clique na figura para abrir a versão maior.

1.7.3. Sobre o formato off-line

O formato off-line mantém a maioria dos recursos do formato on-line. De forma mais destacada, as figuras estão incorporadas no arquivo HTML. Você precisa apenas de um arquivo para usar o formato off-line.

Comparado ao formato on-line, o formato off-line não inclui:

- as imagens maiores
- as fontes originais do formato on-line
  Os padrões do seu navegador definem as fontes.

1.7.4. Sobre o formato PDF

Se você usar o formato PDF no seu computador, ainda será possível clicar em todas as referências. Mas se você imprimir a versão em PDF, não contará com elementos como números de página e vai precisar pesquisar as referências por conta própria.

2. Introdução

As seções a seguir apresentam o conceito TISAX.

Se você estiver com pressa, poderá pular essa parte e começar imediatamente na Seção 4.3, “Preparação do cadastro”.

2.1. Por que o TISAX?

Ou melhor, por que você está aqui?

Para responder a essa pergunta, vamos começar com algumas considerações sobre como fazer negócios em geral e proteger informações em particular.

Imagine seu parceiro. Ele tem informações confidenciais. Ele deseja compartilhá-las com seu fornecedor — que é você. A cooperação entre você e seu parceiro produz valor. As informações que o seu parceiro compartilha com você são uma parte importante dessa produção de valor. Portanto, ele deseja protegê-las adequadamente. E ele quer ter certeza de que você está tratando as informações dele com o mesmo cuidado.

Mas como ele pode ter certeza de que as informações dele estão em boas mãos? Ele não poderá simplesmente “acreditar” em você. Seu parceiro precisa de alguma prova.

Agora temos duas perguntas. Quem define o que significa o tratamento “seguro” das informações? E a próxima pergunta é: como você prova isso?

2.2. Quem define o que significa "seguro"?

Você e seu parceiro não são os únicos se deparando com essas perguntas pela primeira vez. Quase todos precisam encontrar respostas para elas e a maioria das respostas será semelhante.

Em vez de criar sempre uma solução independente para um problema comum, uma maneira padrão de fazer isso elimina o fardo de criar tudo sempre a partir do zero. Embora definir um padrão seja um esforço enorme, isso é feito somente uma vez e aqueles que o seguem sempre se beneficiam.

Com toda certeza, existem diversas visões sobre o que é o correto a fazer para proteger informações. Mas devido aos benefícios acima mencionados, a maioria das empresas adota padrões. Um padrão é a síntese de todas as melhores práticas comprovadas e consolidadas ao longo do tempo para um determinado desafio.

No seu caso, normas como a ISO/IEC 27001 (sobre sistemas de gerenciamento de segurança da informação, ou SGSI) e a sua implementação estabelecem uma forma de última geração para lidar com informações confidenciais com segurança. Um padrão como esse como este economiza o trabalho de ter de reinventar a roda todas as vezes. Mais importante ainda, os

padrões fornecem uma base comum quando duas empresas precisam compartilhar dados confidenciais.

2.3. O jeito automotivo

Por natureza, os padrões independentes do setor são concebidos como soluções aplicáveis a diversas situações, em vez de adaptados às necessidades específicas das empresas automotivas.

Há muito tempo, o setor automotivo formou associações que visavam, — entre outros objetivos, — refinar e definir padrões que atendessem às suas necessidades mais específicas. A “Verband der Automobilindustrie” (VDA) é uma delas. No grupo de trabalho que trata da segurança da informação, vários integrantes do setor automotivo chegaram à conclusão de que têm necessidades semelhantes para adaptar os padrões de gerenciamento de segurança da informação existentes.

Seus esforços conjuntos levaram a um questionário que abrange os requisitos amplamente aceitos de segurança da informação do setor automotivo. Ele é denominado “Avaliação de Segurança da Informação” (ISA).

Com a ISA, temos agora uma resposta à pergunta “Quem define o que significa “seguro”?” Através da VDA, o próprio setor automotivo oferece essa resposta aos seus integrantes.

2.4. Como comprovar a segurança de forma eficiente?

Enquanto algumas empresas utilizam a ISA apenas para finalidades internas, outras a utilizam para avaliar a maturidade da gerenciamento de segurança da informação dos seus fornecedores. Em alguns casos, uma autoavaliação é suficiente para o relacionamento comercial. No entanto, em determinados casos, as empresas realizam uma avaliação completa da gerenciamento de segurança da informação dos seus fornecedores (incluindo auditorias no local).

Junto com o aumento geral da conscientização sobre a necessidade de gerenciamento de segurança da informação e a crescente adoção da ISA como uma ferramenta para avaliações da segurança da informação, mais fornecedores estavam se deparando com pedidos semelhantes de diferentes parceiros.

Esses parceiros ainda aplicavam padrões diferentes e tinham opiniões diversas sobre como interpretá-los. Mas os fornecedores essencialmente tinham que comprovar as mesmas coisas, apenas de maneiras diferentes.

E quanto mais os fornecedores precisavam comprovar o seu nível de gerenciamento de segurança da informação para os seus parceiros, mais aumentavam as suas reclamações em termos de esforços repetidos. Mostrar a auditor após auditor as mesmas medidas de gerenciamento de segurança da informação simplesmente não é eficiente.

O que pode ser feito para tornar isso mais eficiente? Não seria útil se o relatório de um auditor pudesse ser reutilizado por diversos parceiros?

OEMs e fornecedores do grupo de trabalho da ENX responsável pela manutenção da ISA ouviram as reclamações de seus fornecedores. Agora eles apresentam uma resposta aos seus fornecedores, bem como a todas as outras empresas do setor automotivo, para a pergunta “Como provar a segurança?”

A resposta é TISAX, abreviação de “Trusted Information Security Assessment Exchange” (
“Trusted Information Security Assessment Exchange” (Compartilhamento confiável de avaliação da segurança da informação)).

3. O processo TISAX

3.1. Visão geral

O processo TISAX geralmente[1] começa com um de seus parceiros solicitando que você comprove um nível definido de gerenciamento de segurança da informação de acordo com os requisitos da “Avaliação de Segurança da Informação” (ISA). Para atender a essa solicitação, você deve concluir o processo TISAX de 3 etapas. Esta seção oferece uma visão geral das etapas que você precisa seguir.

O processo TISAX de 3 etapas consiste nas seguintes etapas:

Figura 1. Visão geral do processo TISAX

1. Etapa 1
   Cadastro
2. Etapa 2
   Avaliação
3. Etapa 3
   Compartilhamento

1. Cadastro
   Reunimos informações sobre a sua empresa e sobre o que deve fazer parte da avaliação.
2. Avaliação
   Você passa pela(s) avaliação(ões), que são realizadas por um dos nossos provedores de auditoria TISAX.
3. Compartilhamento
   Você compartilha o resultado da sua avaliação com o seu parceiro.

Cada etapa consiste em subetapas. Elas são apresentadas nas três seções abaixo e descritas em detalhes em suas respectivas seções mais adiante.

Observe:

Embora certamente gostaríamos de dizer quanto tempo levará para receber o resultado da sua avaliação TISAX, pedimos sua compreensão, pois não é possível prever isso de forma confiável. A duração geral do processo TISAX depende de muitos fatores. A grande variedade de tamanhos de empresas e objetivos da avaliação, além do respectivo nível de preparação de um sistema

> de gerenciamento de segurança da informação, impossibilitam essa previsão.

3.2. Cadastro

Sua primeira etapa é o cadastro TISAX.

A principal finalidade do cadastro TISAX é coletar informações sobre sua empresa. Usamos um processo de cadastro on-line para ajudar você a nos fornecer essas informações.

É o pré-requisito para todas as etapas subsequentes. Ele está sujeito a uma taxa.

Durante o processo de cadastro on-line:

- Solicitamos dados de contato e informações de faturamento.
- Você deve aceitar nossos termos e condições.
- Você pode definir o escopo da sua avaliação de segurança da informação.

Para iniciar diretamente com essa etapa, consulte a Seção 4, “Cadastro (Etapa 1)”.

O processo de cadastro on-line é descrito detalhadamente na Seção 4.5, “Processo de cadastro on-line”. Mas se você desejar começar imediatamente, acesse enx.com/en-US/TISAX/.

3.3. Avaliação

A segunda etapa é passar pela avaliação de segurança da informação.

Existem quatro subetapas:

a. Preparação da avaliação
   É necessário se preparar para a avaliação. A abrangência disso está condicionada ao nível atual de maturidade do seu sistema de gerenciamento de segurança da informação. A sua preparação deve ser baseada na lista da ISA.

b. Seleção do provedor de auditoria
   Você deve escolher um de nossos provedores de auditoria TISAX.

c. Avaliação(ões) de segurança da informação
   Seu provedor de auditoria vai realizar a avaliação com base em um escopo da avaliação que corresponda aos requisitos do seu parceiro. O processo de avaliação vai consistir, no mínimo, na auditoria inicial.
   Se a sua empresa não for aprovada imediatamente, o processo de avaliação poderá exigir etapas adicionais.

d. Resultado da avaliação
   Depois da aprovação da sua empresa na avaliação, seu provedor de auditoria fornecerá a você o relatório oficial de avaliação TISAX. O resultado da sua avaliação também receberá

selos TISAX[2].

Para obter mais informações sobre essa etapa, consulte a Seção 5, “Avaliação (Etapa 2)”.

3.4. Compartilhamento

A terceira e última etapa é compartilhar o resultado da avaliação com seu parceiro. O conteúdo do relatório de avaliação da TISAX está estruturado em níveis. Você pode decidir até qual nível seu parceiro terá acesso.

O resultado da sua avaliação é válido por três anos. Supondo que você ainda seja um fornecedor do seu parceiro, você precisará passar pelo processo de três etapas novamente[3].

Para obter mais informações sobre essa etapa, consulte a Seção 6, “Compartilhamento (Etapa 3)”.

Agora que você entende fundamentalmente o que é o processo TISAX, você encontrará instruções sobre como concluir cada etapa nas seções seguintes.

4. Cadastro (Etapa 1)

O tempo estimado de leitura da seção de cadastro é de 30 a 40 minutos.

4.1. Visão geral

O cadastro TISAX é a sua primeira etapa. É o pré-requisito para todas as etapas subsequentes.

As seções a seguir vão orientar você durante o cadastro:

1. Começamos explicando um novo termo essencial.
2. A seguir damos conselhos sobre o que você deve fazer para estar preparado para o processo de cadastro on-line.
3. A seguir, damos orientações sobre o processo de cadastro on-line.

4.2. Você é um participante TISAX

Vamos primeiro apresentar um novo termo que é necessário entender. Até agora, você tem sido o “fornecedor”. Você está aqui para atender a um requisito do seu “cliente”. Entretanto, o TISAX não diferencia realmente essas duas funções. Para o TISAX, todos os cadastrados são “participantes”. Você — e seu parceiro — “participam” do compartilhamento dos resultados da avaliação de segurança da informação.

Figura 2. Cadastre-se para se tornar um participante TISAX

1. Sua empresa
2. Cadastro no processo de avaliação TISAX
3. Participante do processo de avaliação TISAX

Para diferenciar as duas funções desde o início, nos referimos a você, fornecedor, como “participante ativo”. E, nos referimos ao seu parceiro como “participante passivo”. Como “participante ativo”, você é avaliado pelo TISAX e compartilha o resultado da sua avaliação com outros participantes. O “participante passivo” é aquele que solicitou que você fosse avaliado pelo TISAX. O “participante passivo” recebe o resultado da sua avaliação.

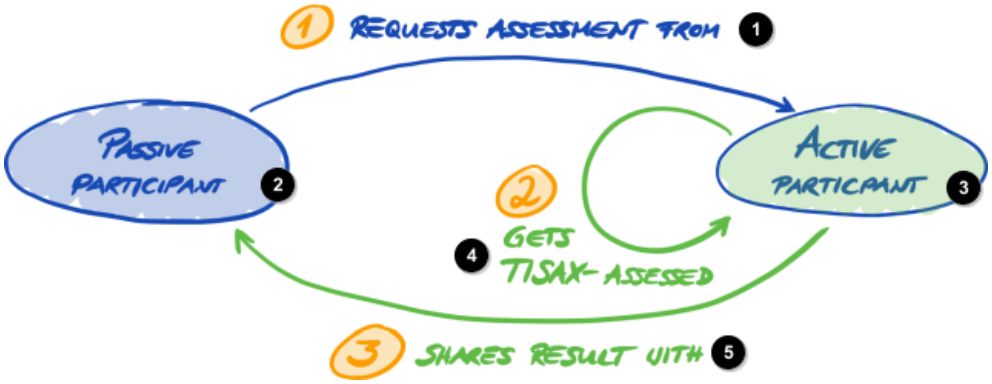


Figura 3. Participante passivo e participante ativo

1. 1 Solicita avaliação de
2. Participante passivo
3. Participante ativo
4. 2 É avaliado pelo TISAX
5. 3 Compartilha resultado com

A empresa pode atuar nas duas funções. Você pode compartilhar o resultado de uma avaliação com seu parceiro e, ao mesmo tempo, solicitar que seus próprios fornecedores sejam avaliados pelo TISAX.

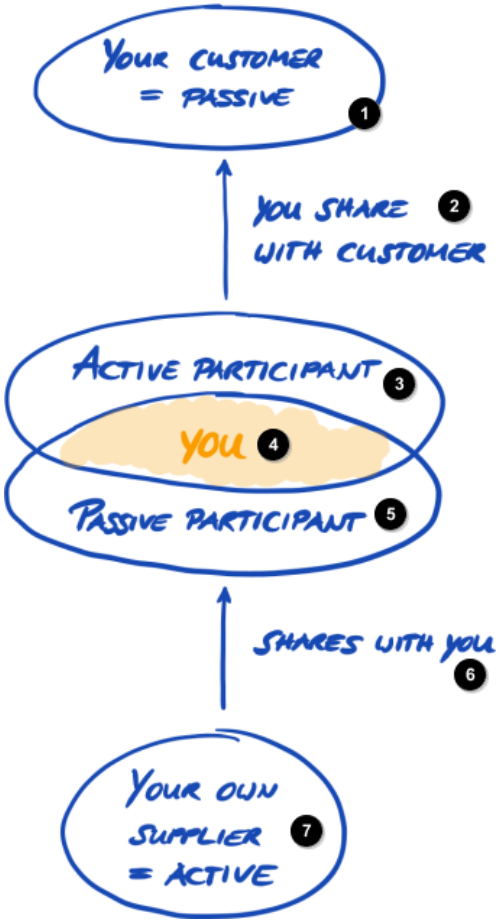


Figura 4. Os participantes TISAX podem ser ativos e passivos ao mesmo tempo

1. Seu cliente
   = passivo
2. Você compartilha com o cliente
3. Participante ativo
4. Você
5. Participante passivo
6. Compartilha com você
7. Seu próprio fornecedor
   = ativo

Solicitar que seus próprios fornecedores sejam avaliados pelo TISAX pode até ser especialmente aconselhável se seus próprios fornecedores também estiverem lidando com as informações de seus parceiros com necessidades de proteção.

4.3. Preparação do cadastro

Nessa seção, damos recomendações sobre como se *preparar* para o cadastro. Descrevemos o processo de cadastro em detalhes na Seção 4.5, “Processo de cadastro on-line”.

Antes de começar a realizar nosso processo de cadastro on-line, recomendamos de forma enfática:

- reunir as informações com antecedência
- e tomar algumas decisões.

4.3.1. A base jurídica

Normalmente, você precisa assinar dois contratos. O primeiro contrato que você assina é entre você e a ENX Association: Os “Termos e Condições Gerais de Participação TISAX” (TCGs do Participante TISAX). O segundo contrato é entre você e um dos nossos provedores de auditoria TISAX. No cadastro, vamos analisar apenas o primeiro contrato.

Os TCGs do Participante TISAX regem o nosso relacionamento mútuo e o seu relacionamento com outros participantes TISAX. Eles definem os direitos e deveres de todos nós. Além das cláusulas usuais que você vai encontrar na maioria dos contratos, eles definem em detalhes o tratamento das informações compartilhadas e obtidas durante o processo TISAX. O objetivo principal dessas regras é manter a confidencialidade dos resultados da avaliação TISAX. Como todos os participantes do TISAX estão sujeitos às mesmas regras, você pode esperar a proteção adequada do resultado da sua avaliação TISAX por parte do seu parceiro (na sua função de participante passivo).

Bem no início do processo de cadastro on-line, vamos solicitar que você aceite os TCGs do Participante TISAX. Por se tratar de um contrato real, recomendamos a leitura dos TCGs do Participante TISAX antes de iniciar o processo de cadastro on-line. Um dos motivos é que, dependendo da sua função na empresa, pode ser necessário obter autorização de um advogado interno ou externo.

Você pode baixar os “Termos e Condições Gerais de Participação TISAX”.[4] em nosso site em:
enx.com/en-US/TISAX/downloads/

Download direto do PDF:
enx.com/tisaxgtcen.pdf

Durante o processo de cadastro on-line, vamos solicitar que você marque duas caixas de seleção obrigatórias:

- ☐ We accept the TISAX Participation General Terms and Conditions (Aceitamos os Termos e Condições Gerais de Participação 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;
(🇵🇹 Confirmamos o conhecimento da liberação do Requerente dos deveres profissionais de sigilo dos Provedores de auditoria de acordo com a Seção IX.5. e X.3 dos Termos e Condições Gerais de Participação TISAX;)

Temos a segunda caixa de seleção porque alguns de nossos provedores de auditoria TISAX são contadores públicos credenciados. Eles têm requisitos específicos em relação ao sigilo profissional. Normalmente, os requisitos específicos em relação ao sigilo profissional proíbem os contadores públicos credenciados dentre os nossos provedores de serviços de auditoria de compartilharem informações conosco. Particularmente, isso comprometeria as opções de controle que precisamos para nossa função de governança. Portanto, precisamos dessa liberação. É aconselhável que você se concentre especialmente nessas cláusulas antes de marcar a caixa.

Se normalmente você precisa de um acordo de não divulgação (NDA) entre você e qualquer pessoa que lide com informações confidenciais, examine as respectivas seções de nossos TCGs. Eles devem abordar todas as suas preocupações. Além disso, normalmente você não precisa nos fornecer nenhuma informação confidencial.

Para concluir a seção jurídica, pedimos a sua compreensão de que o sistema depende de todos aceitarem as mesmas regras. Portanto, não podemos aceitar quaisquer termos e condições gerais adicionais.[5].

4.3.2. O escopo da avaliação TISAX

Na segunda etapa do processo TISAX, um dos nossos provedores de auditoria TISAX vai realizar a avaliação de segurança da informação. Ele precisa saber por onde começar e onde parar. É por isso que você precisa definir um “escopo da avaliação”.

O “escopo da avaliação” descreve o escopo da avaliação da segurança da informação. Em termos simples, todas as partes da sua empresa que lidam com as informações confidenciais do seu parceiro fazem parte do escopo da avaliação. Você pode considerá-lo um elemento importante da descrição da tarefa do provedor de auditoria. Ele determina o que o provedor de auditoria precisa avaliar.

O escopo da avaliação é importante por dois motivos:

a. O resultado de uma avaliação só vai atender aos requisitos do seu parceiro se o respectivo escopo da avaliação abranger todas as partes da sua empresa que lidam com as informações do parceiro.
b. Um escopo da avaliação definido com precisão é um pré-requisito essencial para cálculos de custos significativos por parte de nossos provedores de auditoria TISAX.

Observação importante:

ISO/IEC 27001 vs. TISAX

Primeiro, precisamos diferenciar dois tipos de escopos:
1) o escopo do seu sistema de gerenciamento de segurança da informação (SGSI) e
2) o escopo da avaliação.
Os dois não são necessariamente idênticos.

Para a certificação ISO/IEC 27001, você define o escopo do seu SGSI (na "declaração do escopo"). Você é totalmente livre para definir o escopo do seu SGSI. No entanto, o escopo da avaliação (também conhecido como "escopo da auditoria") deve ser idêntico ao escopo do seu SGSI.

Para o TISAX, você também deve definir seu SGSI. Mas o escopo da avaliação pode ser diferente.

Para a certificação ISO/IEC 27001, você pode configurar livremente o escopo da avaliação através da forma como define o escopo do seu SGSI.

Em contrapartida, para o TISAX, o escopo da avaliação é predefinido. O escopo da avaliação pode ser menor que o escopo do seu SGSI. Mas deve estar dentro do escopo do seu SGSI.

4.3.2.1. Descrição do escopo

A descrição do escopo define o escopo da avaliação. Na descrição do escopo, você deve escolher um dos dois tipos de escopo:

1. Standard scope (Escopo padrão)
2. Custom scope (Escopo personalizado)
    a. Custom extended scope (Escopo ampliado personalizado)
    b. Full custom scope (Escopo personalizado completo)

Vamos discutir o escopo padrão na próxima seção. O escopo padrão é a opção certa para mais de 99% de todos os participantes. Portanto, vamos discutir apenas os escopos personalizados na Seção 7.8, "Anexo: Escopos personalizados".

4.3.2.2. Escopo padrão

A descrição do escopo padrão é a base para uma avaliação TISAX. Outros participantes TISAX aceitam apenas resultados de avaliação baseados na descrição do escopo padrão.

A descrição do escopo padrão é predefinida e não é possível alterá-la.

Um benefício importante de um escopo padrão é que você não precisa criar sua própria

definição.

Essa é a descrição do escopo padrão (versão 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.
```

```
O escopo da avaliação TISAX define o
escopo da avaliação. A avaliação
inclui todos os processos,
procedimentos e recursos sob a
responsabilidade da organização
avaliada que são relevantes para a
segurança dos objetos de proteção e
seus objetivos de proteção, conforme
definido nos objetivos da avaliação
listados nas localizações listadas.
A avaliação é realizada pelo menos no
nível de avaliação mais elevado
listado em qualquer um dos objetivos
da avaliação listados. Todos os
critérios da avaliação listados nos
objetivos da avaliação listados estão
sujeitos à avaliação.
```

Recomendamos de forma enfática a escolha do escopo padrão. Todos os participantes TISAX aceitam os resultados da avaliação de segurança da informação com base no escopo padrão.

4.3.2.3. Definição do escopo

Sua próxima tarefa após a definição do tipo de escopo é decidir quais localizações pertencem ao escopo da avaliação.

Se a sua empresa for pequena (uma localização), a tarefa é fácil. Basta adicionar sua localização ao escopo da avaliação.

Se a sua empresa for grande, considere cadastrar mais de um escopo da avaliação.

Ter um único escopo contendo todas as suas localizações tem vantagens:

- Você tem um relatório de avaliação, um resultado da avaliação, uma data de validade.
- Você pode se beneficiar de custos reduzidos para a avaliação porque um provedor de auditoria TISAX só precisa avaliar seus processos, procedimentos e recursos centrais uma vez.

Mas um único escopo pode ter desvantagens como:

- Todas as localizações devem ter os mesmos objetivos da avaliação.
- O resultado da avaliação só estará disponível depois que o provedor de auditoria TISAX tiver avaliado todas as localizações. Esse fato pode ser relevante se você precisar urgentemente de um resultado da avaliação.
- O resultado da avaliação depende de todas as localizações que passarem na avaliação. Se houver erro em apenas uma localização, você não terá um resultado da avaliação positivo. Uma solução alternativa para isso é: a) remover a localização do escopo, b) resolver os problemas, c) adicionar a localização posteriormente com uma avaliação da ampliação do escopo.

4.3.2.4. Adaptação do escopo

A dúvida sobre se deve haver apenas um escopo ou vários escopos é algo que somente você pode decidir. Mas responder às perguntas do diagrama a seguir pode ajudar na decisão.

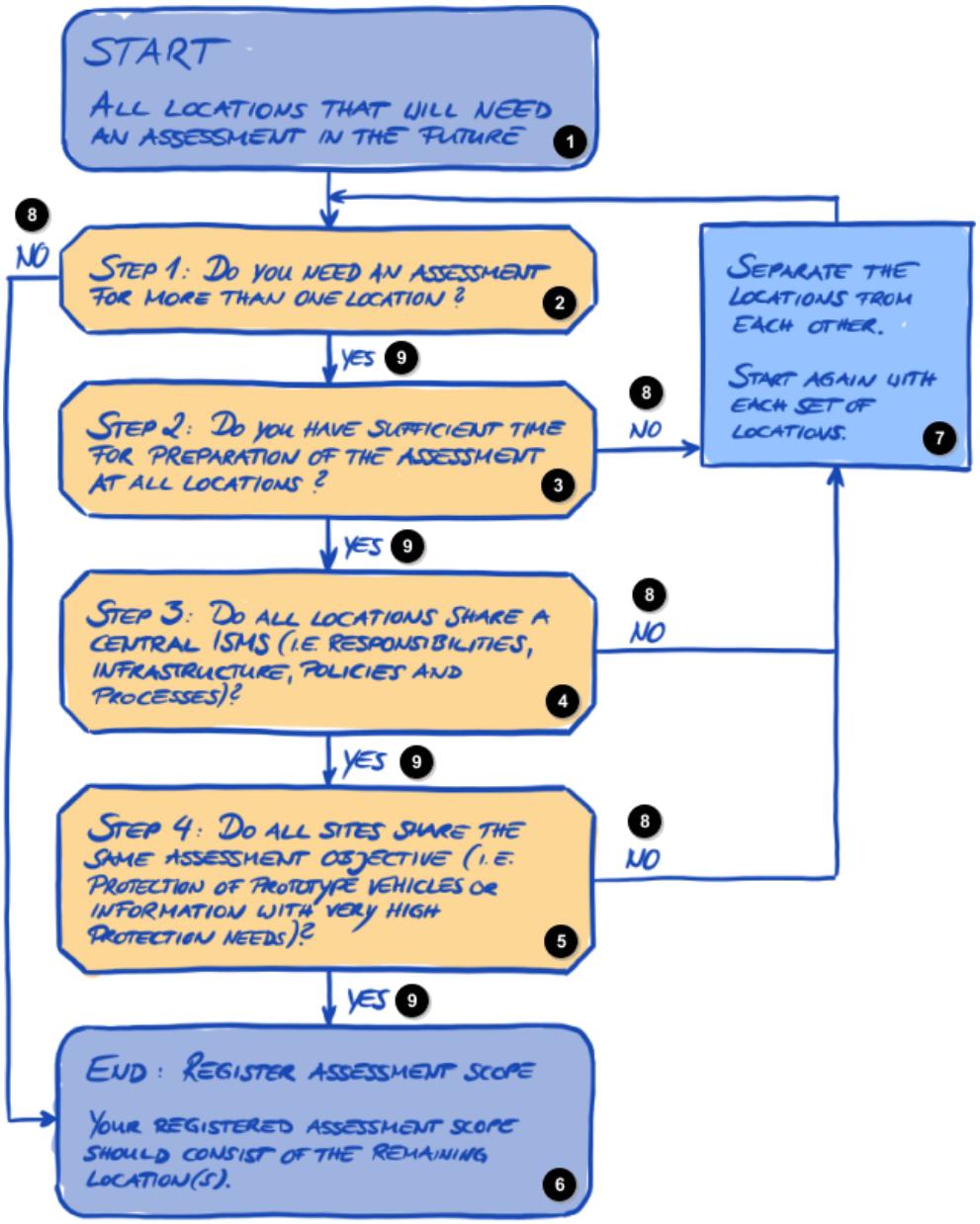


Figura 5. Árvore de decisão de adaptação do escopo

1. INÍCIO
   Todas as localizações que vão precisar de uma avaliação no futuro
2. Etapa 1: você precisa de uma avaliação para mais de uma localização?
3. Etapa 2: você tem tempo suficiente para se preparar para a avaliação em todas as localizações?
4. Etapa 3: todas as localizações compartilham um SGSI central (ou seja, responsabilidades, infraestrutura, políticas e processos)?
5. Etapa 4: todas as localizações compartilham o mesmo objetivo da avaliação (ou seja, proteção de protótipos de veículos ou informações com necessidades de proteção muito elevadas)?

6. Final: cadastrar o escopo da avaliação
   O escopo da avaliação cadastrada deve abranger as localizações restantes.
7. Separe as localizações umas das outras.
   Comece novamente com cada conjunto de localizações.
8. Não
9. Sim

Observe:

Não deixe essa decisão intimidar você. Você pode alterar qualquer escopo, desde que o provedor de auditoria não tenha concluído a avaliação.

Por exemplo, durante a preparação da sua avaliação você pode descobrir que o escopo não se enquadra em — e alterá-lo conforme necessário. Ou o seu provedor de auditoria pode recomendar a alteração do escopo durante as etapas iniciais da avaliação.

Observações adicionais:

- Tecnicamente, você não pode alterar o escopo da avaliação definido durante o processo de cadastro on-line no portal ENX. Mas o provedor de auditoria pode atualizar o escopo da sua avaliação ao carregar o resultado da sua avaliação no portal ENX.
- Adicionar itens ao escopo aumenta a taxa e você não receberá reembolso se remover localizações do escopo. Como os provedores de auditoria usam o escopo original como base para o cálculo de custos, você também deve esperar alterações.

4.3.2.5. Localizações do escopo

Agora que você decidiu quais localizações fazem parte do escopo da sua avaliação, é possível continuar coletando algumas informações específicas da localização.

Para cada localização solicitamos informações como nome e endereço da empresa. Solicitamos também algumas informações adicionais que permitam aos nossos provedores de auditoria TISAX ter uma ideia melhor da estrutura da sua empresa. Suas respostas serão usadas como base para as estimativas de esforço deles.

Prepare-se para fornecer os seguintes dados para cada uma das suas localizações (o asterisco vermelho * indica informações obrigatórias no processo on-line):

Campo	Opções
Nome da localização *	N/A
NÚMERO D-U-N-S da D&B	N/A
Tipo da localização *	Edifício(s) pertencente(s) e utilizado(s) exclusivamente pela empresa Edifício(s) alugado(s) pela empresa Andar/escritório alugado pela empresa em edifício compartilhado Escritório compartilhado com outras empresas Centro de dados próprio Centro de dados compartilhado
Proteção passiva do local *	Sim Não
Indústria *(Possibilidade de várias seleções)*	Tecnologia da Informação ☐ Serviços de TI ☐ Serviços de telecomunicações ☐ Desenvolvimento de software
	Gerenciamento ☐ Consultoria
	Mídia ☐ Marketing ☐ Agência ☐ Serviços de impressão ☐ Fotografia ☐ Serviços de tradução
	Pesquisa e Desenvolvimento ☐ Testes de veículos ☐ Simulação de veículos ☐ Criação de protótipo ☐ Modelos de carros em miniatura ☐ Serviços de desenvolvimento ☐ Serviços de desenvolvimento CAx

Campo	Opções
	Produção • Serviços de produção • Fabricação por contrato • Chão de fábrica • Logística
	Vendas e pós-venda • Importação, NSC • Concessionária • Serviços financeiros • Seguros • Liquidação de sinistros
	Outra indústria *(digite)*
Funcionários na localização: Geral *	0 1–10 11–100 101–1.000 1.001–5.000 Mais de 5.000
Funcionários na localização: TI *	0 1–10 11–25 26–50 Mais de 50
Funcionários na localização: Segurança de TI *	0 Meio período 1–5 6–25 Mais de 25
Funcionários na localização: Segurança da localização *	0 Meio período 1–3 4–10 Mais de 10

Campo	Opções
Certificações para essa localização	ISO 27001 Outra *(digite)* ISAE 3402 SOC2

Tabela 1. Dados específicos da localização

Observe:

Em relação ao “Setor”: Selecione de acordo com seu melhor conhecimento. Não há resposta certa ou errada ao selecionar uma das opções acima. Se não encontrar uma opção que corresponda ao seu tipo de negócio, basta inserir a opção adequada em “Outro”.

Para cada localização você deve especificar um “location name” (“nome da localização”). A finalidade do nome da localização é facilitar a referência à mesma ao atribuí-lo a um escopo da avaliação.

Recomendamos a atribuição dos nomes das localizações com base no seguinte padrão:

Padrão: [Referência geográfica]

Exemplo: para a empresa fictícia “ACME”

- Frankfurt
  (para uma localização na **cidade** alemã Frankfurt)

4.3.2.6. Nome do escopo

Para cada escopo você deve especificar um “scope name” (“nome do escopo”). A finalidade principal do nome do escopo é facilitar a identificação de um escopo na lista de visão geral de escopos no portal ENX. Você deve atribuir um nome que seja útil para o leitor e seus colegas. Para a comunicação externa, você deve usar o ID do escopo.

Você pode especificar qualquer nome que desejar. Mas não deve atribuir o mesmo nome de escopo para mais de um escopo.

Mais tarde, quando você quiser renovar sua avaliação TISAX, será necessário criar um novo escopo (possivelmente idêntico ao escopo atual). Portanto, recomendamos adicionar o ano da avaliação ao nome do escopo.

Recomendamos a atribuição dos nomes das escopos com base no seguinte padrão:

Padrão: [Referência geográfica ou *funcional*] [Ano da avaliação]

Exemplos: para a empresa fictícia “ACME”

- 2024
  (sem referência geográfica se sua empresa tiver apenas uma localização)
- Frankfurt 2024
  (para um escopo com várias localizações na **cidade** alemã Frankfurt)
- Baixa Saxônia 2024
  (para um escopo com todas as localizações no **estado** alemão Baixa Saxônia)
- Alemanha 2024
  (para um escopo com todas as localizações no **país** Alemanha)
- EMEA 2024
  (para um escopo com todas as localizações na **região** EMEA (“Europa, Oriente Médio, África”))
- Desenvolvimento de protótipo 2024
  (referência *funcional* para um escopo com todas as localizações envolvidas no desenvolvimento de protótipos)

4.3.2.7. Contatos

Para nos comunicarmos com você, coletamos informações sobre os contatos da sua empresa.

Solicitamos pelo menos um contato da sua empresa como participante TISAX em geral e um para cada escopo da avaliação. Você tem a opção de fornecer contatos adicionais.

Durante os preparativos para o cadastro, você deve decidir quem será o contato na sua empresa.

Solicitamos os seguintes dados do contato:

	Dado do contato	**Obrigatório?**	**Exemplo**
1.	Cumprimentos	Sim	Sra., Sr.
2.	Título acadêmico		Dr., Ph.D., outro
3.	Nome	Sim	John
4.	Sobrenome	Sim	Doe
5.	Cargo	Sim	Chefe do departamento
6.	de TI	Sim	Tecnologia da Informação

	Dado do contato	Obrigatório?	Exemplo
7.	Telefone principal	Sim	+49 69 986692777
8.	Telefone secundário		
9.	Endereço de e-mail	Sim	john.doe@acme.com
10.	Idioma preferido	Sim	Inglês (padrão)
11.	Outros idiomas		Alemão, francês
12.	Identificador de endereço pessoal		HPC 1234
13.	Endereço	Sim	Bockenheimer Landstraße 97-99
14.	CEP	Sim	60325
15.	Cidade	Sim	Frankfurt
16.	Estado/Província		
17.	País	Sim	Alemanha

Tabela 2. Dados do contato

Observação importante:

Recomendamos a atribuição de pelo menos um substituto para cada contato. Se um contato estiver temporariamente indisponível ou sair da empresa, outra pessoa poderá gerenciar os dados dos participantes da sua empresa.
Se precisar fazer a atribuição de um novo contato (na ausência de outros contatos válidos), você precisará passar por um processo complexo. Nosso processo garante que somente pessoas que possam provar que têm o direito de representar legalmente a empresa possam aprovar a atribuição de um novo contato principal.

4.3.2.8. Publicação e compartilhamento

A finalidade principal do TISAX é publicar o resultado da sua avaliação para outros participantes TISAX e compartilhar o resultado da sua avaliação com seu(s) parceiro(s).

Você pode decidir sobre a publicação e compartilhamento do resultado da sua avaliação durante o processo de cadastro ou a qualquer momento posteriormente.

Se você estiver passando pelo processo TISAX como uma etapa preventiva, já poderá decidir publicar o resultado da sua avaliação para a comunidade de participantes TISAX. Caso contrário, não há nada a ser preparado nesta fase.

Se seu parceiro solicitou que você passasse pelo processo TISAX, você vai precisar compartilhar o resultado da sua avaliação mais cedo ou mais tarde. Você já pode compartilhar as informações

do status com seu parceiro durante o cadastro. Assim que o resultado da sua avaliação estiver disponível, seu parceiro terá automaticamente permissão para acessá-lo.[6].

Existem duas coisas necessárias para compartilhar as informações do status:

1. ID de participante TISAX do seu parceiro

   O ID de participante TISAX identifica seu parceiro como participante TISAX.

   Normalmente, seu parceiro deve fornecer a você seu ID de participante TISAX.

   Para sua conveniência, nosso formulário de cadastro fornece uma lista suspensa de IDs de participantes para algumas empresas que frequentemente recebem resultados de avaliações compartilhadas.[7]

2. O nível de compartilhamento necessário

   O nível de compartilhamento define o grau de acesso do seu parceiro aos resultados da sua avaliação.

   Seu parceiro solicitar um nível de compartilhamento específico ou você decidir até qual nível deseja conceder acesso ao resultado da avaliação ao seu parceiro.

   Para obter mais informações sobre os níveis de compartilhamento, consulte Seção 6.5, “Níveis de compartilhamento”.

Portanto, você pode querer garantir a posse dessas informações.

Observe:

- Você sempre pode decidir publicar o resultado da sua avaliação posteriormente.
- Você pode criar uma permissão de compartilhamento para seu parceiro posteriormente.

Observação importante:

Se você não publicar ou compartilhar o resultado da sua avaliação, ninguém poderá ver o seu resultado.

Observação importante:

Você não pode revogar a publicação ou o compartilhamento.

Para obter detalhes, consulte Seção 6.4, “Permanência dos resultados

compartilhados”.

Observe:

Pode parecer estranho, mas na verdade você pode compartilhar o “resultado da avaliação” mesmo que ainda não tenha iniciado o processo de avaliação. Nessa fase inicial, você está apenas compartilhando o “status da avaliação”. O participante com quem você compartilha o “resultado da avaliação” verá onde você está no processo de avaliação.

Alguns participantes TISAX precisam emitir uma autorização especial se você precisar mostrar os selos TISAX, mas ainda não concluiu o processo de avaliação. Nesse caso, seu parceiro pode precisar ver seu “status da avaliação” em sua conta no portal ENX.

Para obter mais informações sobre o status da avaliação, consulte Seção 7.6, “Anexo: Assessment status (Status da avaliação)”.

Para obter mais informações sobre como publicar e compartilhar o resultado da sua avaliação, consulte Seção 6, “Compartilhamento (Etapa 3)”.

4.3.3. Objetivos da avaliação

Você precisa definir seu(s) objetivo(s) da avaliação durante o processo de cadastro. O objetivo da avaliação (assessment objective) determina os requisitos aplicáveis que seu sistema de gerenciamento de segurança da informação (SGSI) deve cumprir. O objetivo da avaliação é inteiramente baseado no tipo de dados que você trata em nome do seu parceiro.

Nas seções a seguir, descrevemos os objetivos da avaliação e damos conselhos sobre como selecionar o(s) objetivo(s) correto(s) da avaliação.

O uso dos objetivos da avaliação facilita a comunicação relacionada ao TISAX com seu parceiro e nossos provedores de auditoria TISAX, porque eles se referem a uma entrada definida para o processo de avaliação TISAX.

Observe:

Alguns parceiros podem solicitar que sua avaliação pelo TISAX seja com um determinado “nível de avaliação” (AL) em vez de especificar um objetivo da avaliação.

Para obter mais informações sobre os níveis de avaliação, consulte a Seção 4.3.3.5, “Necessidades de proteção e os níveis de avaliação” (subseção “Additional information” (Informações adicionais)).

4.3.3.1. Lista dos objetivos da avaliação

Atualmente existem doze objetivos da avaliação TISAX. Você deve selecionar pelo menos um objetivo da avaliação. Você pode selecionar mais de um.

Considere o seu objetivo da avaliação como referência para o seu sistema de gerenciamento de segurança da informação. O objetivo da avaliação é uma entrada essencial para o processo TISAX. Todos os provedores de auditoria TISAX baseiam a sua estratégia de avaliação principalmente no objetivo da avaliação.

Os objetivos atuais da avaliação TISAX são:

N.º	Nome	Descrição
1.	Info high	Handling of information with high protection needs Tratamento de informações com necessidades de proteção elevadas
2.	Info very high	Handling of information with very high protection needs Tratamento de informações com necessidades de proteção muito elevadas
3.	Confidential	Handling of information with high protection needs in the context of confidentiality (access to confidential information) Tratamento de informações com necessidades de proteção elevadas em relação à confidencialidade (acesso a informações confidenciais)
4.	Strictly confidential	Handling of information with very high protection needs in the context of confidentiality (access to strictly confidential information) Tratamento de informações com necessidades de proteção muito elevadas em relação à confidencialidade (acesso a informações confidenciais)
5.	High availability	Handling of information with high protection needs in the context of *availability* (high availability of information) Tratamento de informações com necessidades de proteção elevadas em relação à *disponibilidade* (disponibilidade elevada de informações)

N.º	Nome	Descrição
6.	Very high availability	Handling of information with very high protection needs in the context of *availability* (very high availability of information) Tratamento de informações com necessidades de proteção muito elevadas em relação à *disponibilidade* (disponibilidade muito elevada de informações)
7.	Proto parts	Protection of Prototype Parts and Components Proteção das peças e componentes do protótipo
8.	Proto vehicles	Protection of Prototype Vehicles Proteção de protótipos de veículos
9.	Test vehicles	Handling of Test Vehicles Tratamento de veículos de teste
10.	Proto events	Protection of Prototypes during Events and Film or Photo Shoots Proteção de protótipos durante eventos e sessões de filmes ou fotos
11.	Data	Data protection according to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR) Proteção de dados de acordo com o Artigo 28 (“Processador”) do Regulamento Geral sobre a Proteção de Dados (RGPD) (UE)
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 Proteção de dados de acordo com o Artigo 28 (“Processador”) do Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) com categorias especiais de dados pessoais, conforme especificado no Artigo 9 do RGPD

Tabela 3. Objetivos atuais da avaliação TISAX:

Exemplo: se você estiver realizando test drives em vias públicas, então o objetivo da avaliação “Test vehicles” é um dos seus objetivos da avaliação.

Observe:

É possível selecionar os objetivos da avaliação “Info high” e “Info very high” somente até 31 de março de 2024.

É possível selecionar os objetivos da avaliação “Confidential” e “Strictly confidential” a partir de 1º de abril de 2024.

Para obter mais informações sobre essa transição, consulte o seguinte artigo de notícias em nosso site:
CHANGES TO TISAX LABELS ACCOMPANYING ISA 6 RELEASE
enx.com/en-US/news/Changes-to-TISAX-Labels-ISA-six-Release/

Observação importante:

No TISAX, o “objetivo da avaliação” é geralmente a entrada do processo. No entanto, alguns parceiros podem solicitar que sua avaliação pelo TISAX seja com um determinado “nível de avaliação” (AL).

Para obter mais informações sobre a relação entre as necessidades de proteção e os níveis de avaliação, consulte a Seção 4.3.3.5, “Necessidades de proteção e os níveis de avaliação”.

4.3.3.2. Objetivos da avaliação e a ISA

A ISA contém três listas de critérios (segurança da informação, proteção de protótipos, proteção de dados). Cada lista de critérios é composta pelas denominadas “perguntas de controle” e requisitos associados.

Cada objetivo da avaliação define:

- a(s) lista(s) de critérios da ISA aplicáveis
- as perguntas de controle que você deve responder
- os requisitos que você deve cumprir

Para alguns objetivos da avaliação, apenas um subconjunto de perguntas e requisitos de controle é aplicável.

Para obter mais informações básicas sobre os objetivos da avaliação TISAX e as perguntas e requisitos de controle aplicáveis, consulte a Seção 5.2.2, “Entenda o documento da ISA”.

4.3.3.3. Objetivos da avaliação e selos TISAX

Seu parceiro pode falar sobre “selos TISAX”. Os “objetivos da avaliação” e os “selos TISAX” são quase idênticos. A diferença é que você inicia o processo de avaliação com os “objetivos da avaliação” e se for aprovado na avaliação recebe os “selos TISAX” correspondentes.

Exemplo: seu parceiro exige que você obtenha o selo TISAX “Info high”. Em seguida, você seleciona o “Info high” como o seu objetivo da avaliação.

A figura abaixo mostra a entrada e a saída do processo TISAX:

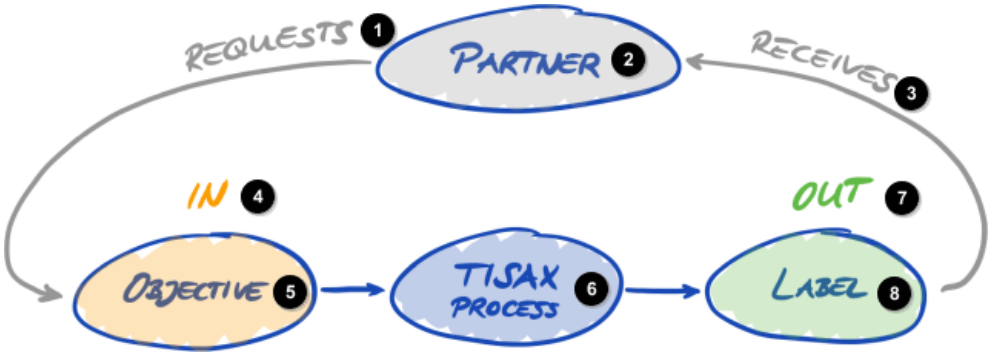


Figura 6. Objetivos da avaliação e selos TISAX

1. Solicita
2. Parceiro
3. Recebe
4. ENTRADA
5. Objetivo
6. Processo TISAX
7. SAÍDA
8. Selo

Para obter mais informações sobre os selos TISAX, consulte Seção 5.4.14, “Selos TISAX”.

4.3.3.4. Seleção do objetivo da avaliação

Teoricamente, o seu parceiro dirá precisamente quais objetivos da avaliação você deve alcançar.

Você deve selecionar o objetivo da avaliação com base no seu próprio discernimento se:

a. você desejar ser avaliado pelo TISAX antes da solicitação de um parceiro, ou

b. seu parceiro não especificar qual objetivo da avaliação que você deve alcançar.

Observação importante:

Nesse item, recomendamos de forma enfática considerar seus outros parceiros. Já existem parceiros com requisitos iguais ou superiores? Você espera que futuros parceiros tenham requisitos mais elevados?

Você pode optar por selecionar objetivos da avaliação que tenham

> necessidades de proteção mais elevadas. Isso evita problemas quando outros parceiros têm requisitos mais elevados.

Se precisar selecionar o objetivo da avaliação com base no seu próprio discernimento, pode ser útil considerar os seguintes aspectos:

N.º	Objetivo da avaliação	Informações
1.	Info high	É possível determinar as necessidades de proteção (elevadas, muito elevadas) com base na classificação de documentos do seu parceiro.
2.	Info very high	
3.	Confidential	Para todas as empresas que recebem e processam informações com alta necessidade de proteção no contexto da confidencialidade ou que são tipicamente classificadas como confidenciais de acordo com o esquema de classificação da própria empresa (por exemplo, o artigo técnico da VDA “Harmonization of classification levels” (Harmonização dos níveis de classificação)). Você deve selecionar esse selo TISAX principalmente se a divulgação não autorizada das informações puder potencialmente causar danos consideráveis (por exemplo, danos à reputação, consequências criminais ou prejuízos financeiros).
4.	Strictly confidential	Para todas as empresas que recebem e processam informações com necessidade muito alta de proteção no contexto da confidencialidade ou que são tipicamente classificadas como estritamente confidenciais ou secretas de acordo com o esquema de classificação da própria empresa (por exemplo, o artigo técnico da VDA “Harmonization of classification levels” (Harmonização dos níveis de classificação)). Você deve selecionar esse selo TISAX principalmente se a divulgação não autorizada das informações puder potencialmente causar danos existenciais ameaçadores ou catastróficos (por exemplo, danos graves à reputação, consequências criminais graves ou prejuízos financeiros muito altos).

N.º	Objetivo da avaliação	Informações
5.	High availability	Para todas as empresas em que a capacidade dos clientes de produzir ou entregar depende da disponibilidade dos produtos ou serviços das empresas, e onde uma falha causaria danos consideráveis aos clientes em um período curto. Exemplo: fornecedores do tipo just-in-time de materiais de produção
6.	Very high availability	Para todas as empresas em que a capacidade dos clientes de produzir e entregar depende da disponibilidade a curto prazo dos produtos e serviços das empresas, e onde uma falha causaria danos consideravelmente altos aos clientes em um prazo muito curto. Exemplo: fornecedores do tipo just-in-time onde uma falha pode resultar em uma paralisação abrangente da produção com um tempo de reinício muito longo em um curto período de tempo.
7.	Proto parts	Para todas as empresas que fabricam, armazenam ou utilizam componentes ou peças fornecidos pelo cliente e que foram classificados como necessitando de proteção em suas próprias localizações. Os requisitos de segurança física e de segurança considerando a área circundante, os requisitos organizacionais e os requisitos específicos para o tratamento de protótipos fazem parte da avaliação.
8.	Proto vehicles	Para todas as empresas que fabricam, armazenam ou utilizam veículos fornecidos pelo cliente e que foram classificados como necessitando de proteção em suas próprias localizações. Os requisitos de segurança física e de segurança considerando a área circundante (incluindo a existência de garagens protegidas e áreas de oficinas), os requisitos organizacionais e os requisitos específicos para o tratamento de protótipos fazem parte da avaliação. Após uma avaliação bem-sucedida, você recebe automaticamente o selo TISAX “Proteção de peças e componentes de protótipos”.

N.º	Objetivo da avaliação	Informações
9.	Test vehicles	Para todas as empresas que realizam testes e test drives (tais como test drives em vias públicas ou pistas de teste) com veículos fornecidos pelo cliente que foram classificados como necessitando de proteção. Requisitos organizacionais, requisitos específicos para o tratamento de protótipos, incl. camuflagem e tratamento de veículos durante test drives em público e em pistas de teste fazem parte da avaliação. Os requisitos de segurança física e de segurança considerando a área circundante, não são necessariamente parte da avaliação. Se as suas localizações estiverem equipadas adequadamente, recomendamos selecionar também o objetivo da avaliação “Proteção de protótipos de veículos”.
10.	Proto events	Para todas as empresas que realizam apresentações ou eventos (por exemplo, pesquisas de mercado, eventos, eventos de marketing) e filmagens e sessões de fotos com veículos, componentes ou peças fornecidos pelo cliente que foram classificados como necessitando de proteção. Os requisitos organizacionais e requisitos específicos para o tratamento de protótipos, incl. os requisitos para apresentações, eventos e sessões de filmes e fotos em salas protegidas e em público fazem parte da avaliação. Os requisitos de segurança física e de segurança considerando a área circundante, não são necessariamente parte da avaliação. Se as suas localizações estiverem equipadas adequadamente, recomendamos selecionar também o objetivo da avaliação “Proteção de protótipos de veículos”.
11.	Data	Se você lida com dados pessoais como processador de acordo com o Artigo 28 do RGPD, provavelmente precisará selecionar “Data”.

N.º	Objetivo da avaliação	Informações
12.	Special data	Se você lida com categorias especiais de dados pessoais (como saúde ou religião) como processador de acordo com o Artigo 28 do RGPD, provavelmente precisará selecionar “Special data”.

Tabela 4. Conselhos para selecionar um objetivo da avaliação.

Outras explicações:

- Se você tiver os requisitos precisos do seu parceiro, normalmente não será necessário discutir os objetivos da avaliação com ele. No entanto, se você não tiver os requisitos precisos do seu parceiro, recomendamos de forma enfática que consulte o seu parceiro antes de iniciar o processo de avaliação.
- A ISA descreve a diferença de implementação entre necessidades de proteção “elevadas” e “muito elevadas” (se houver) para cada requisito.
  Para obter mais informações sobre isso, consulte Figura 11, “Captura de tela: principais elementos das perguntas da lista de critérios da ISA “Segurança da informação””.

4.3.3.5. Necessidades de proteção e os níveis de avaliação

Seu parceiro tem vários tipos de informações, algumas das quais podem merecer um nível de proteção mais elevado do que outras. A ISA aborda isso classificando três “necessidades de proteção” (🇬🇧 “protection needs”normal, elevada e muito elevada). Seu parceiro classifica suas informações e normalmente atribui necessidades de proteção.

Quanto maiores as necessidades de proteção, mais o seu parceiro estará interessado em garantir se é seguro permitir que você processe as informações dele. Portanto, o TISAX diferencia três “níveis de avaliação” (AL). O nível de avaliação define qual método de avaliação o provedor de auditoria deve aplicar. Um nível de avaliação mais alto aumenta o esforço investido na avaliação. Isso resulta em maior cuidado e precisão na avaliação.

A tabela abaixo mostra os níveis da avaliação que se aplicam aos objetivos da avaliação TISAX:

N.º	Objetivo da avaliação TISAX	Nível de avaliação (AL)
1.	Info high	AL 2
2.	Info very high	AL 3
3.	Confidential	AL 2
4.	Strictly confidential	AL 3
5.	High availability	AL 2
6.	Very high availability	AL 3

N.º	Objetivo da avaliação TISAX	Nível de avaliação (AL)
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

Tabela 5. Mapeamento dos objetivos da avaliação TISAX para os níveis da avaliação

Nível de avaliação 1 (AL 1):

As avaliações no nível de avaliação 1 são principalmente para finalidades internas, no verdadeiro sentido de uma autoavaliação (self-assessment).

Para uma avaliação no nível de avaliação 1, um auditor verifica a existência de uma autoavaliação concluída. Ele não avalia o conteúdo da autoavaliação. Ele não exige mais evidências.

Os resultados das avaliações no nível de avaliação 1 têm um baixo nível de confiança e, portanto, não são utilizados no TISAX. Mas é claro que é possível que o seu parceiro solicite essa autoavaliação fora do TISAX.

Nível de avaliação 2 (AL 2):

Para uma avaliação no nível de avaliação 2, o provedor de auditoria faz uma verificação da plausibilidade na sua autoavaliação (para todas as localizações no escopo da avaliação). Ele apoia isso verificando as evidências.[8] e vai fazer uma entrevista com o responsável pela segurança da informação.

O provedor de auditoria geralmente faz a entrevista através de teleconferência. A seu pedido, ele pode fazer a entrevista pessoalmente.

Se você tiver evidências que não deseja enviar ao provedor de auditoria, poderá solicitar uma inspeção no local. Dessa forma, o provedor de auditoria ainda pode verificar suas evidências “somente para você”.

Observe:

Existe um método alternativo para realizar uma avaliação no nível de

avaliação 2. Em vez da verificação da plausibilidade, o provedor de auditoria realiza uma avaliação remota completa. Esse método é algumas vezes mencionado como “**nível de avaliação 2,5**”.

Em comparação com uma avaliação no nível de avaliação 2, o auditor *verifica* se o seu SGSI cumpre os requisitos aplicáveis. No entanto, em contraste com uma avaliação no nível de avaliação 3, o auditor não realiza as atividades no local descritas na seção sobre o nível de avaliação 3 abaixo.

Formalmente, essa avaliação será efetuada como uma avaliação no AL 2.

A vantagem do AL 2,5 é que a abordagem é metodicamente compatível com o AL 3 Portanto, é possível atualizar para uma avaliação completa no AL 3 com um esforço gerenciável posteriormente. Para a atualização, o auditor só precisa realizar as atividades no local descritas na seção sobre o AL 3 abaixo.

Recomendamos avaliações no nível de avaliação 2,5 nesses casos:

1. Atualmente, você só precisa dos selos TISAX que impliquem uma avaliação no AL 2, mas não pode excluir a possibilidade de outros parceiros exigirem selos TISAX que impliquem uma avaliação no AL 3. Uma avaliação no AL 2,5 mantém o caminho aberto para atualização posterior para o AL 3.
2. Você tem dificuldades em elaborar uma autoavaliação suficientemente plausível. Para a verificação da plausibilidade, a autoavaliação deve ser conclusiva, bem compreensível e fundamentada. A elaboração de uma autoavaliação desse tipo pode exigir um esforço considerável dentro da empresa, mesmo para aquelas que estão bem posicionadas em termos fundamentais.

Para obter mais informações sobre como atualizar o nível de avaliação, consulte Seção 7.10, “Anexo: Avaliação da ampliação do escopo”.

Esta alternativa é opcional e não obrigatória para cumprir os requisitos do AL 2. A diferença entre o AL 2 e o AL 2,5 não será visível para parceiros com quem você compartilha o resultado da sua avaliação.

Nível de avaliação 3 (AL 3):

Para uma avaliação no nível de avaliação 3, o provedor de auditoria faz uma verificação abrangente da conformidade da sua empresa com os requisitos aplicáveis. O auditor utiliza a sua autoavaliação e a documentação enviada para preparar a avaliação. Mas, ao contrário do nível de avaliação 2, o auditor verificará tudo. Ele vai:

- examinar documentos e evidências

- realizar entrevistas planejadas com os responsáveis pelos processos.
- observar as condições locais
- observar a execução dos processos
- realizar entrevistas *não* planejadas com os participantes do processo

Observe:

O texto a seguir faz referência a vários conceitos que serão explicados somente posteriormente nesse documento.

Com AL 3, o provedor de auditoria deve comparecer à(s) sua(s) localização(ões). Se, por algum motivo, isso não for temporariamente possível ou exigir esforços excessivos, seu provedor de auditoria poderá usar o **método de avaliação remota com suporte de vídeo** para realizar as atividades de avaliação no local.

Seu provedor de auditoria deve registrar isso no relatório de avaliação TISAX como uma não conformidade menor. Assim que seu provedor de auditoria puder chegar à(s) sua(s) localização(ões), ele deverá realizar uma avaliação de acompanhamento que inclua todas as atividades no local anteriormente impossíveis. Além disso, você deve agendar a avaliação de acompanhamento mesmo que ainda não tenha concluído as outras ações corretivas.

Em comparação com aguardar pela disponibilidade do seu provedor de auditoria para atividades no local, essa abordagem permite que você já compartilhe os selos TISAX temporários com seu parceiro.

Níveis de avaliação e métodos de avaliação

A tabela a seguir fornece uma visão geral simplificada dos métodos de auditoria associados a cada nível de avaliação:

Método de avaliação	Nível 1 de avaliação (AL 1)	Nível 2 de avaliação (AL 2)	Nível 3 de avaliação (AL 3)
Autoavaliação	Sim	Sim	Sim
Evidências	Não	Verificação da plausibilidade	Verificação completa
Entrevistas	Não	Via teleconferência[9]	Pessoalmente, no local
Inspeção no local	Não	A seu pedido	Sim

Tabela 6. Relevância dos métodos de avaliação com os diferentes níveis de avaliação

Informações adicionais:

- Diferença entre o AL 2 e o AL 3
  Em termos de metodologia, as duas abordagens diferem significativamente. Nas avaliações no nível de avaliação 2, o auditor não verificará tudo. Ele vai verificar apenas a plausibilidade. Portanto, o provedor de auditoria não pode usar os resultados de uma avaliação no nível de avaliação 2 como base para uma atualização para o nível de avaliação 3. Os esforços para uma atualização para o nível de avaliação 3 são essencialmente os mesmos que para uma nova avaliação inicial.
- Verificação da plausibilidade vs. verificação
  De forma simplificada, uma verificação da plausibilidade consiste em verificar se algo existe e *parece* estar correto. Em contraste, uma verificação significa realmente verificar se algo é o que afirma ser.
- Classificação de informações e necessidades de proteção
  O mapeamento da classificação da informação (como confidencial ou secreta) para as necessidades de proteção pode ser diferente para vários parceiros. Portanto, por mais que desejássemos, não podemos fornecer uma tabela simples na qual a classificação das informações do seu parceiro corresponda exatamente a uma necessidade de proteção.
- Apenas conhecer um nível de avaliação não é suficiente
  Alguns parceiros podem solicitar que sua avaliação pelo TISAX seja com um determinado nível de avaliação. Entenda que apenas conhecer o nível de avaliação não é suficiente para iniciar o processo TISAX. Um nível de avaliação só faz sentido em combinação com uma lista de critérios da ISA e uma necessidade de proteção correspondente. Normalmente, os parceiros solicitam que você obtenha um selo TISAX (lista de critérios mais necessidade de proteção). No entanto, como as necessidades de proteção são mapeadas individualmente para os níveis de avaliação, é suficiente conhecer a(s) lista(s) de critérios e o nível de avaliação.
- Hierarquia do nível de avaliação
  Níveis de avaliação mais elevados incluem sempre níveis de avaliação mais baixos. Por exemplo, se a sua avaliação for baseada no nível de avaliação 3, ela atenderá automaticamente a todas as solicitações de avaliação de nível 2.
- Nossa recomendação em relação aos níveis de avaliação
  Se tiver de selecionar um objetivo da avaliação (e, portanto, implicitamente, um nível de avaliação correspondente) com base no seu próprio discernimento, recomendamos selecionar os objetivos da avaliação que impliquem um nível de avaliação 3. Os esforços para as avaliações TISAX no nível de avaliação 3 não são geralmente superiores aos do nível de avaliação 2.
  Os fornecedores com vários parceiros selecionam frequentemente os objetivos da avaliação que impliquem um nível de avaliação 3. Dessa forma, ficam preparados para todas as solicitações futuras e não precisam se preocupar com diferentes níveis de avaliação.

- Outras considerações comerciais
  Em relação aos níveis de avaliação, o custo total de uma avaliação TISAX consiste na soma dos seus esforços internos e no custo da avaliação. Embora o custo de uma avaliação no nível 2 seja menor, seus esforços internos podem ser maiores. Isso acontece devido ao fato de que uma avaliação no nível de avaliação 2 normalmente necessita de uma autoavaliação mais abrangente e uma documentação interna mais sólida. Nas avaliações no nível de avaliação 3, geralmente é suficiente demonstrar como as atividades são realizadas e apresentar uma documentação básica como evidência para o auditor. Mas sem uma inspeção no local, o auditor solicitará documentação precisa. Portanto, escolher o nível de avaliação 3 em vez do nível de avaliação 2 não é incomum. No entanto, essa é uma opção de empresas menores, não de empresas maiores.

4.3.3.6. Objetivos da avaliação e seus próprios fornecedores

O TISAX não exige necessariamente que você submeta todos os seus fornecedores aos mesmos requisitos. Se o seu objetivo da avaliação for “Segurança da informação com necessidades de proteção *muito* elevadas”, isso NÃO significa automaticamente que os seus próprios fornecedores precisem alcançar o mesmo objetivo da avaliação. Isso nem significa que eles precisem ter selos TISAX.

Mas você ainda precisa verificar para todos os seus fornecedores se a utilização dos seus serviços aumentar os riscos ou apresentar novos riscos.

Dois exemplos muito simplificados:

1. Você tem uma política de que o e-mail comum não pode ser usado para dados com necessidades de proteção muito elevadas. Portanto, o seu provedor de e-mail não precisa obter o selo TISAX com necessidades de proteção muito elevadas.
   Você poderia chegar a uma conclusão semelhante se enviar apenas e-mails criptografados e o provedor de e-mail não conseguir ver nenhum dos dados com necessidades de proteção muito elevadas.
2. Você descarta dados impressos com necessidades de proteção muito elevadas na trituradora. Nesse caso, é claro, o provedor de serviços de descarte de resíduos não precisa atender aos mesmos requisitos que você.

No entanto, a avaliação dos riscos pode demonstrar que o seu fornecedor também precisa cumprir os requisitos relativos a necessidades de proteção muito elevadas. Nesse caso, os selos TISAX são uma opção para demonstrar isso a você de forma adequada.

4.3.4. Taxa

Nós aumentamos uma taxa. Nossa lista de preços informa sobre as taxas aplicáveis, possíveis descontos e nossos termos de pagamento.

Você pode baixar a lista de preços em nosso site:

enx.com/en-US/TISAX/downloads/
Download direto do PDF:
enx.com/pricelist.pdf

Existem alguns aspectos relacionados à fatura que você deve considerar durante a preparação do cadastro:

- Seleção do endereço da fatura
  Por padrão, enviaremos a fatura para o endereço que você forneceu como a localização do participante. Mas você tem a opção de fornecer um endereço diferente para recebimento da fatura.

Observação importante:

Certifique-se de que o endereço da fatura está correto. A legislação contábil exige que o endereço em nossa fatura seja igual ao endereço da sua empresa (fatura). Por motivos de conformidade, não podemos alterar o endereço de uma fatura depois de sua emissão.

- Referência do pedido
  Se precisar ver um número de pedido de compra específico ou algo semelhante em nossa fatura, você poderá nos fornecer uma referência do pedido.
- Número de IVA
  Todas as nossas taxas estão sujeitas ao imposto sobre o valor agregado (IVA) alemão, se aplicável.
  Precisamos desse número para processar pagamentos da UE. É obrigatório fornecer um número de IVA, se o seu endereço de fatura estiver em um dos seguintes países:
  Áustria, Bélgica, Bulgária, Croácia, Chipre (parte grega), República Tcheca, Dinamarca, Estônia, Finlândia, França, Alemanha, Grécia, Hungria, Irlanda, Itália, Letônia, Lituânia, Luxemburgo, Malta, Países Baixos, Polônia, Portugal, Eslováquia, Eslovênia, Espanha, Suécia, Reino Unido
- Gerenciamento de fornecedores

Observação importante:

Por favor, entenda que devido à mutualidade entre todos os participantes TISAX, não podemos aceitar quaisquer termos adicionais (como termos gerais de compra, códigos de conduta).

Informações adicionais sobre nosso processo de faturamento:

- Não podemos aceitar termos de compra individuais.
- Aceitamos:

- transferências de dinheiro para a conta bancária especificada na fatura
- pagamentos com cartão de crédito (durante o processo de cadastro através do nosso provedor de serviços de pagamentos “Stripe”)

- Nossa fatura conterá as seguintes referências ao seu cadastro:
  - O nome e endereço de e-mail do seu contato principal do participante
  - Nome do escopo da avaliação

  Você pode encontrar um exemplo de fatura no anexo em Seção 7.1, “Anexo: Exemplo de nota fiscal”.

- Fornecemos a maioria dos fatos que você normalmente precisa para processar nossa fatura diretamente nele. Essas e outras ocorrências estão disponíveis no nosso documento “Information for Members and Business Partners” (Informações para Integrantes e Parceiros de negócios). Envie-nos um e-mail e enviaremos para você uma versão atual.

Observe:

Sabemos que às vezes o processo interno de aprovação de pagamentos de uma empresa é bastante demorado. Portanto, a sua próxima etapa imediata no processo TISAX não depende do recebimento do pagamento. Mas saiba que você não poderá compartilhar o resultado da sua avaliação se não tivermos recebido o seu pagamento.
Por este motivo, recomendamos que se certifique de que enviamos a nossa fatura ao destinatário apropriado e que ele contenha uma referência do pedido, se aplicável. Você também pode acompanhar internamente se alguém pagou a fatura.

Observação importante:

Nós — ENX Association — emitimos uma fatura para a taxa. É apenas uma parte do custo total de uma avaliação TISAX. Seu provedor de auditoria TISAX fatura os custos da(s) avaliação(ões).

Para obter mais informações sobre os custos relacionados ao provedor de auditoria, consulte a Seção 5.3.4, “Avaliação de propostas”.

Observação importante:

A taxa é devida independentemente de você:

- continuar o processo TISAX ou não.
- passar com sucesso no processo de avaliação TISAX.

> Portanto, a fatura pode chegar antes do começo da avaliação inicial.

4.4. Portal ENX

A próxima seção descreverá o processo de cadastro on-line, onde você insere todos os dados coletados conforme recomendado na seção anterior. Antes de iniciar o processo de cadastro on-line, vamos explicar brevemente a finalidade e os benefícios do portal ENX.

O portal ENX nos permite manter um banco de dados de todos os participantes TISAX e desempenha um papel importante em todo o processo TISAX. Durante o cadastro TISAX você insere os dados que os provedores de auditoria TISAX podem utilizar (se concordar) para calcular as suas propostas e planejar os procedimentos da avaliação. Depois de passar pelo processo de avaliação TISAX, você vai usar a plataforma de compartilhamento no portal ENX para compartilhar o resultado da avaliação com o seu parceiro.

O nome do portal é “Portal ENX” em vez de “portal TISAX”, porque também utilizamos o portal para gerenciar outras atividades comerciais (como a Rede ENX).

4.5. Processo de cadastro on-line

Se você se preparou de acordo com nossos conselhos acima (Seção 4.3, “Preparação do cadastro”), você está pronto para iniciar o processo de cadastro on-line.

4.5.1. Tempo necessário

Quanto tempo levará depende muito do número de escopos e localizações cadastrados. Para o seu primeiro cadastro como participante com um escopo em uma localização, você deverá esperar um tempo mínimo de 20 minutos.

Recomendamos realizar o cadastro em uma única sessão, pois atualmente não é possível acompanhar facilmente algumas etapas posteriormente. Caso ainda precise fazer uma pausa, entraremos em contato para solicitar quaisquer dados ausentes.

4.5.2. Comece aqui

Inicie seu cadastro em nosso site:
enx.com/en-us/Account/Login/Register?returnUrl=%2FTISAX%2Ftisax-initial-registration%2F

Basicamente, tudo que você precisa fazer é seguir as instruções na tela. No entanto, vamos descrever abaixo brevemente o processo.

4.5.3. Conta do portal

A primeira etapa é criar uma conta no portal ENX. Você precisa da conta do portal para poder gerenciar os “dados dos participantes” da sua empresa.

Observe:

Caso o portal ENX afirme que seu endereço de e-mail já está sendo usado, entre em contato conosco. Essa mensagem pode indicar que por algum motivo você já está armazenado em nosso sistema.

Observe:

Conforme descrito, as contas no portal não são necessariamente “contatos de participantes” ou “contatos do escopo” (veja abaixo) com uma função ativa no processo de avaliação.

Vice-versa, um “contato do participante” ou “contato do escopo” não inclui automaticamente os mesmos direitos para gerenciar os dados do participante que uma conta do portal. Isso significa que colegas indicados como “contato do participante” ou “contato do escopo” não podem acessar automaticamente os dados do participante no portal ENX.

Se desejar atribuir o direito de gerenciar os dados do participante a um contato que você já criou no portal ENX (independentemente de você ter atribuído uma função a ele), você precisa convidar o contato. Para obter mais informações, consulte a última observação em Seção 4.5.5, “Contato do participante”.

4.5.4. Cadastro do participante

A segunda etapa é cadastrar sua empresa como participante TISAX. O “participante TISAX” é a empresa que compartilha os resultados da avaliação com outros participantes.

4.5.5. Contato do participante

Essa é a pessoa geralmente responsável por todos os tópicos da avaliação de segurança da informação da sua empresa. Pode ser você ou outra pessoa da sua empresa.

Normalmente, o contato do participante principal é tudo o que precisamos. Caso prefira que todas as comunicações enviadas por nós e pelos nossos provedores de auditoria TISAX no contexto desse cadastro também sejam enviadas a outras pessoas, adicione os contatos adicionais dos participantes.

Observação importante:

Recomendamos a atribuição de pelo menos um substituto para cada contato. Se um contato estiver temporariamente indisponível ou sair da empresa, outra pessoa poderá gerenciar os dados dos participantes da sua empresa.
Se precisar fazer a atribuição de um novo contato (na ausência de outros

contatos válidos), você precisará passar por um processo complexo. Nosso processo garante que somente pessoas que possam provar que têm o direito de representar legalmente a empresa possam aprovar a atribuição de um novo contato principal.

Observe:

Você sempre pode adicionar ou remover contatos posteriormente (mesmo depois de concluir o processo de cadastro on-line e mesmo depois de concluir as avaliações).

Observe:

Você não pode usar endereços de e-mail de grupo para contatos de participantes (como “info@acme.com” ou “IT@acme.com”).

Isso está de acordo com os requisitos da ISA em relação a logins de usuários.

Observe:

Você pode escolher se cada contato deve ter acesso aos dados dos participantes da sua empresa. Há duas opções:

1. Você acabou de adicionar o contato. O contato fica armazenado em nosso sistema, mas não consegue fazer login e gerenciar nenhum dado.
2. Ou você convida o contato. Em seguida, o portal ENX envia um e-mail de convite ao contato. O contato deverá seguir o link de convite no e-mail. Depois que o contato tiver criado sua conta pessoal no portal ENX, ele poderá gerenciar os dados dos participantes da sua empresa.

Para criar um novo contato: Sign in (Entrar) > MY TISAX (MEU TISAX) > ADMINISTRATORS (ADMINISTRADORES) > Create new TISAX Administrator (Criar novo Administrador TISAX)

Para convidar um contato: Sign in (Entrar) > MY TISAX (MEU TISAX) > ADMINISTRATORS (ADMINISTRADORES) > Vá até o final da linha da tabela do contato e clique no botão com a seta para baixo > Edit TISAX Administrator (Editar Administrador TISAX) > Vá para a seção “ENX PORTAL ACCESS” (ACESSO DO PORTAL ENX) > Defina “INVITE THIS CONTACT" (CONVIDAR ESTE CONTATO) para “Yes” (Sim) > Clique em “Save Contact” (Salvar contato)

4.5.6. Termos e condições gerais

A terceira etapa é aceitar os “Termos e Condições Gerais de Participação TISAX”.

Você pode desejar consultar as notas explicativas na Seção 4.3.1, “A base jurídica”.

4.5.7. Cadastro do escopo da avaliação

A quarta etapa é cadastrar o escopo da avaliação de segurança da informação.

Solicitamos que você:

1. atribua um nome ao escopo da avaliação.
   A finalidade principal do nome do escopo é facilitar a identificação de um escopo na lista de visão geral de escopos no portal ENX.
   Você pode desejar consultar as notas explicativas na Seção 4.3.2.6, “Nome do escopo”
2. escolha um tipo de escopo da avaliação.
   (Padrão, personalizado)
   Você pode desejar consultar as notas explicativas na Seção 4.3.2, “O escopo da avaliação TISAX”.
3. especifique o contato principal do escopo.
   Essa é a pessoa que, em geral, tem a responsabilidade pela avaliação de um escopo específico. Pode ser você ou outra pessoa da sua empresa.
   Normalmente, o contato principal do escopo é tudo o que precisamos. Caso prefira que todas as comunicações por nós enviadas no contexto desse escopo específico também seja enviada para outras pessoas, você poderá adicionar contatos adicionais de participantes.
4. selecione seu(s) objetivo(s) da avaliação.
   Você pode desejar consultar as notas explicativas na Seção 4.3.3, “Objetivos da avaliação”.
5. adicione localização(ões) ao escopo da avaliação.
   Solicitamos que você especifique todas as localizações que estão incluídas no escopo da avaliação.
   Você pode desejar consultar as notas explicativas na Seção 4.3.2, “O escopo da avaliação TISAX”.

Observe:

Depois de criar uma nova localização, você não poderá editá-la. Para pequenas alterações (mudança de nome da empresa, erros de digitação no nome da rua, código postal, cidade, etc.), entre em contato conosco. Faremos a edição para você.

Observação importante:

Essa observação só é relevante se você estiver renovando seus selos TISAX.

Reutilize os registros da localização existentes que foram criados e usados durante o cadastro do seu escopo anterior. Não crie um novo registro da

localização com o mesmo endereço.

O motivo: alguns participantes do TISAX processam automaticamente os resultados da avaliação dos seus parceiros. Eles sincronizam seu próprio sistema com o portal ENX. Até mesmo pequenas diferenças podem bloquear o sucesso da sincronização. Além disso, você não sobrecarrega os dados dos participantes com duplicatas desnecessárias.

6. selecione os níveis de publicação e compartilhamento (opcional).
   Você já pode decidir publicar o resultado da sua avaliação para outros participantes TISAX e compartilhar o resultado da sua avaliação com seu(s) parceiro(s). Normalmente, você estaria concordando em nos permitir pelo menos mostrar que sua empresa é participante e que você passou com sucesso pelo processo TISAX.
   Você pode ignorar essa etapa com segurança durante seu cadastro inicial. Você sempre pode definir o acesso ao resultado da sua avaliação posteriormente.
   Você pode desejar consultar as notas explicativas na Seção 4.3.2.8, “Publicação e compartilhamento”.

Observação importante:

Você não pode revogar nenhuma permissão de publicação ou compartilhamento.
Para obter detalhes, consulte Seção 6.4, “Permanência dos resultados compartilhados”.

7. especifique quem recebe a fatura.
   Solicitamos que você especifique quem receberá nossa(s) fatura(s).
   Você pode desejar consultar as notas explicativas na Seção 4.3.4, “Taxa”.

Observe:

Aqui, você não pode errar muito. Se mais tarde descobrir que deveria ter cadastrado um escopo ligeiramente diferente (você esqueceu uma localização, tem outro objetivo da avaliação, etc.), o provedor de auditoria poderá, no entanto, realizar a avaliação.

Exemplo: o auditor determina que o escopo deve conter uma localização adicional que você originalmente não adicionou ao escopo. O auditor prosseguirá e, em seguida, atualizará seu escopo da avaliação no portal ENX ao carregar o resultado da avaliação.

Observe:

Cada escopo da avaliação passa por um ciclo de vida. Nessa fase, o status do seu escopo da avaliação pode ser “Incomplete” (Incompleto), “Awaiting your order” (Aguardando seu pedido) ou “Awaiting ENX approval” (Aguardando aprovação da ENX).

Para obter mais informações sobre o status de um escopo da avaliação, consulte a Seção 7.5.1, “Visão geral: Assessment scope status (Status do escopo da avaliação)”.

Observe:

Para grandes corporações com muitas localizações, a TISAX oferece a avaliação de grupo simplificada. Você pode considerar essa opção se:

- você tem pelo menos três localizações em seu escopo[10] e o
- seu sistema de gerenciamento de segurança da informação está em excelente condição e organizado centralmente[11].

Para uma avaliação de grupo simplificada, o esforço inicial é maior. No entanto, isso compensa quanto mais localizações você tiver.

Para obter mais informações sobre a “avaliação de grupo simplificada”, consulte o documento “TISAX Simplified Group Assessment” (Avaliação de grupo simplificada TISAX).

Você pode baixar o documento “TISAX Simplified Group Assessment” (Avaliação de grupo simplificada TISAX) em nosso site em:
enx.com/en-US/TISAX/downloads/

Download direto do PDF:
enx.com/sga.pdf

Observe:

Depois que você cadastra o escopo da sua avaliação, você não pode alterá-lo por conta própria.

Caso possa nos garantir de maneira confiável que ainda NÃO enviou seu “TISAX scope excerpt” (extrato do escopo TISAX) para os nossos provedores de auditoria, entre em contato conosco. Podemos mudar isso para você.

Se você já enviou seu “TISAX scope excerpt” (extrato do escopo TISAX) para (um de) nossos provedores de auditoria, basta criar a(s) nova(s) localização(ões) no portal ENX (se aplicável) e discutir quaisquer alterações com seu provedor de auditoria. Seu provedor de auditoria vai realizar a

avaliação com base nas alterações e atualizará as informações do escopo no portal ENX.

Observe:

Não é possível excluir um escopo da avaliação no portal ENX. Se você criou um escopo da avaliação por engano, entre em contato conosco. Excluiremos isso para você.

4.5.8. E-mail de confirmação

Depois de concluir todas as etapas obrigatórias acima, vamos verificar sua inscrição. Em seguida, enviaremos a você um e-mail de confirmação.

Esse e-mail tem dois elementos importantes:

- Uma lista de contatos de todos os provedores de auditoria TISAX
  Você deve escolher um de nossos provedores de auditoria TISAX para realizar uma avaliação do seu escopo da avaliação. Você pode usar os contatos para solicitar propostas. Para obter mais informações sobre a seleção do provedor de auditoria, consulte Seção 5.3, “Seleção do provedor de auditoria”.
- O “TISAX scope excerpt” (extrato do escopo TISAX) como um arquivo PDF anexo

  Ele contém:

  - As informações que armazenamos em nosso banco de dados
  - Seu ID de participante
    Consulte Seção 4.5.8.1, “Participant ID (🇵🇹 ID de participante)” abaixo.
  - Seu(s) ID(s) do escopo
    Consulte Seção 4.5.8.2, “Scope ID (🇵🇹 ID do escopo)” abaixo.

Para obter um exemplo do nosso e-mail de confirmação, consulte Seção 7.2, “Anexo: Exemplo de e-mail de confirmação”.

Para obter um exemplo do “TISAX scope excerpt” (extrato do escopo TISAX), consulte Seção 7.3, “Anexo: Exemplo do extrato do escopo TISAX”.

Você receberá nosso e-mail de confirmação normalmente dentro de três dias úteis.

Se você não receber uma resposta nossa dentro de sete dias úteis, verifique se a) você forneceu todas as informações e b) o status do escopo da avaliação é “Awaiting ENX approval” (Aguardando aprovação da ENX). Iniciaremos o processamento do seu cadastro somente quando tudo estiver concluído. Se você achar que tudo está completo, mas ainda não entramos em contato com você, entre em contato conosco.

Enviamos nosso e-mail de confirmação para o contato principal do participante.

Observe:

Cada escopo da avaliação passa por um ciclo de vida. Nessa fase, o seu escopo da avaliação está com o status “Awaiting ENX approval” (Aguardando aprovação da ENX).

Para obter mais informações sobre o status de um escopo da avaliação, consulte a Seção 7.5.5, “Assessment scope status “Awaiting your payment” (Status do escopo da avaliação “Awaiting your payment” (Aguardando seu pagamento))”.

As próximas duas subseções fornecem informações detalhadas sobre a finalidade do seu ID de participante e do ID do escopo.

4.5.8.1. Participant ID (ID de participante)

O ID de participante:

- identifica um participante TISAX.
- é exclusivo para cada participante.
- é atribuído por nós após a conclusão do cadastro.
- é um pré-requisito para solicitar uma avaliação de segurança da informação por qualquer um de nossos provedores de auditoria TISAX.
- ele fica assim:

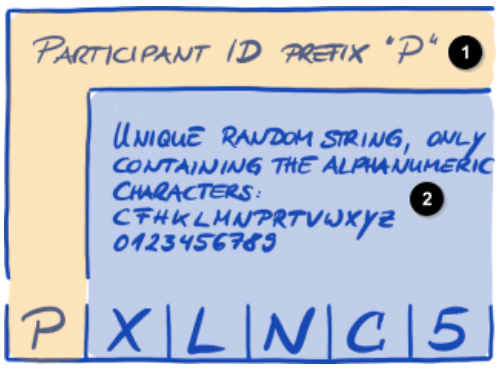


Figura 7. Formato do ID de Participante[12]

1. Prefixo do ID de participante “P”
2. String aleatória exclusiva, contendo apenas os caracteres alfanuméricos:
   CFHKLMNPRTVWXYZ
   0123456789

Observe:

Existem duas maneiras de encontrar seu ID de participante:

1. Verifique seu “TISAX scope excerpt” (extrato do escopo TISAX).
   Consulte Seção 4.5.8, “E-mail de confirmação” acima.
2. Faça login no portal ENX, vá até a barra de navegação principal e selecione “DASHBOARD” (🇵🇹 “DASHBOARD” (PAINEL)). Lá você encontrará seu ID de participante.

4.5.8.2. Scope ID (🇵🇹 ID do escopo)

O ID do escopo:

- identifica um escopo da avaliação.
- é exclusivo para cada escopo da avaliação.
- é atribuído por nós após a conclusão do cadastro.
- é um pré-requisito para poder solicitar uma avaliação de segurança da informação por qualquer um dos nossos provedores de auditoria TISAX.
- ele fica assim:

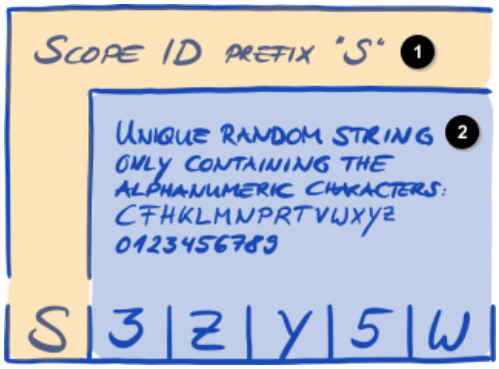


Figura 8. Formato do ID do escopo

1. Prefixo do ID do escopo “S”
2. String aleatória exclusiva, contendo apenas os caracteres alfanuméricos:
   CFHKLMNPRTVWXYZ
   0123456789

Observe:

Existem duas maneiras de encontrar seu ID do escopo:

1. Verifique seu “TISAX scope excerpt” (extrato do escopo TISAX).

Consulte Seção 4.5.8, “E-mail de confirmação” acima.

2. Faça login no portal ENX, acesse a barra de navegação principal, selecione “MY TISAX” (MEU TISAX) e depois “SCOPES AND ASSESSMENTS” (ESCOPOS E AVALIAÇÕES). Lá você encontrará seu(s) ID(s) do escopo.

Observe:

Cada escopo da avaliação (identificado por seu ID do escopo) passa por um ciclo de vida.

Para obter mais informações sobre o status de um escopo da avaliação, consulte a Seção 7.5, “Anexo: Assessment scope status (Status do escopo da avaliação)”.

4.5.9. Informações do status

Nessa fase, existem dois status relevantes que utilizamos para descrever a sua posição no processo TISAX:

1. Status do participante
2. Status do escopo da avaliação

O diagrama a seguir ilustra as condições que devem ser atendidas para atingir um determinado status:

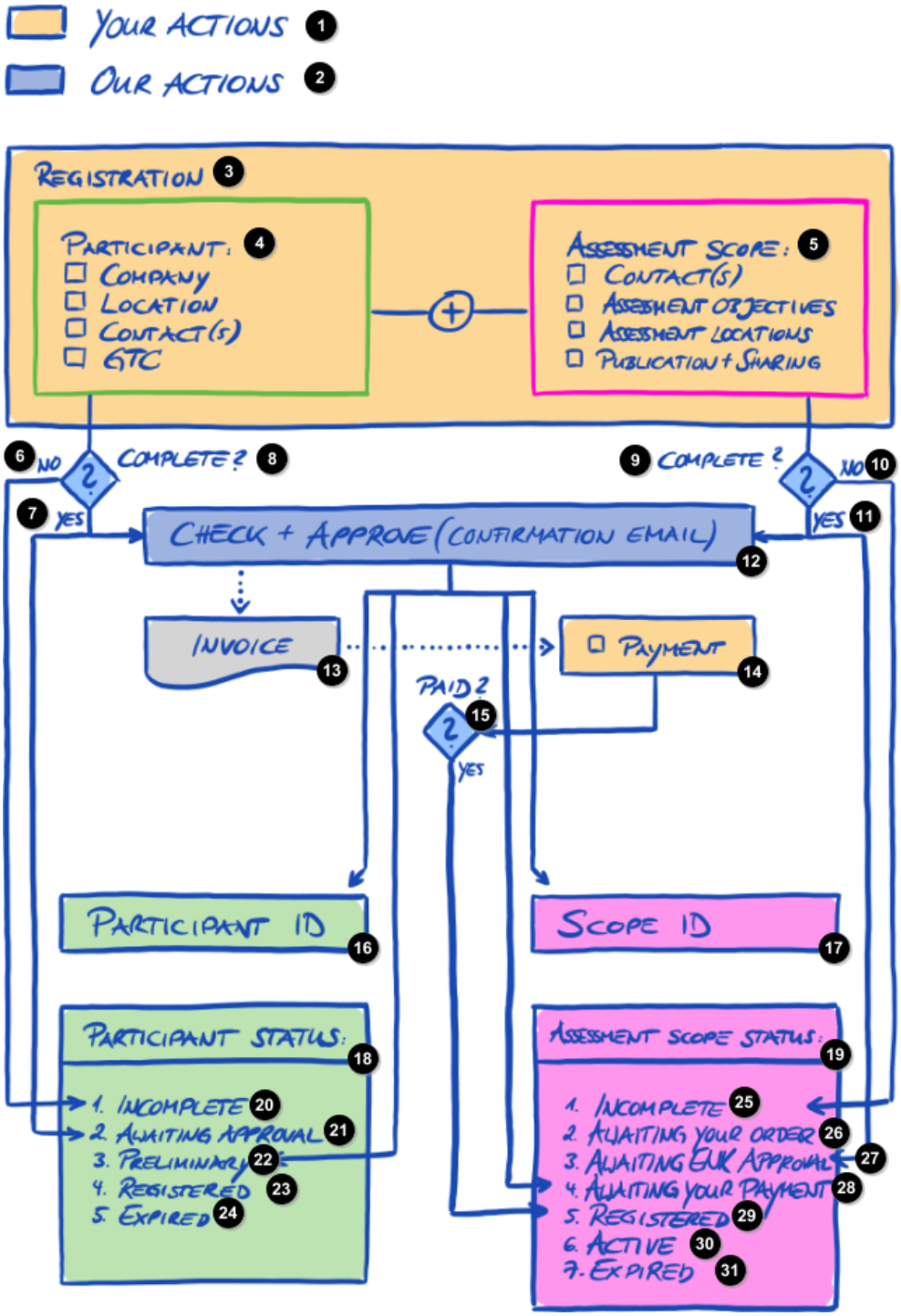


Figura 9. Condições para o status do participante e o status do escopo da avaliação

1. Suas ações
2. Nossas ações
3. Cadastro

4 Participante:
[ ] Empresa
[ ] Localização
[ ] Contato(s)
[ ] TCG

5 Escopo da avaliação:
[ ] Contato(s)
[ ] Objetivos da avaliação
[ ] Localizações da avaliação
[ ] Publicação + Compartilhamento

6 Não

7 Sim

8 Concluído?

9 Concluído?

10 Não

11 Sim

12 Verificar + Aprovar (e-mail de confirmação)

13 Nota fiscal

14 [ ] Pagamento

15 Paga?

16 ID de participante

17 ID do escopo

18 Status do participante:

19 Status do escopo da avaliação:

20 1. Incompleto

21 2. Aguardando aprovação

22 3. Provisório

23 Cadastrado

24 Vencido

25 1. Incompleto

26 2. Aguardando seu pedido

27 3. Aguardando aprovação da ENX

28 4. Aguardando seu pagamento

29 5. Cadastrado

30 6. Ativo

31 7. Vencido

Você pode encontrar as definições de status e o que precisa fazer para avançar para o próximo status no anexo.

Para obter mais informações sobre o:

- status do participante, consulte a Seção 7.4, “Anexo: Participant status (Status do participante)”.
- status do escopo da avaliação, consulte a Seção 7.5, “Anexo: Assessment scope status (Status do escopo da avaliação)”.

4.5.10. Alterações nas suas informações de cadastro

Observe:

Para todas as respostas sobre o ciclo de vida dos dados, consulte Seção 7.9, “Anexo: Gerenciamento do ciclo de vida dos dados do participante”. Ele contém as instruções para os casos em que você desejar alterar ou atualizar os dados como o nome da sua empresa ou suas informações de contato.

Parabéns, você concluiu o cadastro como participante TISAX. Você está pronto para continuar com a próxima etapa do processo TISAX.

5. Avaliação (Etapa 2)

O tempo estimado de leitura da seção de avaliação é de 30 a 35 minutos.

5.1. Visão geral

A avaliação TISAX é a segunda etapa. É aqui que você faz a maior parte do trabalho para obter a avaliação TISAX.

As seções a seguir vão orientar você durante a avaliação:

1. Começamos explicando como você pode usar a autoavaliação ISA para descobrir se está preparado para uma avaliação TISAX.
2. Em seguida, aconselhamos você sobre como escolher um de nossos provedores de auditoria TISAX.
3. A seguir, descrevemos seu caminho através do processo de avaliação.
4. No final, explicamos o “resultado do processo”: o resultado da sua avaliação e os selos TISAX.

5.2. Autoavaliação baseada na ISA

Para estar pronto para uma avaliação TISAX, você precisa, em primeiro lugar, ter seu sistema de gerenciamento de segurança da informação (SGSI) em excelente condição. Para descobrir se o seu SGSI corresponde ao nível de maturidade esperado, é necessário realizar uma autoavaliação com base na ISA.

A “Avaliação de Segurança da Informação” (ISA) é uma lista de critérios publicada pela “Associação Alemã do Setor Automotivo” (Verband der Automobilindustrie e.V. - VDA). É o padrão do setor automotivo para avaliações de segurança da informação.

As seções a seguir se concentram nas instruções práticas para realizar uma autoavaliação baseada na ISA.

As explicações, exemplos e capturas de tela nesse manual são baseados na versão 5 da ISA.

Observe:

Você vai encontrar informações sobre alterações em comparação com versões anteriores da ISA em sua planilha Excel “Change history” (Histórico de alterações).

Observe:

Para obter informações sobre qual versão da ISA é aplicável à sua avaliação

> quando a VDA publicar uma nova versão, consulte Seção 7.11, “Anexo: Gerenciamento do ciclo de vida da ISA”.

5.2.1. Baixe o documento da ISA

Comece a sua autoavaliação baixando o documento da ISA.

Você pode baixá-lo em nosso site:
enx.com/en-US/TISAX/downloads/

Download direto do arquivo Excel:
portal.enx.com/isa5-en.xlsx

O documento da ISA também está disponível em alemão:
enx.com/de-de/TISAX/downloads/

5.2.2. Entenda o documento da ISA

Antes de iniciar sua autoavaliação, aqui estão algumas explicações que podem ser úteis. Fornecemos isso além das explicações e definições oficiais no documento da ISA, mas com foco no uso para avaliações TISAX.

5.2.2.1. Lista de critérios

A ISA tem atualmente três “listas de critérios”[13]:

1.	Segurança da informação	Information Security
2.	Proteção do protótipo	Prototype Protection
3.	Proteção de dados	Data Protection

Cada lista de critérios tem sua própria planilha Excel:

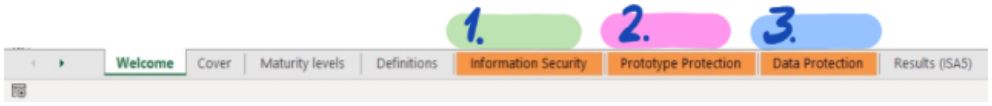


Figura 10. Captura de tela: listas de critérios da ISA como planilhas Excel

Qual lista de critérios é relevante para você? Isso depende do(s) seu(s) objetivo(s) da avaliação.

Cada objetivo da avaliação define quais requisitos de qual lista de critérios são relevantes. Para alguns objetivos da avaliação, são relevantes apenas os requisitos de *uma* lista de critérios; para outros, são relevantes os requisitos de *mais de uma* lista de critérios.

Os objetivos da avaliação acima mencionados são mapeados para essas listas de critérios:

N.º	Objetivo da avaliação (Assessment objective)	Lista(s) de critérios ISA
1.	Info high	Information Security (Segurança da informação)
2.	Info very high	Information Security (Segurança da informação)
3.	Confidential	Information Security (Segurança da informação)
4.	Strictly confidential	Information Security (Segurança da informação)
5.	High availability	Information Security (Segurança da informação)
6.	Very high availability	Information Security (Segurança da informação)
7.	Proto parts	Prototype Protection (Proteção do protótipo)
8.	Proto vehicles	Prototype Protection (Proteção do protótipo)
9.	Test vehicles	Prototype Protection (Proteção do protótipo)
10.	Proto events	Prototype Protection (Proteção do protótipo)
11.	Data	Information Security (Segurança da informação) Data Protection (Proteção de dados)
12.	Special data	Information Security (Segurança da informação) Data Protection (Proteção de dados)

Tabela 7. Mapeamento entre os objetivos da avaliação TISAX e as listas de critérios da ISA

Exemplo: se você selecionou o objetivo da avaliação “Proteção de dados”, então deverá responder às perguntas das listas de critérios “Segurança da informação” E “Proteção de dados”.

Você deve ter observado que existe mais de um objetivo da avaliação de acordo com a lista de critérios. Como saber quais requisitos são aplicáveis a qual objetivo da avaliação?

A tabela a seguir mostra quais requisitos são aplicáveis:

N.º	Objetivo da avaliação (Assessment objective)	Requisitos aplicáveis
1.	Info high	▪ Lista de critérios “Information Security” (“Segurança da informação” ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios)) ◦ Coluna “Requirements (should)” (“Requirements (should)” (Requisitos (obrigatórios)) ◦ Coluna “Additional requirements for high protection needs” (“Additional requirements for high protection needs” (Requisitos adicionais para necessidades de proteção elevada))
2.	Info very high	▪ Lista de critérios “Information Security” (“Segurança da informação” ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios)) ◦ Coluna “Requirements (should)” (“Requirements (should)” (Requisitos (obrigatórios)) ◦ Coluna “Additional requirements for high protection needs” (“Additional requirements for high protection needs” (Requisitos adicionais para necessidades de proteção elevada)) ◦ Coluna ( ) “Additional requirements for very high protection needs” (Requisitos adicionais para necessidades de proteção muito elevadas)

N.º	Objetivo da avaliação (Assessment objective)	Requisitos aplicáveis
3.	Confidential	▪ Lista de critérios “Information Security” (“Information Security” (Segurança da informação)) ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios))) ◦ Coluna “Requirements (should)” (“Requirements (should)” (Requisitos (obrigatórios))) ◦ Coluna “Additional requirements for high protection needs” (“Additional requirements for high protection needs” (Requisitos adicionais para necessidades de proteção elevada)) (mas apenas aqueles marcados com “**C**” como em **C**onfidentiality (**C**onfidentiality (Confidencialidade))
4.	Strictly confidential	▪ Lista de critérios “Information Security” (“Information Security” (Segurança da informação)) ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios))) ◦ Coluna “Requirements (should)” (“Requirements (should)” (Requisitos (obrigatórios))) ◦ Coluna “Additional requirements for high protection needs” (“Additional requirements for high protection needs” (Requisitos adicionais para necessidades de proteção elevada)) (mas apenas aqueles marcados com “**C**” como em **C**onfidentiality (**C**onfidentiality (Confidencialidade)) ◦ Coluna ( ) “Additional requirements for very high protection needs” (Requisitos adicionais para necessidades de proteção muito elevadas) (mas apenas aqueles marcados com “**C**” como em **C**onfidentiality (**C**onfidentiality (Confidencialidade))

N.º	Objetivo da avaliação (Assessment objective)	Requisitos aplicáveis
5.	High availability	▪ Lista de critérios “Information Security” (“Information Security” (Segurança da informação)) ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios))) ◦ Coluna “Requirements (should)” (“Requirements (should)” (Requisitos (obrigatórios))) ◦ Coluna “Additional requirements for high protection needs” (“Additional requirements for high protection needs” (Requisitos adicionais para necessidades de proteção elevada)) (mas apenas aqueles marcados com “**A**” como em **A**vailability (**A**vailability (Disponibilidade)))
6.	Very high availability	▪ Lista de critérios “Information Security” (“Information Security” (Segurança da informação)) ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios))) ◦ Coluna “Requirements (should)” (“Requirements (should)” (Requisitos (obrigatórios))) ◦ Coluna “Additional requirements for high protection needs” (“Additional requirements for high protection needs” (Requisitos adicionais para necessidades de proteção elevada)) (mas apenas aqueles marcados com “**A**” como em **A**vailability (**A**vailability (Disponibilidade))) ◦ Coluna ( ) “Additional requirements for very high protection needs” (Requisitos adicionais para necessidades de proteção muito elevadas) (mas apenas aqueles marcados com “**A**” como em **A**vailability (**A**vailability (Disponibilidade)))

N.º	Objetivo da avaliação (Assessment objective)	Requisitos aplicáveis
7.	Proto parts	▪ Lista de critérios “Prototype Protection” (“Prototype Protection”) (Proteção de protótipos) Mas apenas estes capítulos: 8.1 Physical and Environmental Security (8.1 Segurança física e ambiental) 8.2 Organizational Requirements (8.2 Requisitos organizacionais) 8.3 Handling of vehicles, components and parts (8.3 Manuseio de veículos, componentes e peças) ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios))) ◦ Coluna “Requirements (should)” (“Requirements (should)” (Requisitos (obrigatórios)))
8.	Proto vehicles	▪ Lista de critérios “Prototype Protection” (“Prototype Protection”) (Proteção de protótipos) Mas apenas estes capítulos: 8.1 Physical and Environmental Security (8.1 Segurança física e ambiental) 8.2 Organizational Requirements (8.2 Requisitos organizacionais) 8.3 Handling of vehicles, components and parts (8.3 Manuseio de veículos, componentes e peças) ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios))) ◦ Coluna “Requirements (should)” (“Requirements (should)” (Requisitos (obrigatórios))) ◦ Coluna “Additional requirements for vehicles classified as requiring protection” (“Additional requirements for vehicles classified as requiring protection” (Requisitos adicionais para veículos classificados como necessitando de proteção))

N.º	Objetivo da avaliação (Assessment objective)	Requisitos aplicáveis
9.	Test vehicles	▪ Lista de critérios “Prototype Protection” (“Prototype Protection”) (Proteção de protótipos) Mas apenas estes capítulos: 8.2 Organizational Requirements (8.2 Requisitos organizacionais) 8.3 Handling of vehicles, components and parts (8.3 Manuseio de veículos, componentes e peças) 8.4 Requirements for trial vehicles (8.4 Requisitos para veículos de teste) ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios))) ◦ Coluna “Requirements (should)” (“Requirements (should)” (Requisitos (obrigatórios)))
10.	Proto events	▪ Lista de critérios “Prototype Protection” (“Prototype Protection”) (Proteção de protótipos) Mas apenas estes capítulos: 8.2 Organizational Requirements (8.2 Requisitos organizacionais) 8.3 Handling of vehicles, components and parts (8.3 Manuseio de veículos, componentes e peças) 8.5 Requirements for events and shootings (8.5 Requisitos para eventos e sessões de filmagem e de fotos) ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios)) ◦ Coluna “Requirements (should)” (“Requirements (should)” (Requisitos (obrigatórios))

N.º	Objetivo da avaliação (Assessment objective)	Requisitos aplicáveis
11.	Data	▪ Lista de critérios “Information Security” (“Segurança da informação” ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios)) ◦ Coluna “Requirements (should)” (“Requirements (should)” (Requisitos (obrigatórios)) ◦ Coluna “Additional requirements for high protection needs” (“Additional requirements for high protection needs” (Requisitos adicionais para necessidades de proteção elevada)) (mas apenas aqueles marcados com “**C**” como em **C**onfidentiality (**C**onfidencialidade)) ▪ Lista de critérios “Data Protection” (“Proteção de dados”) ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios))

N.º	Objetivo da avaliação (Assessment objective)	Requisitos aplicáveis
12.	Special data	▪ Lista de critérios “Information Security” (“Segurança da informação” ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios)) ◦ Coluna “Requirements (should)” (“Requirements (should)” (Requisitos (obrigatórios)) ◦ Coluna “Additional requirements for high protection needs” (“Additional requirements for high protection needs” (Requisitos adicionais para necessidades de proteção elevada)) (mas apenas aqueles marcados com “**C**” como em **C**onfidentiality (**C**onfidencialidade)) ◦ Coluna ()“Additional requirements for very high protection needs” (Requisitos adicionais para necessidades de proteção muito elevadas) (mas apenas aqueles marcados com “**C**” como em **C**onfidentiality (**C**onfidencialidade)) ▪ Lista de critérios “Data Protection” (“Proteção de dados”) ◦ Coluna “Requirements (must)” (“Requirements (must)” (Requisitos (obrigatórios))

Tabela 8. Relevância dos requisitos aos objetivos da avaliação

Observe:

Cada requisito nas duas colunas “Additional requirements for high protection needs” (Requisitos adicionais para necessidades de proteção elevadas) e “Additional requirements for very high protection needs” (Requisitos adicionais para necessidades de proteção muito elevadas) é marcado com um “**C**” como em **C**onfidentiality (**C**onfidencialidade) ou um “**I**” como em **I**ntegrity (**I**ntegridade) ou um “**A**” como em **A**vailability (Disponibilidade, **a**vailability, em inglês) ou qualquer combinação dessas três letras.

Quando a tabela acima restringe os requisitos nessas duas colunas para aqueles marcados com *uma* das letras acima mencionadas, isso sempre inclui os requisitos que também estão marcados com *mais do que essa* letra.

Exemplo: todos os requisitos marcados com “(C)”, “(C, I, A)” ou “(C, I)” são

> aplicáveis quando “C” estiver especificado na tabela acima (por exemplo, no objetivo da avaliação “Special data”).

A captura de tela abaixo mostra os principais elementos das perguntas de controle da lista de critérios de “Segurança da informação”. (As outras listas de critérios têm apenas um subconjunto desses elementos.) Explicamos todos os elementos mais abaixo.

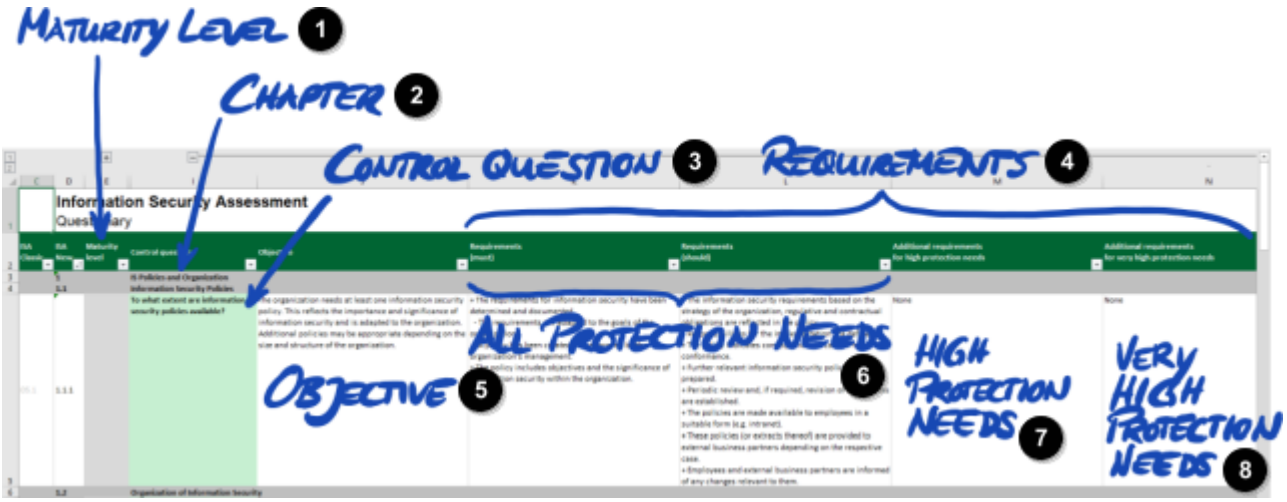


Figura 11. Captura de tela: principais elementos das perguntas da lista de critérios da ISA “Segurança da informação”

1. Nível de maturidade
2. Capítulo
3. Pergunta de controle
4. Requisitos
5. Objetivo
6. Todas as necessidades de proteção
7. Necessidades de proteção elevadas
8. Necessidades de proteção muito elevadas

5.2.2.2. Capítulos

Cada lista de critérios agrupa as perguntas em capítulos.

Exemplo: “2 Recursos Humanos”

O agrupamento é baseado nas responsabilidades normais de uma empresa. Esses departamentos estão especificados na coluna “Usual person responsible for process implementation” (Responsável habitual pela implementação do processo) (“RH” no exemplo acima).

5.2.2.3. Perguntas de controle

Você encontra as perguntas de cada lista de critérios nas respectivas planilhas Excel.

Exemplo: “4.1.2 Até que ponto o acesso do usuário aos serviços de rede, sistemas de TI e aplicativos de TI está protegido?”

As perguntas de controle também são chamadas de “controles”. Esse é jargão dos auditores. Os padrões ISO nos quais a ISA se baseia usam o termo “controle”.

5.2.2.4. Campos do formulário de autoavaliação

Entre as colunas “Maturity level” (🇵🇹 “Maturity level” (Nível de maturidade)) e “Control question” (🇵🇹 “Control question” (Pergunta de controle)) estão os campos do formulário que você precisa preencher quando estiver realizando uma autoavaliação:

Campo do formulário	Finalidade	Obrigatório?
Implementation description (🇵🇹 Descrição da implementação) (Coluna F)	Aqui você deve descrever brevemente o que implementou para solucionar essa pergunta de controle em sua empresa.	Sim
Reference Documentation (🇵🇹 Documentação de referência) (Coluna G)	Aqui você deve especificar em quais documento(s) comprova a implementação.	Sim
Findings/Result (🇵🇹 Achados/Resultado) (Coluna H)	Aqui você pode anotar quaisquer achados onde você acha que existe uma lacuna entre o que deveria ser e o que é.	Não

Tabela 9. Campos do formulário de autoavaliação e sua finalidade

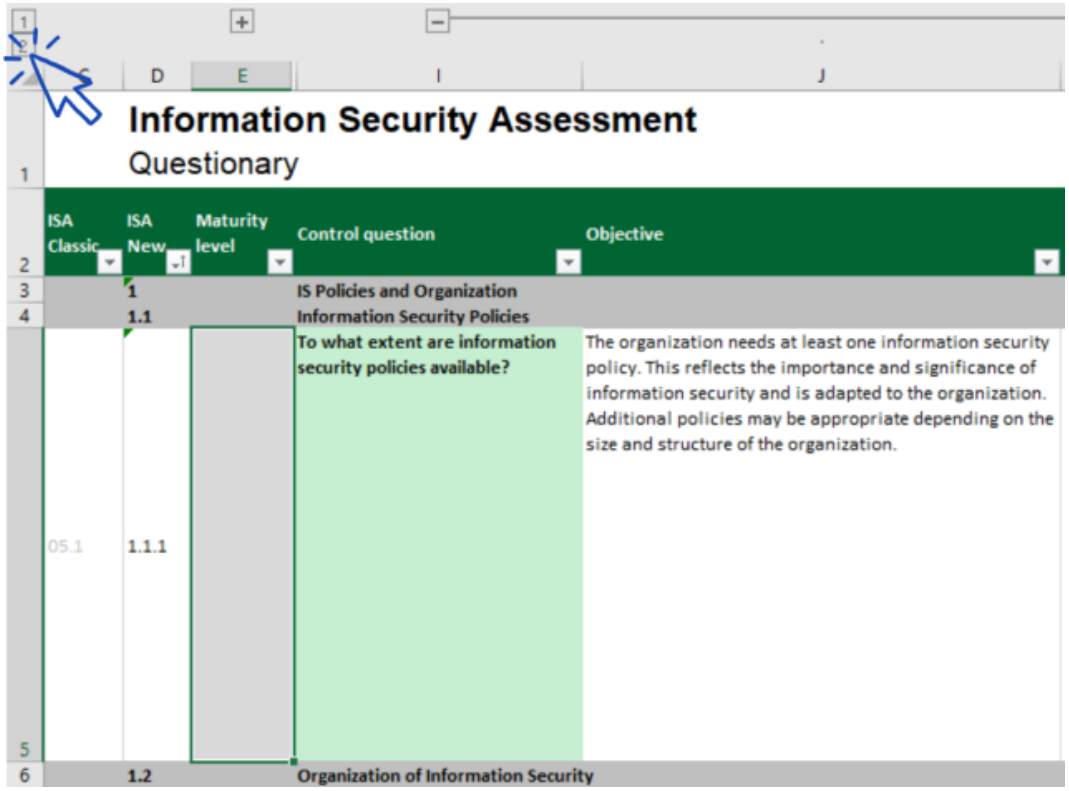
Apenas a breve descrição da sua implementação e a referência à sua documentação são obrigatórias. Essas informações vão ajudar nossos provedores de auditoria TISAX a entender melhor sua empresa e a preparar a avaliação.

Existem mais colunas opcionais para apoiar sua autoavaliação:

- Measures/recommendations (🇵🇹 Measures/recommendations (Medidas/recomendações)) (Coluna R)
- Date of assessment (🇵🇹 Date of assessment (Data da avaliação)) (Coluna S)
- Date of completion (🇵🇹 Date of completion (Data da conclusão)) (Coluna T)
- Responsible department (🇵🇹 Responsible department (Departamento responsável)) (Coluna U)
- Contact (🇵🇹 Contact (Contato)) (Coluna V)

Observação importante:

Se você abrir o arquivo Excel baixado e selecionar uma das planilhas da lista de critérios (por exemplo, Segurança da informação), provavelmente não verá imediatamente os campos do formulário de autoavaliação. Para mostrá-los, você precisa clicar no botão de agrupamento para o nível “2”[14]. O botão está acima e à esquerda da célula C1. Isso vai expandir a visualização para mostrar os campos do formulário de autoavaliação.



Outra dica é usar as teclas de seta para rolar para baixo. Porque devido ao grande tamanho das células, a rolagem com a barra de rolagem pode exigir excelentes habilidades motoras finas. Se você usar o recurso de rolagem do seu dispositivo indicador, você também poderá ignorar acidentalmente algumas das células maiores.

5.2.2.5. Objetivo

À direita da coluna “Control question” (Pergunta de controle) está a coluna “Objective” (Objetivo) (coluna J). Seu conteúdo descreve o que você precisa alcançar em relação a esse aspecto de gerenciamento de segurança da informação.

Exemplo (para a pergunta de controle 4.1.2): “Apenas usuários identificados de forma segura (autenticados) podem obter acesso aos sistemas de TI. Para essa finalidade, a identidade de um usuário é determinada de forma segura por procedimentos adequados.”

5.2.2.6. Requisitos

Os requisitos são o que é esperado que você cumpra para alcançar o objetivo.

Os requisitos estão distribuídos em quatro colunas:

1. Requirements (must) (Requirements (must) (Requisitos (obrigatórios) (Coluna K))
2. Requirements (should) (Requirements (should) (Requisitos (obrigatórios) (Coluna L))
3. Additional requirements for high protection needs (Additional requirements for high protection needs (Requisitos adicionais para necessidades de proteção elevada)) (Coluna M)
4. Additional requirements for very high protection needs (Additional requirements for very high protection needs (Requisitos adicionais para necessidades de proteção muito elevada)) (Coluna N)

Você deve cumprir todos os requisitos até a necessidade de proteção que precisar alcançar (que pode ser derivada do seu objetivo da avaliação).

Para alguns objetivos da avaliação, apenas um subconjunto de requisitos é aplicável. Para obter mais informações sobre a relevância dos requisitos, consulte a Tabela 8, “Relevância dos requisitos aos objetivos da avaliação” em Seção 5.2.2.1, “Lista de critérios” e especialmente em note no final da seção.

Para obter mais informações sobre as definições da ISA dos níveis de requisitos “must” (obrigatórios) e “should” (obrigatórios), consulte os “Termos-chave” na planilha Excel “Definições”.

Observação importante:

É muito importante que você entenda que deve interpretar cada requisito no contexto e na essência do objetivo. Mesmo o cumprimento minucioso de um requisito não garante que o provedor de auditoria confirme que você o cumpre no contexto e na essência do objetivo (coluna J).

Os requisitos e sua redação são baseados em uma implementação teórica por uma empresa média fictícia de tamanho desconhecido.

O provedor de auditoria deve sempre pesar o objetivo em relação à implementação exclusiva em sua empresa. O que é apropriado para uma empresa média pode não ser suficiente em sua situação específica.

Para obter mais informações, consulte a Seção 5.2.5, “Abordar o resultado da autoavaliação”.

5.2.2.7. Níveis de maturidade

A ISA usa o conceito de “maturity levels” (🇵🇹 “níveis de maturidade”) para atribuir uma classificação à qualidade de todos os aspectos do seu sistema de gerenciamento de segurança da informação. Quanto mais sofisticado for o seu sistema de gerenciamento de segurança da informação, mais elevado será o seu nível de maturidade.

A ISA diferencia seis níveis de maturidade. Você pode encontrar a definição detalhada na planilha Excel “Maturity levels” (🇵🇹 “Níveis de maturidade”). Para uma visão consolidada dos níveis de maturidade, citamos as descrições informais fornecidas na ISA:

Maturity level (🇵🇹 Nível de maturidade)	**Em uma palavra**	**Descrição**
0	Incomplete (🇵🇹 Incompleto)	Um processo não está disponível, não é seguido ou não é adequado para alcançar o objetivo.
1	Performed (🇵🇹 Realizado)	Um processo não documentado ou documentado de forma incompleta é seguido e existem indicadores de que ele alcança seu objetivo.
2	Managed (🇵🇹 Gerenciado)	É seguido um processo que alcança seus objetivos. A documentação do processo e as evidências de implementação do processo estão disponíveis.
3	Established (🇵🇹 Estabelecido)	É seguido um processo padrão integrado ao sistema geral. As dependências de outros processos são documentadas e são criadas interfaces adequadas. Existem evidências de que o processo foi usado de forma sustentável e ativa por um longo período.
4	Predictable (🇵🇹 Previsível)	É seguido um processo estabelecido. A eficácia do processo é monitorada continuamente através da coleta de números-chave. São definidos valores-limite nos quais o processo é considerado insuficientemente eficaz e exige ajuste. (Principais indicadores de desempenho)
5	Optimizing (🇵🇹 Otimização)	É seguido um processo previsível com melhoria contínua como objetivo principal. A melhoria é ativamente promovida por recursos dedicados.

Tabela 10. Descrição informal dos níveis de maturidade

Você precisa avaliar o nível de maturidade do seu sistema de gerenciamento de segurança da informação de acordo com a pergunta. Insira seu nível de maturidade na coluna “Maturity level” (🇵🇹 “Maturity level” (Nível de maturidade)) (coluna E).

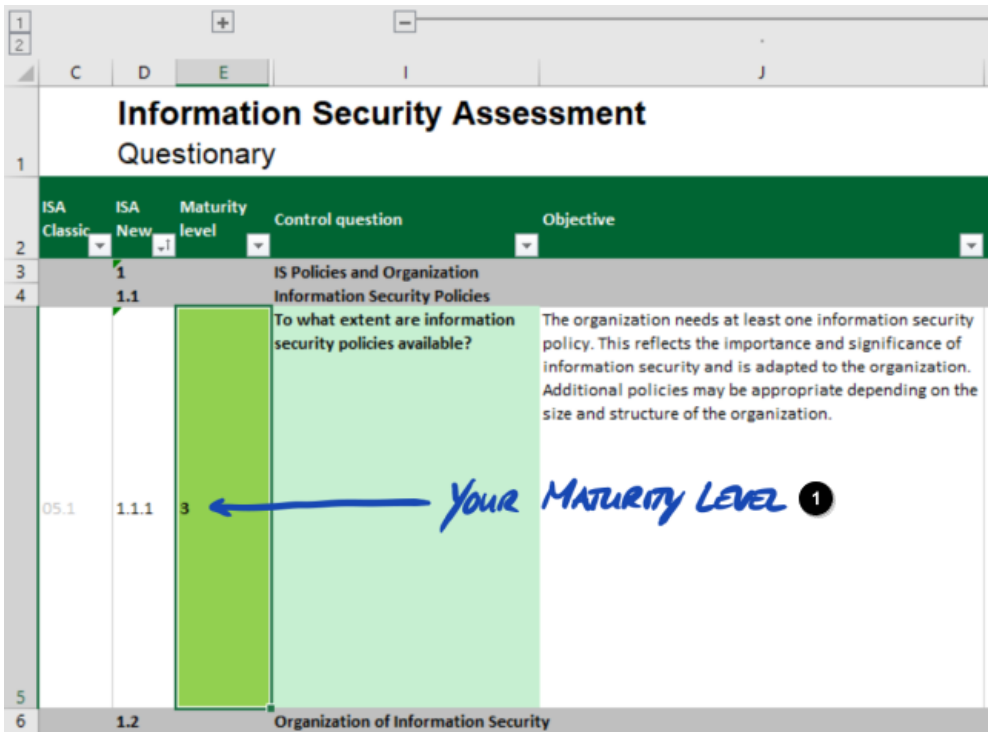


Figura 12. Captura de tela: exemplo de seleção de nível de maturidade no documento da ISA (planilha Excel "Segurança da informação")

1 Seu nível de maturidade

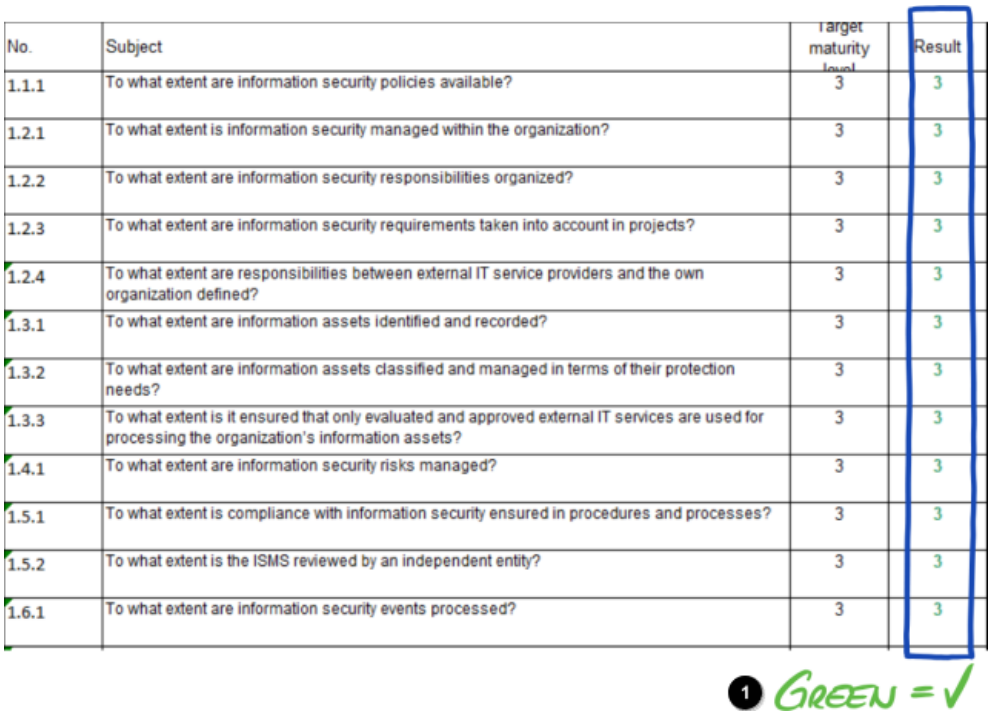
Para obter mais informações sobre os níveis de maturidade desejados e seu impacto no resultado da sua avaliação, consulte a Seção 5.2.4, "Interprete o resultado da autoavaliação".

Com esse entendimento aprimorado, agora você está pronto para iniciar a autoavaliação.

5.2.3. Faça a autoavaliação

Abra o arquivo do Excel e percorra todas as perguntas de controle de cada lista de critérios que se apliquem ao(s) seu(s) objetivo(s) da avaliação e defina o nível de maturidade que corresponda ao estado atual do seu sistema de gerenciamento de segurança da informação. Faça isso com base em seu melhor discernimento. Não existe certo ou errado nessa fase.

Depois de concluída a autoavaliação, a coluna "Result" (Resultado) (H) da planilha Excel "Resultados (ISA5)" deverá ser totalmente preenchida, seja com números (0–5) ou "n.a." (como em "não aplicável").



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

Figura 13. Captura de tela: exemplo de planilha "Resultados (ISA5)" no documento da ISA

1 Verde

Se você tiver dúvidas sobre a ISA, entre em contato conosco.

5.2.4. Interprete o resultado da autoavaliação

As próximas cinco subseções explicam como analisar e interpretar o resultado da sua autoavaliação. A análise dirá se você está pronto ou não para uma avaliação TISAX.

5.2.4.1. Análise

A pontuação do seu resultado resume o resultado da autoavaliação.

Você encontra a pontuação do resultado ("Resultado com redução para o nível de maturidade desejado") na planilha Excel "Resultados (ISA5)" (célula D6). Explicaremos a "redução" em breve.

Information Security Assessment Results

VDA Verband der Automobilindustrie

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

YOUR RESULT SCORE 1 MAXIMUM RESULT SCORE 2

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

Figura 14. Captura de tela: sua pontuação do resultado e a pontuação máxima do resultado (planilha Excel "Resultados (ISA5)", células D6 e G6)

1. Sua pontuação do resultado
2. Pontuação máxima do resultado

Para entender e posteriormente interpretar o resultado da sua autoavaliação e a pontuação do seu resultado, você precisa diferenciar dois níveis de análise:

1. Na pergunta
   Esse nível tem todas as perguntas. Para cada pergunta, existe um nível de maturidade desejado e o seu nível de maturidade.
2. Nível da pontuação
   Nesse nível, fica o resultado geral que resume os resultados de todas as perguntas. Existe uma pontuação máxima do resultado e sua pontuação do resultado.

A figura abaixo mostra os níveis da análise:

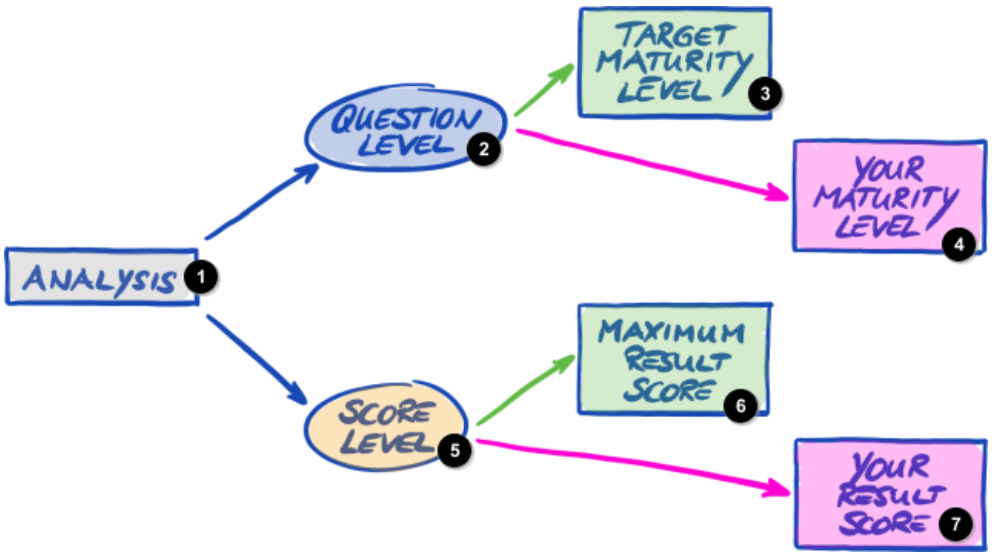


Figura 15. Análise do resultado da autoavaliação na pergunta e no nível da pontuação

1. Análise
2. Na pergunta
3. Nível de maturidade desejado
4. Seu nível de maturidade
5. Nível da pontuação
6. Pontuação máxima do resultado
7. Sua pontuação do resultado

A figura abaixo mostra onde encontrar os resultados no nível da pontuação e os resultados na pergunta:

Figura 16. Nível da pontuação e na pergunta na planilha Excel "Resultados (ISA5)"

1. Nível da pontuação
2. Na pergunta

A próxima figura mostra uma visão simplificada dos níveis da análise, as definições desejadas da ISA e seus próprios resultados:

Figura 17. As metas e seus resultados na pergunta e no nível da pontuação

1. Nível de maturidade desejado
2. Seu nível de maturidade
3. Na pergunta
4. P (Pergunta)
5. TML (Nível de maturidade desejado)
6. YML (Seu nível de maturidade)
7. Pontuação máxima do resultado
8. Sua pontuação do resultado
9. Nível da pontuação

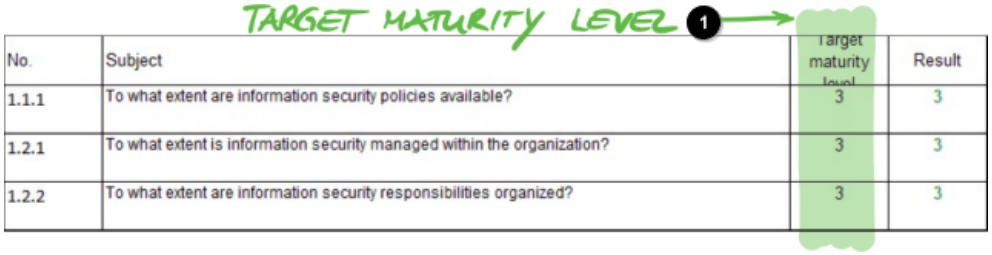
As seções a seguir explicam o resultado e sua análise em detalhes.

5.2.4.2. O nível de maturidade desejado (na pergunta)

A ISA define um “nível de maturidade desejado” de 3 para cada pergunta.

Para obter mais informações sobre a definição de cada nível de maturidade, consulte Seção 5.2.2, “Entenda o documento da ISA”.

A ISA define os níveis de maturidade desejado na planilha Excel “Resultados (ISA5)” (começando na coluna G, linha 22; consulte a figura abaixo).



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. A definição do nível de maturidade desejado na planilha Excel “Resultados (ISA5)”

1. Nível de maturidade desejado

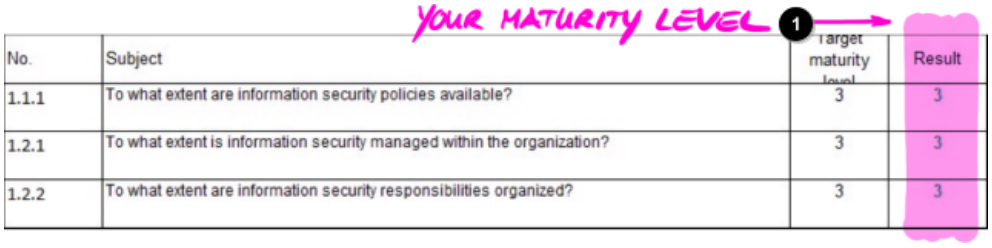
5.2.4.3. Seu resultado (na pergunta)

Para receber selos TISAX, normalmente você precisa ter níveis de maturidade para cada pergunta iguais ou superiores ao nível de maturidade desejado.

Exemplo: se o nível de maturidade desejado para a pergunta X for “3”, o seu nível de maturidade para essa pergunta deverá ser “3” ou superior. Se o seu nível de maturidade para essa pergunta for inferior a “3”, você poderá não receber os selos TISAX.

Isso ocorre em cada pergunta. Se o nível de maturidade desejado para duas perguntas for “3”, você não poderá compensar um nível de maturidade de “2” para uma pergunta com um nível de maturidade de “4” para a outra pergunta.

O documento da ISA transfere automaticamente seus níveis de maturidade da planilha Excel “Segurança da Informação” (coluna E) para a planilha Excel “Resultados (ISA5)” (começando na coluna H, linha 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. Seus níveis de maturidade na planilha Excel “Resultados (ISA5)”

1. Seu nível de maturidade desejado

Seu nível de maturidade está sujeito a um cálculo antes que o documento da ISA o resuma em sua pontuação do resultado. Basicamente, seu nível de maturidade é “reduzido” ao nível de maturidade desejado. Isso é feito para que as perguntas em que seu nível de maturidade esteja *acima* do nível de maturidade desejado não compensem as perguntas em que seu nível de maturidade esteja *abaixo* do nível de maturidade desejado.

Veja como a ISA calcula seu resultado na pergunta:

- Ele pega o seu nível de maturidade e o compara com o nível de maturidade desejado da pergunta.
- Se o seu nível de maturidade estiver acima do nível de maturidade desejado, ele será “reduzido” para o nível de maturidade desejado.
- Se o seu nível de maturidade estiver abaixo ou igual ao nível de maturidade desejado, nada acontecerá para essa pergunta.

Exemplo (consulte a figura abaixo): o nível de maturidade desejado é “3”. Seu nível de maturidade é “4”. Seu “resultado de redução” para essa pergunta será “3”.

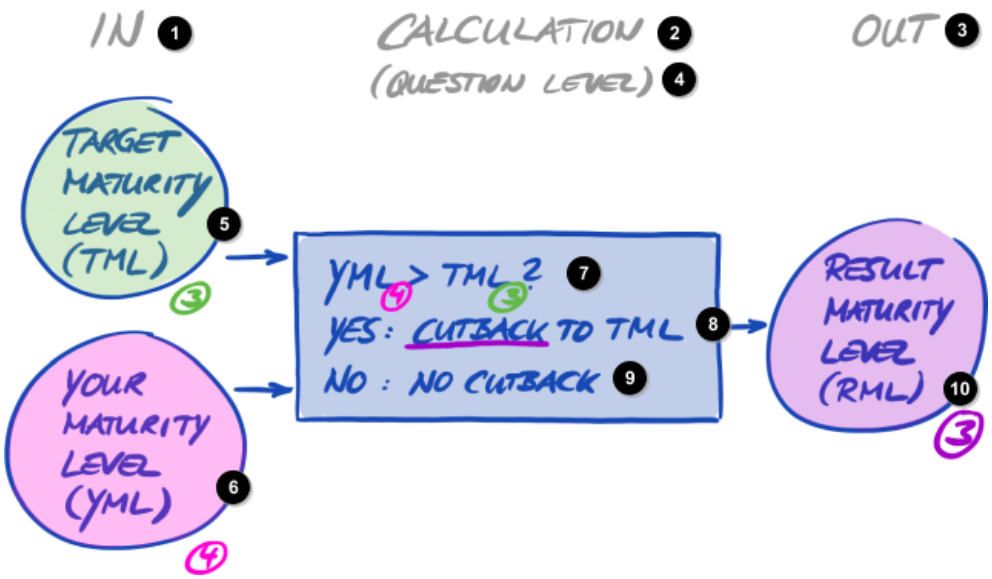


Figura 20. Cálculo da redução do nível de maturidade do resultado

1. Entrada
2. Cálculo
3. Saída
4. (Na pergunta)
5. Nível de maturidade desejado (TML)

6. Seu nível de maturidade (YML)
7. YML > TML?
8. Sim: redução para TML
9. Não: sem redução
10. Nível de maturidade do resultado (RML)

A figura abaixo mostra que se o seu nível de maturidade for superior ao nível de maturidade desejado, a ISA o reduzirá (as cores verde, laranja e vermelho correspondem às cores usadas na coluna “Resultado”, consulte a Figura 19, “Seus níveis de maturidade na planilha Excel “Resultados (ISA5)””).

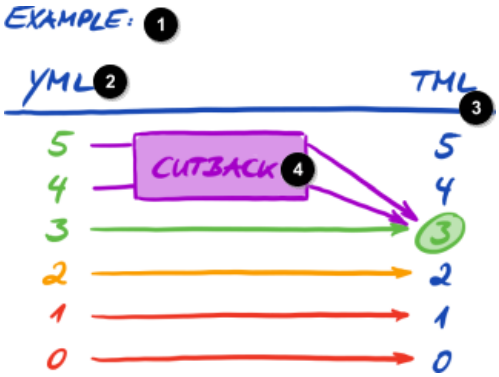


Figura 21. Ilustração da redução com as cores utilizadas na planilha Excel “Resultados (ISA5)”

1. Exemplo:
2. YML
3. TML
4. Redução

Abaixo está outra maneira de visualizar os níveis de maturidade na pergunta. As cores dos círculos ilustram o nível de maturidade desejado ou a “distância” até ele (exemplo: o círculo é laranja se o nível de maturidade estiver “-1” abaixo do nível de maturidade desejado). As marcas de seleção ilustram seu nível de maturidade.

Figura 22. Níveis de maturidade na pergunta

1. Nível de maturidade
2. Pergunta
3. Redução
4. Nível de maturidade desejado (TML)
5. Um ou mais acima do TML
6. Um abaixo do TML
7. Dois ou mais abaixo do TML
8. Seu nível de maturidade (YML)
9. Redução para TML

Observe:

É possível passar com sucesso em uma avaliação TISAX mesmo que você não atinja o nível de maturidade desejado em todas as perguntas. A pergunta principal nesses casos é se você corre um risco relevante. Se o seu nível de maturidade estiver abaixo do valor desejado, mas não houver risco, isso pode ser satisfatório.

5.2.4.4. A meta (no nível da pontuação)

A ISA define um nível de maturidade geral “ideal” — a “pontuação máxima do resultado” (ou “pontuação máxima”, célula 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 ❶
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 23. Pontuação máxima do resultado (planilha Excel "Resultados (ISA5)")

❶ Pontuação máxima do resultado

Teoricamente, este nível de maturidade global é a média de todos os níveis de maturidade desejados (na pergunta). Esta seria uma pontuação máxima do resultado de "3,0".

No entanto, é "3,0" apenas se todas as perguntas forem aplicadas à sua situação. Assim que uma pergunta não for aplicável à sua situação, a média muda e a pontuação máxima do resultado é inferior a "3,0".

Com base na visualização mostrada acima (Figura 22, "Níveis de maturidade na pergunta"), você pode ver abaixo o que é colocado na média para a pontuação máxima do resultado:

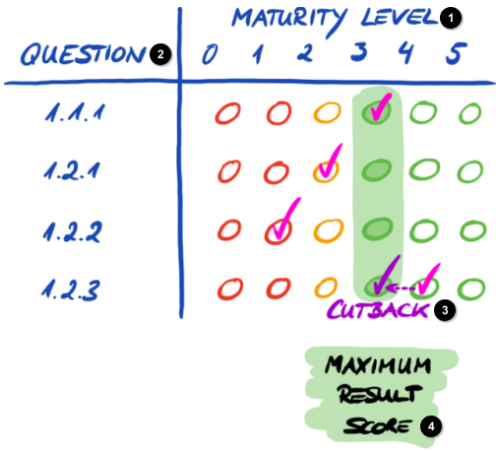


Figura 24. A pontuação máxima do resultado (no nível da pontuação)

❶ Nível de maturidade

❷ Pergunta

❸ Redução

❹ Pontuação máxima do resultado

5.2.4.5. Seu resultado (no nível da pontuação)

Sua pontuação geral do resultado (“Resultado com redução para os níveis de maturidade desejados”, célula D6):

- resume o nível geral de maturidade do seu sistema de gerenciamento de segurança da informação.
- é a média de todos os seus níveis de maturidade desejados (na pergunta).
- pode ser inferior ou igual à pontuação máxima do resultado.
- deve estar o mais próximo possível da pontuação máxima do resultado. Quanto mais a pontuação do seu resultado estiver abaixo da pontuação máxima do resultado, menor será a probabilidade de você receber os selos 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. Sua pontuação do resultado (planilha Excel “Resultados (ISA5)”)

❶ Sua pontuação do resultado

Novamente, usando uma visualização mostrada acima (Figura 22, “Níveis de maturidade na pergunta”), você pode ver abaixo o que é colocado na média da pontuação do resultado:

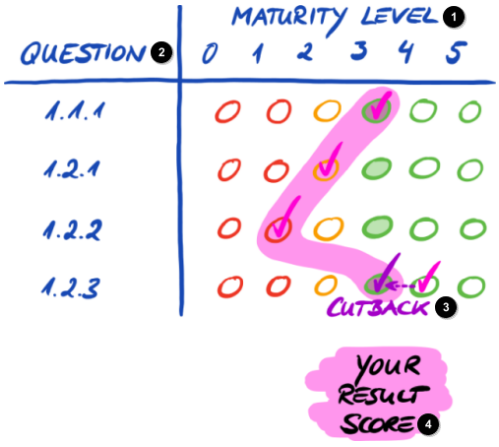


Figura 26. Sua pontuação do resultado (no nível da pontuação)

❶ Nível de maturidade

2. Pergunta
3. Redução
4. Sua pontuação do resultado

A pontuação do resultado informa se você:

- está pronto para uma avaliação TISAX.
- pode esperar receber os selos TISAX.

Se a pontuação do seu resultado (“Resultado com redução para os níveis de maturidade desejados”) estiver abaixo de “3,0”, então pelo menos em uma pergunta o seu nível de maturidade não corresponde ao nível de maturidade desejado. Nesse caso, você provavelmente deve melhorar seu sistema de gerenciamento de segurança da informação antes de estar pronto para a sua avaliação TISAX.

Observe:

Para a pontuação geral, existem limites formais para uma “distância” aceitável entre a pontuação do seu resultado e a pontuação máxima do resultado (“Resultado com redução para os níveis de maturidade desejados”).

Se a pontuação do resultado for superior a:

- 10% abaixo, o resultado geral da avaliação será “não conformidade menor”.
- 30% abaixo, o resultado geral da avaliação será “não conformidade importante”.

Observação importante:

Ter uma pontuação de resultado (“Resultado com redução para os níveis de maturidade desejados”) de “3” não é uma garantia de que você passará na avaliação TISAX sem quaisquer achados proibitivos. Tenha em mente que o provedor de auditoria pode ver alguns aspectos de maneira diferente da sua.

5.2.4.6. Você está pronto?

O objetivo da análise acima é saber se você está pronto para uma avaliação TISAX.

Você está definitivamente pronto para uma avaliação TISAX se a pontuação do seu resultado (“Resultado com redução para os níveis de maturidade desejados”) for (próximo de) “3,0”. Nesse caso, todos os valores da coluna “Results” (Resultados) (H) são verdes (sem laranja ou vermelho).

Se não estiverem verdes, você precisará abordar o resultado da sua autoavaliação (consulte

Seção 5.2.5, “Abordar o resultado da autoavaliação”).

A figura abaixo mostra o gráfico de teia de aranha da ISA na planilha Excel “Resultados (ISA5)”. A linha verde marca o nível de maturidade desejado de acordo com o capítulo. Se seus níveis de maturidade estiverem dentro ou acima dessa linha, você está pronto para uma avaliação TISAX. Se estiverem abaixo dessa linha, isso pode não ser suficiente para receber os selos TISAX.

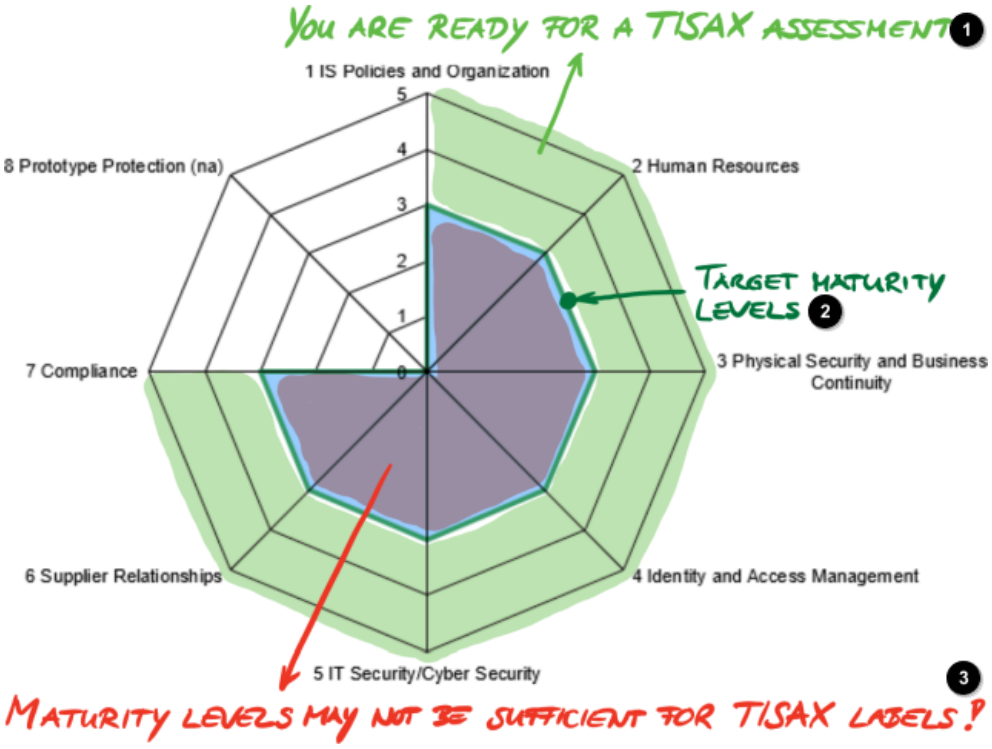


Figura 27. Captura de tela: realização do nível de maturidade desejado no gráfico de teia de aranha da ISA (planilha Excel “Resultados (ISA5)”)

1. Você está pronto para uma avaliação TISAX
2. Níveis de maturidade desejados
3. Os níveis de maturidade podem não ser suficientes para os selos TISAX!

Se você “desdobrar” a teia de aranha da ISA para a pergunta, você obterá uma visualização semelhante verde/vermelho na pergunta:

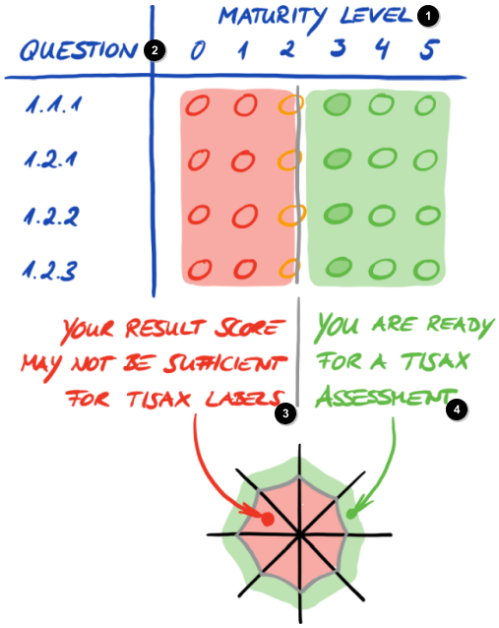


Figura 28. "Desdobrando" o gráfico de teia de aranha da ISA

1. Nível de maturidade
2. Pergunta
3. Sua pontuação do resultado pode não ser suficiente para os selos TISAX
4. Você está pronto para uma avaliação TISAX

5.2.5. Abordar o resultado da autoavaliação

O resultado da sua autoavaliação pode mostrar que você precisa melhorar seu sistema de gerenciamento de segurança da informação antes de estar pronto para receber os selos TISAX.

Você já deve saber como resolver algumas lacunas entre o seu nível de maturidade e o nível de maturidade desejado. Para outros, você pode precisar de aconselhamento externo. Nesse caso, você pode solicitar serviços de consultoria aos nossos provedores de auditoria TISAX. O TISAX permite a consulta, mas não exige. Observe que qualquer provedor de auditoria que preste consultoria para você não poderá mais realizar as avaliações TISAX para você.

Observação importante:

Não abordar adequadamente o resultado da autoavaliação *antes* de ser avaliada é um grande obstáculo para muitas empresas. Não subestime o esforço que pode ser necessário para configurar seu sistema de gerenciamento de segurança da informação de acordo com os requisitos. Muitas empresas precisam estabelecer formalmente um grande projeto para se prepararem para uma avaliação TISAX.

Observe:

Ao procurar ajuda externa para passar pelo processo TISAX, você descobrirá que várias empresas oferecem serviços de consultoria e treinamento. Nenhuma dessas empresas está associada conosco.

Na situação atual, nós:

- não oferecemos treinamentos oficiais, seja diretamente ou através de terceiros.
- não fazemos nenhuma declaração sobre a qualidade dos serviços de terceiros e, portanto, aconselhamos cautela.

Observe:

Aconselhamos não solicitar ou pedir itens como uma “pré-avaliação” ou uma “análise de lacunas”. Embora reconheçamos o desejo de nos prepararmos para a avaliação dessa forma, em quase todos os casos faz mais sentido iniciar a avaliação imediatamente.

Para obter mais informações sobre o motivo pelo qual desaconselhamos pré-avaliações, consulte Seção 7.7, “Anexo: A lógica contra “avaliações prévias” e “análises de lacunas””.

5.3. Seleção do provedor de auditoria

Apenas os provedores de auditoria que contratamos podem realizar as avaliações TISAX[15]. Os provedores de auditoria TISAX estão autorizados a realizar avaliações TISAX para você apenas se não tiverem tido nenhuma atribuição anterior de consultoria com você.

Todos os nossos provedores de auditoria TISAX são obrigados a realizar avaliações TISAX apenas para as empresas que são participantes cadastradas no TISAX.

Observação importante:

Depois de cadastrar o escopo da avaliação TISAX, você *deve* começar a entrar em contato com nossos provedores de auditoria. Eles têm um determinado prazo de entrega quanto à sua disponibilidade. Entrar em contato com eles *após* terminar suas preparações pode causar um atraso desnecessário.

Observe:

Cada escopo da avaliação passa por um ciclo de vida. Nessa fase, o escopo da

sua avaliação deve ter o status “Aprovado” ou “Cadastrado”

Para obter mais informações sobre o status de um escopo da avaliação, consulte a Seção 7.5.5, “Assessment scope status “Awaiting your payment” (Status do escopo da avaliação “Awaiting your payment” (Aguardando seu pagamento))”.

5.3.1. Informações de contato

Depois de registrar um escopo de avaliação TISAX, você pode entrar em contato com todos os provedores de auditoria TISAX e solicitar propostas. Suas informações de contato são fornecidas no e-mail de confirmação de cadastro que você recebeu[16] (Consulte Seção 4.5.8, “E-mail de confirmação”).

Observe:

Solicite propostas dos nossos provedores de auditoria TISAX somente após a conclusão do seu cadastro. Os provedores de auditoria verificarão se já existe um cadastro. Eles precisam rejeitar solicitações sem cadastro.

Esse também é o motivo pelo qual você recebe as informações de contato do provedor de auditoria apenas no e-mail de confirmação de cadastro e não em nosso site público.

5.3.2. Abrangência

Embora atualmente muitos dos contatos dos provedores de auditoria estejam sediados na Alemanha, é importante entender que todos os nossos provedores de auditoria são geralmente capazes de realizar as avaliações TISAX em todo o mundo. A maioria deles tem até funcionários próprios em muitos países.

Em nosso site, oferecemos uma página onde você pode selecionar seu país e ver qual provedor de auditoria tem equipe de vendas local e/ou auditores locais (enx.com/en-US/TISAX/xap/).

5.3.3. Solicitação de propostas

Para permitir que os nossos provedores de auditoria TISAX calculem com precisão os esforços da avaliação esperados, você deve sempre incluir o “TISAX scope excerpt” (extrato do escopo TISAX).

Figura 29. Miniatura de um extrato do escopo (primeira página)

Para obter mais informações, consulte a Seção 4.5.8, “E-mail de confirmação”.

Observe:

A imparcialidade é uma característica fundamental dos nossos provedores de auditoria TISAX. Eles vão garantir que não exista nenhum conflito de interesses. Você pode considerar isso ao entrar em contato com eles. Se sua empresa estiver de alguma forma relacionada a um provedor de auditoria, não é possível esperar ser avaliado por ele.

5.3.4. Avaliação de propostas

Você pode escolher livremente entre todos os nossos provedores de auditoria TISAX. Todos estão vinculados ao mesmo contrato. Todos realizam as avaliações com base nos mesmos critérios e nos mesmos métodos de auditoria. Em termos do resultado da avaliação, não haverá diferença, independentemente do provedor de auditoria que você escolher. O resultado da sua avaliação será aceito por todos os participantes TISAX.

Além de fatores óbvios como preço, reputação e amabilidade, existem alguns aspectos de uma proposta que você pode procurar:

- Disponibilidade:
  Quando é possível começar o processo de avaliação? Esse pode ser um aspecto importante se a avaliação TISAX for urgente para você.
- Custos relacionados a viagens para consultas presenciais:
  Os provedores de auditoria com escritórios no seu país podem ter custos mais baixos relacionados a viagens.
- Idioma:
  Você e todos os outros entrevistados em sua empresa poderão se comunicar com o auditor em seu idioma nativo?
- Escopo da proposta:
  Quais avaliações estão incluídas?

Para obter mais informações sobre as avaliações, consulte Seção 5.4.3, “Tipos de avaliação TISAX”.
Normalmente, as propostas incluem a avaliação inicial e a avaliação do plano de ação corretiva. Como é difícil prever os esforços das avaliações de acompanhamento, elas costumam ser oferecidas após a conclusão das outras avaliações.

Em última análise, tudo se resumirá à confiança. Você vai precisar formar uma relação de confiança com seu provedor de auditoria, pois ele terá um profundo conhecimento de sua empresa.

Observe:

Aconselhamos não solicitar ou pedir itens como uma “pré-avaliação” ou uma “análise de lacunas”. Embora reconheçamos o desejo de nos prepararmos para a avaliação dessa forma, em quase todos os casos faz mais sentido iniciar a avaliação imediatamente.

Para obter mais informações sobre o motivo pelo qual desaconselhamos pré-avaliações, consulte Seção 7.7, “Anexo: A lógica contra “avaliações prévias” e “análises de lacunas””.

Observe:

Embora certamente gostaríamos de dizer quanto nossos provedores de auditoria vão cobrar pela avaliação, pedimos a sua compreensão de que não podemos fornecer essas informações. Os custos dependem de muitos fatores. Além disso, nossos provedores de auditoria são livres em relação aos seus cálculos comerciais.

No entanto, podemos mencionar algumas estimativas aproximadas de quantos dias-homem nossos provedores de auditoria vão cobrar de você. Para uma empresa pequena comum com uma única localização, é razoável esperar gastar de três dias e meio a quatro dias-homem em uma avaliação no nível de avaliação 2 e de cinco a seis dias-homem em uma avaliação no nível de avaliação 3.

Observe:

Cada avaliação passa por um ciclo de vida.

Para obter mais informações sobre o status de uma avaliação, consulte a Seção 7.6, “Anexo: Assessment status (Status da avaliação)”.

Depois de escolher um dos nossos provedores de auditoria TISAX, você poderá finalmente

iniciar o processo de avaliação TISAX.

5.4. Processo de avaliação TISAX

5.4.1. Visão geral

O processo de avaliação TISAX consiste em vários tipos de avaliações. Na maioria dos casos, haverá mais de uma avaliação.

Você deve ver o processo de avaliação como uma sequência entrelaçada de etapas onde:

- Você prepara seu sistema de gerenciamento de segurança da informação para estar em excelente condição.
- O provedor de auditoria verifica se o seu sistema de gerenciamento de segurança da informação atende a um conjunto definido de requisitos. Ele pode encontrar lacunas.
- Em seguida, você preenche as lacunas dentro de períodos definidos.
- O provedor de auditoria verifica novamente se você preencheu as lacunas.

Essas etapas alternadas são realizadas até que todas as lacunas sejam preenchidas.

É importante entender que *você* inicia cada subetapa do processo de avaliação. Todo o processo de avaliação está sob seu controle. E é claro que cabe a você interromper e sair do processo de avaliação sempre que desejar.[17]

O processo de avaliação TISAX tem a seguinte macroestrutura:

- Reunião inicial
  Você e o provedor de auditoria planejam os detalhes do processo de avaliação
- Fase 1 de avaliação
  O provedor de auditoria verifica sua autoavaliação
- Fase 2 de avaliação
  O provedor de auditoria realiza a(s) avaliação(ões)

5.4.2. Reunião inicial

O processo de avaliação TISAX começa com a reunião inicial. É o local para planejar os detalhes do processo de avaliação. Normalmente, a reunião inicial é feita em uma teleconferência. O provedor de auditoria vai orientar você durante a reunião.

Entre outros, os seguintes tópicos estarão na agenda:

- Quem são os participantes da reunião?
- Quem é a empresa avaliada?

- Como funciona o processo de avaliação TISAX?
- Qual é o escopo da avaliação e ele é o correto?
- Não há conflitos de interesses?
- Como é uma boa autoavaliação?
- Quem é responsável por fazer o quê?
- Como nos comunicamos?
- Quando ocorre a avaliação (e outro planejamento de tempo)?
- Quem precisa participar da(s) avaliação(ões)?
- Com quem você pode entrar em contato quando tiver reclamações?

O período entre o final da reunião inicial e a entrega da sua autoavaliação é normalmente de um a três meses. Mas mesmo seis meses não é incomum. O período depende do status da sua preparação. O TISAX não impõe nenhum prazo para este período. Você pode levar todo o tempo necessário para preparar sua autoavaliação e ficar pronto para a avaliação.

5.4.3. Tipos de avaliação TISAX

O processo de avaliação TISAX é composto por estes três tipos de avaliações TISAX:

- Avaliação inicial (Initial assessment)
- Avaliação do plano de ação corretiva (Corrective action plan assessment)
- Avaliação de acompanhamento (Follow-up assessment) [18]

A avaliação inicial sempre será realizada. As outras duas avaliações TISAX podem acontecer e podem se repetir várias vezes. Elas acontecerão:

- até você preencher todas as lacunas
- ou você sair do processo de avaliação TISAX
- ou você atingir o período máximo de nove meses após o término da reunião de encerramento da avaliação inicial (momento em que outra avaliação inicial será necessária).

Todas as avaliações TISAX serão descritas nas próximas seções.

Observe:

Cada avaliação passa por um ciclo de vida.

Para obter mais informações sobre o status de uma avaliação, consulte a Seção 7.6, “Anexo: Assessment status (Status da avaliação)”.

5.4.4. Elementos da avaliação TISAX

Cada avaliação TISAX é composta pelos seguintes elementos:

- Reunião formal de abertura[19][20]
  - Seu objetivo é cobrir todos os tópicos da organização.
  - Não precisa ser necessariamente uma reunião física.
  - Os tópicos podem ser abordados de uma só vez ou distribuídos em diversas ocasiões.
  - É um “recipiente lógico” para todos os tópicos da avaliação *prévia* da organização.
- Procedimento de avaliação
  - Seu provedor de auditoria verifica todos os requisitos.
  - Os métodos de avaliação são selecionados de acordo com o respectivo nível de avaliação.
- Reunião formal de encerramento[21]
  - Ela conclui uma avaliação TISAX.
  - O provedor de auditoria apresenta seus achados.
  - O provedor de auditoria anuncia o resultado da avaliação.
  - Não precisa ser necessariamente uma reunião física.
  - É um “recipiente lógico” para todos os tópicos de *pós*-avaliação da organização.

Após a “reunião de encerramento”, o provedor de auditoria prepara e envia para você a versão preliminar do “relatório de avaliação TISAX” atualizado. Você pode apresentar objeções se acreditar que o provedor de auditoria interpretou algo de forma equivocada.[22] Em seguida, o provedor de auditoria emite o “relatório de avaliação TISAX” final.

Todos esses elementos serão descritos nas próximas seções.

5.4.5. Sobre a conformidade

Antes de continuarmos descrevendo o processo de avaliação TISAX, queremos explicar um conceito importante que é essencial para a sua compreensão das próximas seções.

A finalidade de uma avaliação TISAX é determinar se o seu sistema de gerenciamento de segurança da informação atende a um conjunto definido de requisitos. O provedor de auditoria verifica se o seu sistema de gerenciamento de segurança da informação “está em conformidade” (🇬🇧 “conforms”) com os requisitos.

Etapa 1: as verificações são feitas para cada requisito aplicável de forma individual.

Se a sua abordagem estiver “em conformidade” com todos os requisitos, você passa na avaliação e recebe os selos TISAX que correspondem aos seus objetivos da avaliação.

Tudo o que estiver abaixo da conformidade total ou ideal com os requisitos é chamado de achado (🇬🇧 finding). O TISAX diferencia quatro tipos de achados:

N.º	Tipo	Definição	Reação	Exemplos
1.	Não conformidade *importante* (🇬🇧 *Major* non-conformity)	Uma não conformidade *importante*: ▪ cria um risco imediato significativo para a segurança da sua informação ▪ **ou** cria dúvidas quanto à eficácia geral do seu sistema de gerenciamento de segurança da informação	Você precisa: ▪ abordar não conformidades *importantes* imediatamente com medidas de compensação adequadas ▪ implementar ações corretivas sem atrasos indevidos	▪ Não conformidades sistemáticas ▪ Déficits de implementação que criam riscos críticos para a segurança de informações confidenciais ▪ Déficits de implementação que não são resolvidos por uma ação corretiva adequada
2.	Não conformidade *menor* (🇬🇧 *Minor* non-conformity)	Uma não conformidade *menor*: ▪ *não* cria um risco imediato significativo para a segurança da sua informação ▪ **e** *não* cria dúvidas quanto à eficácia geral do seu sistema de gerenciamento de segurança da informação	Você precisa: ▪ implementar ações corretivas sem atrasos indevidos	▪ Erros isolados ou esporádicos ▪ Não conformidade ou déficits na implementação de requisitos ou de suas políticas

N.º	Tipo	Definição	Reação	Exemplos
3.	Observação (Observation)	Uma observação representa uma não conformidade com os requisitos ou suas próprias políticas que não cria um risco imediato para a segurança da informação, mas que pode criar em algum momento no futuro.	Você precisa: ▪ investigar, monitorar e avaliar cuidadosamente possíveis riscos ▪ decidir como lidar com a observação	N/A
4.	Espaço para melhorias (Room for improvement)	Uma irregularidade que não pertence aos tipos mencionados anteriormente e que não coloca em risco a segurança de suas informações, mas claramente oferece oportunidade para melhorias evidentes.	Você pode decidir se ou como abordar esse tipo de achado.	N/A

Tabela 11. Os quatro tipos de achados:

Etapa 2: todos os resultados da etapa anterior “de acordo com o requisito” são misturados no resultado geral da avaliação.

O resultado geral da avaliação pode ser:

a. Em conformidade (Conform)
   O resultado geral da avaliação está “conforme”. Todos os requisitos foram atendidos.

b. Não conformidade menor (Minor non-conform)
   O resultado geral da avaliação é “não conformidade menor” se você tiver pelo menos uma “não conformidade menor” para um requisito.

c. Não conformidade importante (Major non-conform)
   O resultado geral da avaliação é “não conformidade importante” se você tiver pelo menos uma “não conformidade importante” para um requisito.
   (Sem um plano de ação corretiva aprovado, toda não conformidade resulta em um resultado geral de avaliação de “não conformidade importante”.)

Se o resultado geral da sua avaliação for:

- “não conformidade menor”, você pode receber os selos TISAX *temporários* até que todas as não conformidades sejam resolvidas.
- “não conformidade importante”, você deve primeiro resolver o respectivo problema antes de receber qualquer selo TISAX.
  Com medidas compensatórias apropriadas e ações corretivas aprovadas pelo provedor de auditoria, é possível alterar o resultado geral da sua avaliação de “não conformidade importante” para “não conformidade menor” e, assim, receber os selos TISAX temporários.

É importante entender que o resultado geral da sua avaliação melhorará durante todo o processo de avaliação TISAX.

Considere esse exemplo simplificado: você pode ter um resultado geral da avaliação de “não conformidade grave” após a avaliação inicial. Depois você ameniza o risco correspondente. Isso altera o resultado geral da sua avaliação de “não conformidade importante” para “não conformidade menor”. E uma vez eliminado o risco, o resultado final da sua avaliação geral será “conforme”.

Tudo isso será explicado a seguir com muito mais detalhes. E você pode descobrir mais sobre os selos TISAX mais abaixo em Seção 5.4.14, “Selos TISAX”.

5.4.6. Sua preparação para o processo de avaliação TISAX

O provedor de auditoria vai preparar a avaliação com base na sua autoavaliação. Portanto, saiba que você deve disponibilizar sua autoavaliação ao seu provedor de auditoria com antecedência. Os prazos exatos de entrega são determinados na reunião inicial.

Um provedor de auditoria bem preparado vai reduzir o tempo necessário para a avaliação. Além da autoavaliação, ele também vai solicitar a documentação relacionada antes da avaliação. Pode ser a documentação referenciada na autoavaliação e outra documentação que o provedor de auditoria considere relevante.

Com base nessas informações, seu provedor de auditoria vai planejar o procedimento de avaliação.

5.4.7. Avaliação inicial

Essa é a primeira avaliação TISAX e marca o início formal do processo de avaliação TISAX.

Observação importante:

A avaliação inicial marca o início de dois períodos importantes:

1. O período máximo de validade dos selos TISAX é de três anos.
2. Você tem até nove meses para solucionar as não conformidades. Se você não solucionar todas as não conformidades dentro desse prazo, você não

receberá os selos TISAX. Se você perdeu esse prazo, poderá continuar diretamente com uma nova avaliação inicial.

Os períodos têm início no dia da reunião de encerramento da avaliação inicial.

Observe:

Além dos dois períodos descritos acima, não existem outras restrições de tempo. Por exemplo, nem a conclusão do processo de cadastro on-line, nem o contato com os nossos provedores de auditoria ou mesmo a realização da reunião inicial acionam quaisquer prazos. Cabe a você começar com a avaliação inicial.

5.4.7.1. A primeira reunião formal de abertura

Como todas as avaliações TISAX, a avaliação inicial começa com uma reunião formal de abertura. A reunião formal de abertura normalmente é feita em uma videoconferência ou teleconferência. Nas pequenas empresas, com experiência em auditorias anteriores, isso não demora muito.

A finalidade dessa reunião é:

- verificar os pré-requisitos da avaliação
- apresentar o líder do projeto de avaliação e a equipe de avaliação
- planejar a avaliação

5.4.7.2. Procedimento de avaliação

De acordo com o plano preparado, o provedor de auditoria realiza a avaliação inicial. Como isso se apresentará em detalhes depende dos seus objetivos da avaliação. A avaliação consiste principalmente em teleconferências, entrevistas no local e inspeções no local em vários graus de profundidade[23].

O provedor de auditoria apresenta todos seus achados durante a avaliação inicial.

5.4.7.3. Reunião de encerramento

Na reunião de encerramento, seu provedor de auditoria resume novamente todos os seus achados.

5.4.7.4. Relatório de avaliação TISAX

Após a reunião de encerramento, o provedor de auditoria prepara e envia para você a versão preliminar do “relatório de avaliação TISAX”. Você pode apresentar objeções se acreditar que o provedor de auditoria interpretou algo de forma equivocada.[24] Em seguida, o provedor de

auditoria emite o “relatório de avaliação TISAX”.

Nessa fase, o resultado da avaliação geral atual será:

- Conforme, ou
- Não conformidade importante
  Ter não conformidades (menores) não abordadas sempre resulta em um resultado geral da avaliação de “não conformidade importante”. O resultado geral da sua avaliação só poderá ser “não conformidade menor” depois que você definir as ações que vão implementar as medidas para solucionar as não conformidades.
  Para obter mais informações sobre como conseguir isso, consulte Seção 5.4.9.4, “Selos TISAX temporários”.

Se o resultado geral da sua avaliação estiver “conforme” logo na avaliação inicial, você pode ignorar o restante da seção de avaliação e prosseguir para o compartilhamento do seu resultado.

Se o resultado geral da sua avaliação for “não conformidade grave”, a sua próxima tarefa é elaborar um plano sobre como abordar os achados e como preencher quaisquer lacunas encontradas pelo provedor de auditoria. O plano é oficialmente chamado de “plano de ação corretiva” (“corrective action plan”).

Observe:

Se, antes do início da avaliação, você souber de uma situação que vai resultar em uma não conformidade e não conseguir corrigi-la antes da avaliação, você já poderá planejar uma ação corretiva (incluindo uma data de implementação) e apresentá-la ao provedor de auditoria durante a avaliação. Isso, teoricamente, poderia levar a um resultado geral da avaliação de “não conformidade menor”. No entanto, essa seria uma situação *rara*.

5.4.8. Preparação do plano de ação corretiva

Seu “plano de ação corretiva” (“corrective action plan”) define como você planeja abordar os achados da avaliação inicial. Seu provedor de auditoria vai avaliar a adequação do seu “plano de ação corretiva” (veja a próxima seção).

Para criar o seu “plano de ação corretiva”, você deve considerar os seguintes requisitos:

- Achado
  - Você precisa indicar qual achado a ação corretiva aborda.
- Causa raiz
  - Você precisa identificar e declarar a causa raiz do achado.

- Ações corretivas
  - Para cada não conformidade é necessário definir uma ou mais “ações corretivas”, que vão implementar as medidas que solucionem a não conformidade.
- Data de implementação
  - Você precisa definir uma data de implementação para cada ação corretiva.
  - O período de implementação deve proporcionar tempo suficiente para implementar completamente as medidas.
- Medidas compensatórias
  - Para todas as não conformidades que criem riscos críticos, é necessário definir as medidas compensatória que abordem as não conformidades até que as ações corretivas sejam implementadas.
- Período de implementação
  - Em todas as ações corretivas que levem mais de três meses para serem implementadas, você precisa justificar o período de implementação.
  - Em todas as ações corretivas que levem mais de seis meses, você também precisa fornecer evidências que demonstrem que uma implementação mais rápida não seria possível.
  - O período de implementação de qualquer ação corretiva não pode ser superior a nove meses.

Assim que seu plano de ação corretiva for concluído, você poderá solicitar a “avaliação do plano de ação corretiva”.

Observação importante:

Recomendamos começar com a implementação o mais rápido possível. Não há necessidade de esperar pelo resultado da “avaliação do plano de ação corretiva”.
A “avaliação do plano de ação corretiva” normalmente ocorre depois que você envia seu plano de ação corretiva ao seu provedor de auditoria.

Observe:

O TISAX tem requisitos apenas em relação ao conteúdo e não quanto à forma dos planos de ação corretiva.
A maioria dos nossos provedores de auditoria oferece modelos para planos de ação corretiva.

5.4.9. Avaliação do plano de ação corretiva

A finalidade da “avaliação do plano de ação corretiva” é verificar se o seu “plano de ação corretiva” (veja acima) atende aos requisitos do TISAX.

Você envia seu “plano de ação corretiva” ao seu provedor de auditoria. Seu provedor de auditoria avalia o plano de acordo com os requisitos (veja abaixo). Se o seu plano atender aos requisitos, seu provedor de auditoria emitirá o “relatório de avaliação TISAX” atualizado.

Essa avaliação normalmente não demora muito. Na maioria dos casos, será uma videoconferência ou teleconferência. Às vezes, isso é feito apenas por e-mail.

5.4.9.1. Motivos para uma avaliação do plano de ação corretiva

Os motivos para uma “avaliação do plano de ação corretiva” são:

- Não conformidades restantes após
  - uma avaliação inicial
  - uma avaliação de acompanhamento
  - uma avaliação da ampliação do escopo
- Um “plano de ação corretiva” que já foi avaliado, mas não atendeu aos requisitos
- Os fatores de influência nos quais se baseia o cálculo dos períodos de implementação de um plano de ação corretiva mudaram

5.4.9.2. Combinação com avaliação inicial

A “avaliação do plano de ação corretiva” não é necessariamente um evento independente. Você tem a opção de já apresentar seu “plano de ação corretiva” na reunião de encerramento da avaliação inicial. O provedor de auditoria poderá então realizar diretamente a “avaliação do plano de ação corretiva”.

Se você combinar a “avaliação do plano de ação corretiva” com a avaliação inicial, e seu “plano de ação corretiva” atender aos requisitos, você poderá chegar a um acordo com o provedor de auditoria de que não precisa de um “relatório de avaliação inicial”. Em vez disso, o seu provedor de auditoria apenas prepararia o “relatório de avaliação do plano de ação corretiva”. Esse relatório permite que você receba os selos TISAX temporários diretamente.

5.4.9.3. Requisitos do plano de ação corretiva

O provedor de auditoria avalia seu “plano de ação corretiva” em relação aos seguintes requisitos:

- As medidas são adequadas
  - O provedor de auditoria vai avaliar a adequação de uma ação corretiva com base na

solução da causa raiz da não conformidade.

- Os riscos críticos são amenizados com medidas compensatórias adequadas[25]
- Os períodos de implementação são adequados
  - Os períodos de implementação começam no dia em que a avaliação inicial foi concluída
- Nenhum período de implementação pode ser superior a:
  - três meses sem justificativa adicional
  - seis meses sem justificativa e evidências adicionais
  - nove meses

5.4.9.4. Selos TISAX temporários

Se o resultado geral da sua avaliação for “não conformidade menor”, você receberá os selos TISAX temporários.

A vantagem dos selos TISAX temporários é que seu parceiro normalmente os aceita sob a condição de que você receba posteriormente os rótulos TISAX definitivos. Isso pode ajudar se for urgente provar a eficácia do seu sistema de gerenciamento de segurança da informação ao seu parceiro.

O pré-requisito para selos TISAX temporários é um relatório de avaliação do plano de ação corretiva com o resultado geral da avaliação “não conformidade menor”.

Os selos TISAX temporários são iguais aos selos TISAX definitivos. A única diferença é o período de validade mais curto dos selos TISAX temporários.

Os selos TISAX temporários podem ser válidos por até nove meses após a reunião de encerramento da avaliação inicial. O período de validade dos selos TISAX temporários é determinado pelo período mais longo de implementação das ações corretivas.

Exemplos:

- Você tem apenas uma não conformidade. Você precisa fazer uma revisão da política. O período de implementação associado é de *dois* meses.
  Então, seus selos TISAX temporários serão válidos por *dois* meses.
- Você tem a não conformidade da revisão da política citada. Além disso, você tem uma não conformidade onde é necessário construir uma nova parede externa como ação corretiva. Devido ao tempo necessário para obter as aprovações necessárias do município, o período de implementação associado é de *oito* meses.
  Então, seus selos TISAX temporários serão válidos por *oito* meses.

Para obter mais informações sobre os requisitos para os períodos de implementação, consulte Seção 5.4.9.3, “Requisitos do plano de ação corretiva”

Observe:

A “avaliação do plano de ação corretiva” é opcional.

Você poderá prosseguir diretamente para a avaliação de acompanhamento se:

- não precisar dos selos TISAX temporários e
- estiver confiante com a implementação de quaisquer ações corretivas sem que seu plano seja aprovado pelo seu provedor de auditoria

Depois de concluir todas as ações corretivas, você deverá solicitar a “avaliação de acompanhamento”.

5.4.10. Avaliação de acompanhamento

A finalidade da “avaliação de acompanhamento” é avaliar se todas as não conformidades previamente identificadas foram solucionadas. Normalmente você solicita a avaliação de acompanhamento quando tiver certeza de que todas as não conformidades foram solucionadas.

Mas você pode fazer quantas avaliações de acompanhamento precisar. Se durante uma avaliação de acompanhamento seu provedor de auditoria ainda atestar não conformidades existentes ou mesmo novas, basta atualizar seu plano de ação corretiva e iniciar esta parte do processo de avaliação novamente.

Essa avaliação pode ser uma reunião física, bem como uma videoconferência ou teleconferência.

5.4.10.1. Cronograma

Seu provedor de auditoria pode realizar a(s) avaliação(ões) de acompanhamento dentro de até nove meses após a conclusão da avaliação inicial[26].

5.4.10.2. Pré-requisitos

Se você não precisar dos selos TISAX temporários, poderá solicitar diretamente uma avaliação de acompanhamento. Você não precisa ter uma “avaliação do plano de ação corretiva” antes de uma avaliação de acompanhamento.

5.4.10.3. Vencimento dos selos TISAX temporários

Caso você precise dos selos TISAX temporários, você pode desejar garantir que não haja nenhuma lacuna no recebimento dos selos TISAX definitivos. Portanto, recomendamos solicitar sua avaliação de acompanhamento bem antes da última data possível[27]. O motivo é que você deseja ter tempo suficiente para abordar quaisquer achados menores identificados durante uma avaliação de acompanhamento.

5.4.11. Diagrama do processo de avaliação TISAX

As seções anteriores estão agora resumidas no seguinte diagrama do processo:

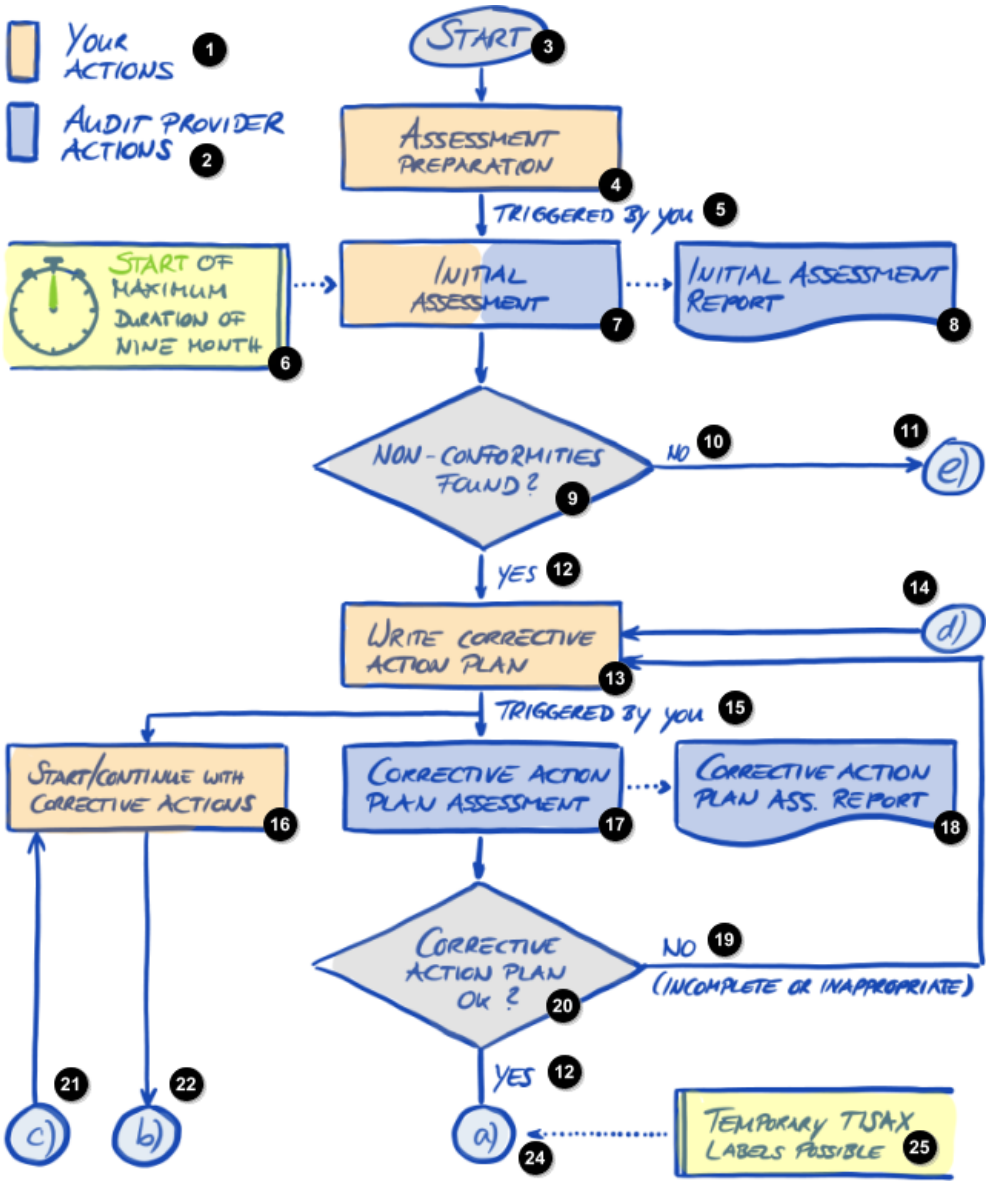


Figura 30. Diagrama do processo de avaliação TISAX (parte 1/2)

1. Suas ações
2. Ações do provedor de auditoria
3. Início
4. Preparação da avaliação
5. Acionada por você
6. Início da duração máxima de nove meses

7. Avaliação inicial
8. Relatório da avaliação inicial
9. Foram encontradas não conformidades?
10. Não
11. e)
12. Sim
13. Escrever um plano de ação corretiva
14. d)
15. Acionada por você
16. Iniciar/continuar com as ações corretivas
17. Avaliação do plano de ação corretiva
18. Relatório da avaliação do plano de ação corretiva
19. Não (incompleto ou inadequado)
20. Plano de ação corretiva ok?
21. c)
22. b)
24. a)
25. Possíveis selos TISAX temporários

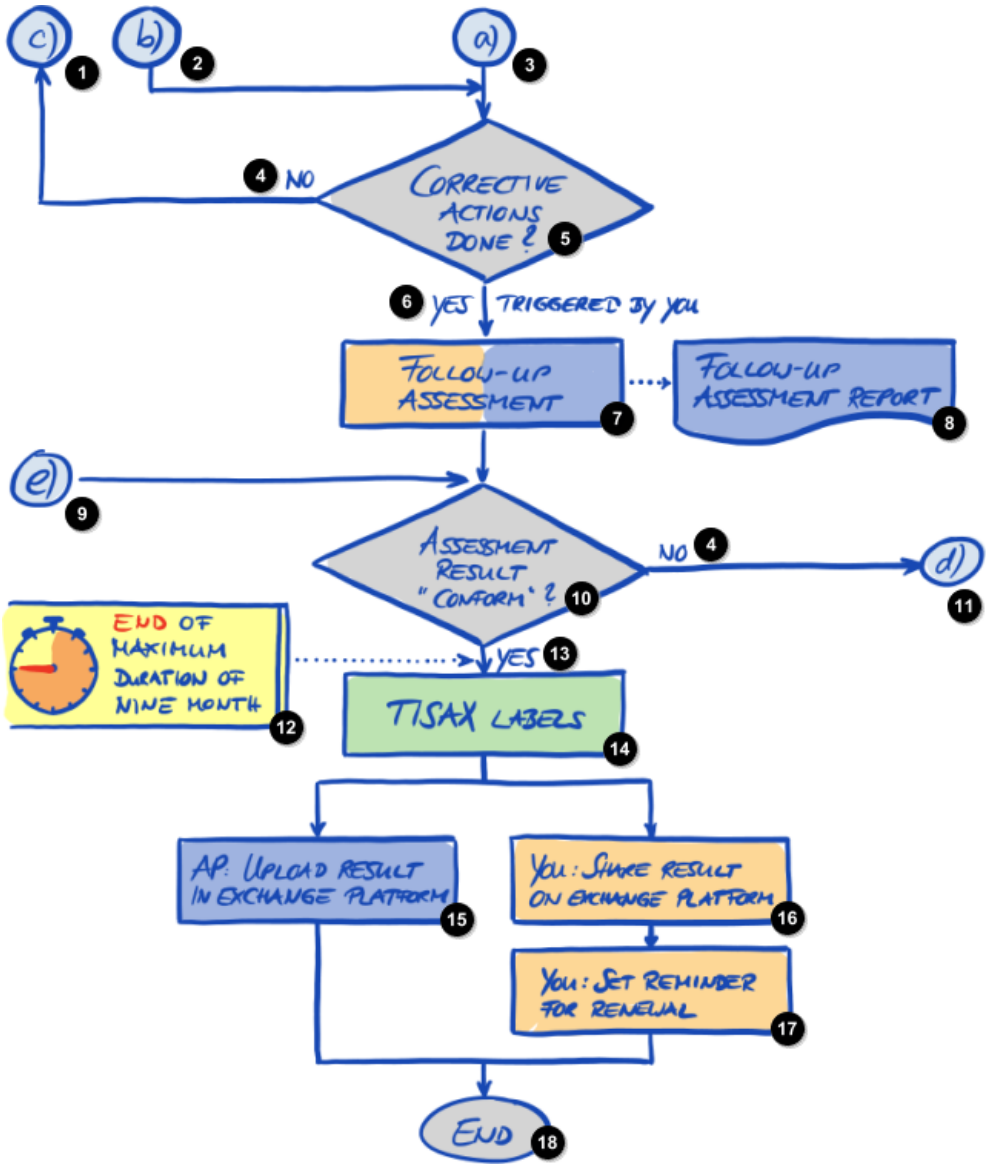


Figura 31. Diagrama do processo de avaliação TISAX (parte 2/2)

1. c)
2. b)
3. a)
4. Não
5. Ações corretivas realizadas?
6. Sim, acionadas por você
7. Avaliação de acompanhamento
8. Relatório da avaliação de acompanhamento
9. e)

10. O resultado da avaliação está “em conformidade”?
11. d)
12. Final da duração máxima de nove meses
13. Sim
14. Selos TISAX
15. Provedor de auditoria: carregar resultado na plataforma de compartilhamento
16. Você: compartilhe o resultado na plataforma de compartilhamento
17. Você: defina lembretes para a renovação
18. Fim

5.4.12. Assessment ID (🇵🇹 ID da avaliação)

Cada avaliação TISAX de um escopo de avaliação é identificada por um “ID da avaliação”. Esse ID se refere ao resultado da sua avaliação e ao relatório de avaliação TISAX correspondente.

O ID da avaliação é assim:

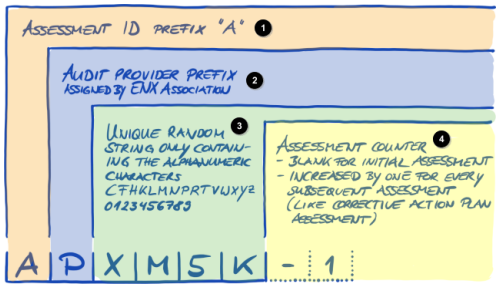


Figura 32. Formato do ID da avaliação

1. Prefixo do ID da avaliação “A”
2. Prefixo do provedor de auditoria atribuído pela ENX Association
3. String aleatória exclusiva, contendo apenas os caracteres alfanuméricos:
   CFHKLMNPRTVWXYZ
   0123456789
4. Marcador da avaliação
   - Em branco para a avaliação inicial
   - Aumento de um para cada avaliação subsequente (como avaliação do plano de ação corretiva)

O ID da avaliação normalmente é usado quando seu provedor de auditoria se comunica com você.

5.4.13. Relatório de avaliação TISAX

O “Relatório de avaliação TISAX” (“TISAX assessment report”):

- é (atualizado e) emitido após cada avaliação TISAX.
- documenta os achados do seu provedor de auditoria.
- contém o resultado geral da avaliação (conforme, não conformidade menor, não conformidade importante).
- contém todas as outras informações relacionadas à sua avaliação TISAX (como objetivo da avaliação, escopo, pessoas envolvidas e localizações).

O “relatório de avaliação TISAX” pode ser dos seguintes tipos (dependendo do tipo de avaliação):

- Relatório da avaliação *inicial* (*Initial* assessment report)
- Relatório da avaliação do *plano de ação corretiva* (*Corrective action plan* assessment report)
- *Relatório da avaliação de acompanhamento* (*Follow-up* assessment report) [28]

O “relatório de avaliação TISAX” tem sempre a mesma estrutura[29]. Seu provedor de auditoria simplesmente amplia isso após cada tipo de avaliação. Isso significa que você só precisa lidar com a última versão do relatório de avaliação TISAX, pois ele sempre contém o conteúdo da(s) versão(ões) mais antiga(s).

As primeiras seções do “relatório de avaliação TISAX” são o que você compartilha com o seu parceiro.

Uma das principais características do TISAX é que cabe totalmente a você decidir quais partes do relatório de avaliação TISAX deseja compartilhar com seu parceiro ou com qualquer outro participante. A estrutura do relatório de avaliação TISAX foi concebida para permitir este tipo de compartilhamento seletivo. Cada seção expande o nível de detalhes.

Aqui está a estrutura do “relatório de avaliação TISAX”:

- A. Informações relacionadas à avaliação
  Nome da empresa, escopo da avaliação, ID do escopo, ID da avaliação, nível de avaliação, objetivo(s) da avaliação, data(s) da avaliação, provedor de auditoria
  Essa seção não contém nenhum resultado da avaliação.
- B. Resultados resumidos
  Resumo do gerenciamento do resultado da avaliação (conforme, não conformidade menor, não conformidade importante), quantidade de achados, categorização abstrata dos riscos resultantes
- C. Resumo do resultado da avaliação
  Resumo do resultado da avaliação de acordo com o capítulo (por exemplo “9 Controle de

acesso”) e com a lista de critérios (por exemplo “Segurança da informação”)

- D. Níveis de maturidade da VDA ISA (aba de resultados)
  Nível de maturidade para cada requisito
- E. Resultados detalhados da avaliação
  Descrição detalhada de todos os achados, resultados correspondentes da avaliação de risco, medidas necessárias, período de implementação

Na etapa de “compartilhamento” (detalhada abaixo) você decide até que nível seu parceiro terá acesso ao conteúdo do seu relatório de avaliação TISAX.

5.4.14. Selos TISAX

Abordamos brevemente este tópico na seção de preparação para cadastro. Conforme explicado, o que antes era um objetivo de avaliação agora se tornou um selo TISAX.

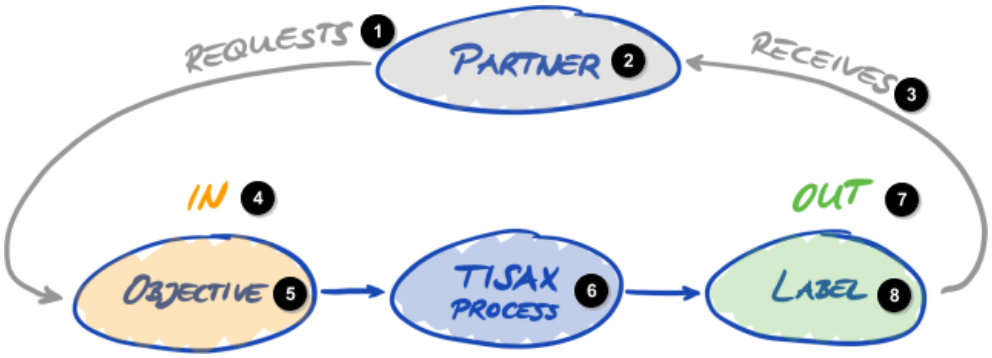


Figura 33. Objetivos da avaliação e selos TISAX

1. Solicita
2. Parceiro
3. Recebe
4. ENTRADA
5. Objetivo
6. Processo TISAX
7. SAÍDA
8. Selo

Os selos TISAX:

- são o resultado do processo de avaliação TISAX.
- resumem o resultado da sua avaliação.
- são a afirmação de que o seu sistema de gerenciamento de segurança da informação atende

a um conjunto definido de requisitos.

O uso dos selos TISAX facilita a comunicação relacionada ao TISAX com seu parceiro e seu provedor de auditoria TISAX, porque eles se referem a uma saída definida do processo de avaliação TISAX.

5.4.14.1. Hierarquia dos selos TISAX

O mapeamento entre os objetivos da avaliação e os selos TISAX correspondentes é bastante simples. Mas existe outro aspecto importante: *Alguns* selos TISAX estão hierarquicamente vinculados. Isso significa que se você receber um determinado selo TISAX, receberá automaticamente os selos TISAX “abaixo” desse selo específico.

Exemplo: se o seu objetivo da avaliação for “Very high availability”, você receberá o selo TISAX “Very high availability” correspondente. Mas como o objetivo da avaliação “Very high availability” é um superconjunto de “High availability”, você também receberá automaticamente o selo TISAX “High availability”.

Essa hierarquia existe atualmente para esses selos TISAX:

- O “Info high” é um superconjunto de “Confidential” e “High availability”.
- O “Info very high” é um superconjunto de “Strictly confidential” e “Very high availability”.
- O “Strictly confidential” é um superconjunto de “Confidential”.
- O “Very high availability” é um superconjunto de “High availability”.
- O “Special data” é um superconjunto de “Data”.

Observe:

Você também pode receber os selos TISAX de forma retroativa. Quando introduzimos um novo selo que é um subconjunto de um dos selos TISAX que você já recebeu, você receberá automaticamente o novo selo.

Exemplo: você recebeu o selo TISAX “Info high” em um momento em que o selo “High availability” ainda não existia. Quando introduzimos o selo High availability, nosso sistema o atribuiu automaticamente a você.

Essas relações hierárquicas podem ser obtidas através da comparação dos requisitos aplicáveis conforme especificados em Tabela 8, “Relevância dos requisitos aos objetivos da avaliação”.

Isso pode não parecer importante para todos os participantes. Mas imagine que um parceiro solicite que você mostre o selo TISAX “Very high availability” e outro solicite o selo TISAX “High availability”. Então, ter os dois selos TISAX facilita muito para todos, porque ninguém precisa entender que “High availability” é um subconjunto de “Very high availability”. Isso pode ser particularmente verdadeiro para parceiros onde ter determinados selos TISAX faz parte de um

processo de compra bastante rigoroso. Você certamente não vai querer explicar que “Very high availability” é “melhor” que “High availability”. Basta mostrar todos os seus selos TISAX e a pessoa que faz a avaliação pode simplesmente marcar o requisito “deve ter o selo TISAX 'High availability'“.

5.4.14.2. Período de validade dos selos TISAX

Os selos TISAX são geralmente válidos por três anos. O período de validade começa no final do processo de avaliação (mesmo antes da emissão do relatório de avaliação TISAX).

O seu período de validade pode ser mais curto se algo significativo no âmbito da avaliação TISAX mudar.

Exemplos: mudança da sua empresa, novas localizações. (Para obter instruções sobre o que fazer nesses casos, consulte Seção 7.9.3.2, “Como solicitar a mudança de uma localização)” e Seção 7.9.3.4, “Como adicionar uma outra localização”.)

Observe:

Você pode visualizar seus selos TISAX apenas no portal ENX. Eles não são registrados no relatório de avaliação TISAX.

5.4.14.3. Renovação dos selos TISAX

Para manter seus selos TISAX por longo prazo, você precisa renová-los.[30] em seguida, a cada três anos.

Para isso, basicamente você precisa passar novamente pelo processo TISAX (cadastrar um escopo de avaliação, ser avaliado novamente pelo TISAX e compartilhar seu resultado de avaliação). O cadastro é um pouco mais fácil, pois você não precisa recriar sua empresa como participante TISAX. E é claro que você pode reutilizar todos os seus contatos e localizações que já estão armazenados no banco de dados do TISAX.

Observação importante:

ANTES de entrar em contato com o seu provedor de auditoria, cadastre um NOVO escopo Seu provedor de auditoria poderá iniciar um novo processo de avaliação somente se você fornecer um novo ID do escopo.

Na maioria dos casos, é fácil cadastrar um novo escopo. Você precisa apenas atribuir um novo nome de escopo, adicionar contatos, selecionar o(s) objetivo(s) da avaliação e adicionar localizações. Você pode reutilizar os contatos e as localizações que já estão no sistema de qualquer escopo cadastrado anteriormente.

Observação importante:

Reutilize os registros da localização existentes que foram criados e usados durante o cadastro do seu escopo anterior. Não crie um novo registro da localização com o mesmo endereço.

O motivo: alguns participantes do TISAX processam automaticamente os resultados da avaliação dos seus parceiros. Eles sincronizam seu próprio sistema com o portal ENX. Até mesmo pequenas diferenças podem bloquear o sucesso da sincronização. Além disso, você não sobrecarrega os dados dos participantes com duplicatas desnecessárias.

Observação importante:

Se a condição for ter selos TISAX válidos durante toda a relação com seu parceiro, recomendamos de forma enfática que você coloque um lembrete em seu calendário para iniciar o processo de renovação necessário.

Recomendamos iniciar a renovação pelo menos um ano antes de seus selos TISAX vencerem.

Agora que você recebeu seus selos TISAX, você pode prosseguir para a última etapa e compartilhá-los com seu parceiro.

6. Compartilhamento (Etapa 3)

O tempo estimado de leitura da seção de compartilhamento é de 7 minutos.

Você já passou pelo processo TISAX até agora, mas seu parceiro ainda não viu nenhuma “prova” de que seu sistema de gerenciamento de segurança da informação é capaz de proteger seus dados confidenciais. Essa seção descreve agora como compartilhar o resultado da sua avaliação com o seu parceiro e apresentar a prova solicitada.

6.1. Premissa

Uma das principais características do TISAX é que o resultado da sua avaliação esteja totalmente sob seu controle. Sem sua permissão explícita, todas as informações relacionadas à sua avaliação não serão compartilhadas com ninguém.

6.2. A plataforma de compartilhamento

O portal ENX disponibiliza a plataforma de compartilhamento.

Seu provedor de auditoria vai fazer o upload das duas primeiras seções (A e B) do seu relatório de avaliação TISAX. Nessa fase, as informações não estão disponíveis para ninguém, exceto você.

Você pode utilizar a conta criada durante o cadastro para acessar o portal e utilizar a plataforma de compartilhamento.

Você pode acessar o portal neste endereço:
enx.com/en-US/SignIn

6.3. Pré-requisitos gerais

Você pode compartilhar o resultado da sua avaliação com seu parceiro somente se estes dois pré-requisitos forem atendidos:

1. Seu provedor de auditoria enviou o resultado da avaliação para a plataforma de compartilhamento.
   Normalmente, o resultado da avaliação estará disponível na plataforma de compartilhamento entre 5 a 10 dias úteis após a emissão do relatório de avaliação TISAX.
2. Recebemos o pagamento da taxa (se aplicável).

O status do seu escopo de avaliação é “Active” (Ativo) quando os pré-requisitos são atendidos.

Observe:

> Cada escopo da avaliação passa por um ciclo de vida. Nessa fase, o escopo da sua avaliação deve ter o status “Active” (Ativo).
>
> Para obter mais informações sobre o status de um escopo da avaliação, consulte a Seção 7.5.5, “Assessment scope status “Awaiting your payment” (Status do escopo da avaliação “Awaiting your payment” (Aguardando seu pagamento))”.

Para verificar se o resultado da sua avaliação está pronto para compartilhamento (status do escopo da avaliação = Active (Ativo)), siga estas etapas:

1. Faça login no portal ENX.
2. Acesse a barra de navegação principal e selecione “MY TISAX” (“MY TISAX” (MEU TISAX)).
3. No menu suspenso, selecione “SCOPES AND ASSESSMENTS” (“SCOPES AND ASSESSMENTS” (ESCOPOS E AVALIAÇÕES)).
4. Vá até a tabela e encontre a linha da tabela com o escopo da sua avaliação.
5. Verifique se o seu escopo da avaliação tem o status do escopo da avaliação “Active” (“Active” (Ativo)) (coluna “Scope Status” (“Scope Status” (Status do Escopo))).

6.4. Permanência dos resultados compartilhados

> Observação importante:
>
> Você não pode revogar nenhuma permissão de publicação ou compartilhamento.
>
> O motivo é que queremos que todos os participantes passivos possam contar com acesso contínuo a todos os resultados de avaliação que receberam. Caso contrário, precisariam gerenciar e arquivar os resultados da avaliação por conta própria.
>
> A permissão continua válida durante todo o período de validade da sua avaliação TISAX.
>
> Se você criou uma publicação ou permissão de compartilhamento por engano, entre em contato conosco imediatamente.

6.5. Níveis de compartilhamento

Os níveis de compartilhamento são mapeados individualmente nas seções principais A-E do relatório de avaliação TISAX.

	Seções principais do relatório de avaliação TISAX	Níveis de compartilhamento na plataforma
1	A. Informações relacionadas à avaliação (Assessment Related Information)	
2	B. Resultados resumidos (Summarized Results)	
3	C. Resumo do resultado da avaliação (Assessment result summary)	
4	D. D. Níveis de maturidade da VDA ISA (aba de resultados) (Maturity Levels of VDA ISA (Result Tab))	
5	E. Resultados detalhados da avaliação (Detailed Assessment Results)	

Tabela 12. Seções principais do relatório de avaliação TISAX e os níveis de compartilhamento na plataforma de compartilhamento

Quanto maior o nível de compartilhamento, mais detalhes sobre sua avaliação TISAX estarão acessíveis para o(s) respectivo(s) participante(s).

Para obter mais detalhes sobre o conteúdo de cada seção do relatório de avaliação TISAX, consulte a Seção 5.4.7.4, “Relatório de avaliação TISAX”.

6.6. Publique o resultado da sua avaliação na plataforma de compartilhamento

Você pode compartilhar o resultado da sua avaliação com todos os outros participantes TISAX, publicando-o na plataforma de compartilhamento. Isso permite que todos os outros participantes TISAX acessem o resultado da sua avaliação até o nível compartilhado concedido.

Você só poderá publicar o resultado da sua avaliação se o resultado geral da avaliação for “conforme”.

Os níveis de compartilhamento para publicação do resultado da sua avaliação na plataforma de compartilhamento estão limitados a essas opções:

- Do not publish (Default) (Não publicar (padrão))
- A. Assessment Related Information (A. Informações relacionadas à avaliação)
- A + Labels (Selos A +)
- A + Labels + B. Summarized Results (Selos A + + B. Resultados resumidos)

Recomendamos o nível de compartilhamento “A + Labels” (“Selos A +”) para esse tipo geral de publicação.

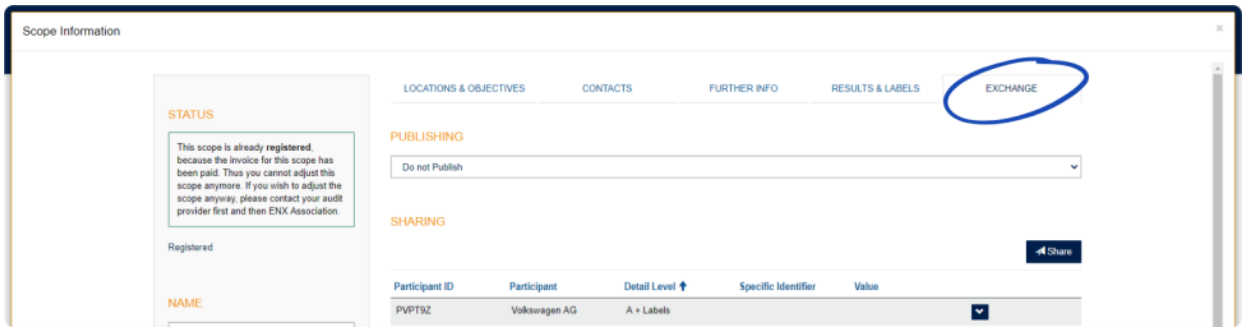
Observação importante:

Você poderá publicar o resultado da sua avaliação somente se os pré-requisitos

descritos em Seção 6.3, “Pré-requisitos gerais” forem atendidos.

Para publicar o resultado da sua avaliação na plataforma de compartilhamento, siga estas etapas:

1. Faça login no portal ENX.
2. Acesse a barra de navegação principal e selecione “MY TISAX” (“MY TISAX” (MEU TISAX)).
3. No menu suspenso, selecione “SCOPES AND ASSESSMENTS” (“SCOPES AND ASSESSMENTS” (ESCOPOS E AVALIAÇÕES)).
4. Vá até a tabela e encontre a linha da tabela com o escopo da sua avaliação.
5. Verifique se o seu escopo da avaliação tem o status do escopo da avaliação “Active” (“Active” (Ativo)) (coluna “Scope Status” (“Scope Status” (Status do Escopo))).
6. Vá até o final da linha da tabela do seu escopo da avaliação e clique no botão com a seta para baixo .
7. Selecione “Scope Information” (“Informações do escopo”).
8. Na nova janela (“Scope Information” (“Scope Information” (Informações do escopo))), selecione a aba “EXCHANGE” (“EXCHANGE” (COMPARTILHAMENTO)).



9. Vá para a seção “PUBLISHING” (“PUBLISHING” (PUBLICAÇÃO)), abra o menu suspenso e selecione o nível de compartilhamento desejado (veja recomendação acima).

Observe:

Os resultados da avaliação são publicados apenas na plataforma de compartilhamento. Eles podem ser acessados apenas por outros participantes TISAX. Não existe uma listagem pública de todos os participantes TISAX. Apenas o número bruto de participantes TISAX pode ser mencionado no site público do TISAX.

6.7. Compartilhar o resultado da sua avaliação com um participante específico

Além da opção mencionada acima de publicar o resultado da sua avaliação TISAX na

plataforma de compartilhamento, você pode compartilhá-lo seletivamente com determinados participantes TISAX com um nível de compartilhamento mais alto.

Em contraste com a publicação mencionada acima, você pode compartilhar o resultado da sua avaliação mesmo que o resultado geral da avaliação seja não conformidade (importante/menor).

O compartilhamento dos resultados da avaliação é parte integrante do TISAX. Seu sistema de gerenciamento de segurança da informação foi avaliado apenas uma vez, mas agora você pode compartilhar o resultado da avaliação com quantos parceiros desejar.

As opções para compartilhar o resultado da sua avaliação na plataforma de compartilhamento são:

1. A: Assessment Related Information (A: Informações relacionadas à avaliação)
2. A + Labels (Selos A +)
3. A + Labels + B: Assessment Summary (Selos A + + B: resumo da avaliação)
4. A + Labels + B + C: Summarized Results (Selos A + + B + C: resultados resumidos)
5. A + Labels + B + C + D: Detailed Assessment Results (Selos A + + B + C + D: resultados detalhados da avaliação)
6. A + Labels + B + C + D + E: Maturity Levels according to ISA (Selos A + + B + C + D + E: níveis de maturidade de acordo com a ISA)

Recomendamos o nível de compartilhamento “A + Labels” (“Selos A +”) para o compartilhamento. Isso é suficiente para a maioria dos parceiros. Você sempre pode selecionar um nível de compartilhamento mais elevado posteriormente.

Observe:

Alguns participantes do TISAX processam automaticamente os resultados da avaliação dos seus parceiros. Eles sincronizam seu próprio sistema com o portal ENX. Apenas os resultados da avaliação compartilhados especificamente com esse participante são sincronizados. Uma publicação sozinha, conforme descrito em Seção 6.6, “Publique o resultado da sua avaliação na plataforma de compartilhamento”, não é reconhecida.

Entre os OEMs que utilizam o TISAX, a BMW é um exemplo disso. Se você for um parceiro da BMW, compartilhe (e não apenas publique) o resultado da sua avaliação com a BMW.

6.7.1. Pré-requisitos

Estes são os pré-requisitos para compartilhar o resultado da sua avaliação com o seu parceiro

(ou qualquer outro participante TISAX):

- Você pode compartilhar o resultado da sua avaliação TISAX apenas com outros participantes TISAX.
- Seu parceiro precisa ser participante TISAX.
- Você precisa do ID de participante do seu parceiro.[31]
- Você precisa pagar a taxa (se aplicável).

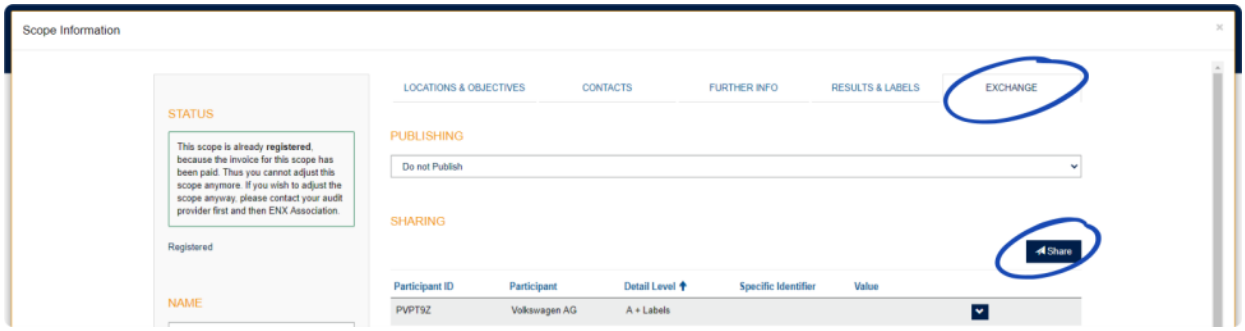
Observação importante:

Você poderá compartilhar o resultado da sua avaliação somente se os pré-requisitos gerais descritos em Seção 6.3, “Pré-requisitos gerais” forem atendidos.

6.7.2. Como criar uma permissão de compartilhamento

Para compartilhar o resultado da sua avaliação com outro participante TISAX, siga estas etapas:

1. Faça login no portal ENX.
2. Acesse a barra de navegação principal e selecione “MY TISAX” (“MY TISAX” (MEU TISAX)).
3. No menu suspenso, selecione “SCOPES AND ASSESSMENTS” (“SCOPES AND ASSESSMENTS” (ESCOPOS E AVALIAÇÕES)).
4. Vá até a tabela, encontre a linha da tabela com o escopo da sua avaliação.
5. Verifique se o seu escopo da avaliação tem o status do escopo da avaliação “Active” (“Active” (Ativo)) (coluna “Scope Status” (“Scope Status” (Status do Escopo))).
6. Vá até o final da linha da tabela do seu escopo da avaliação e clique no botão com a seta para baixo .
7. Selecione “Scope Information” (“Informações do escopo”).
8. Na nova janela (“Scope Information” (“Scope Information” (Informações do escopo))), selecione a aba “EXCHANGE” (“EXCHANGE” (COMPARTILHAMENTO)).



9. Vá para a seção “SHARING” (“SHARING” (COMPARTILHAMENTO) e clique no botão “Share” (“Share” (Compartilhar).

10. Na nova janela (“SHARE THIS SCOPE” (🇵🇹 “SHARE THIS SCOPE” (COMPARTILHAR ESSE ESCOPO))), insira o ID de participante do seu parceiro (ou selecione-o na lista de participantes na caixa de pesquisa vizinha).
11. Selecione o nível de compartilhamento desejado.
12. Clique no botão “Next” (🇵🇹 “Next” (Avançar).
13. Leia e entenda as instruções em relação à permanência da permissão de compartilhamento.
14. Marque as duas caixas de seleção “confirm” (🇵🇹 “confirmar”).
15. Clique no botão “Submit” (🇵🇹 “Submit” (Enviar).

Todo o resto é feito pela plataforma de compartilhamento. Para o compartilhamento dos níveis A e B, as informações estão disponíveis na plataforma de compartilhamento. Agora seu parceiro pode fazer login no portal ENX e ver o resultado da avaliação compartilhada[32].

Para os níveis de compartilhamento mais elevados (C-E), a plataforma de compartilhamento notifica seu provedor de auditoria. Em seguida, seu provedor de auditoria envia as informações (correspondentes ao nível de compartilhamento selecionado) para o contato participante principal do seu parceiro.

6.8. Compartilhamento do resultado da sua avaliação fora do TISAX

A regra[33] é que você pode usar a plataforma de compartilhamento TISAX apenas para informar outros participantes TISAX sobre o resultado da sua avaliação.

6.8.1. Os motivos para a regulamentação estrita do mecanismo de compartilhamento

O TISAX fornece um mecanismo padronizado de compartilhamento dos resultados da avaliação. Isso proporciona um valor agregado em comparação com o compartilhamento dos resultados de outras certificações (por exemplo, ISO), onde isso acontece de várias formas e nem sempre contém todas as informações necessárias do cenário completo.

Os OEMs, em particular, apreciam essa padronização. Mas outras empresas também se beneficiam de procedimentos claramente definidos.

6.8.2. Um guia para escrever sobre o TISAX em público

Embora não seja possível escrever publicamente sobre o resultado da avaliação, você pode mencionar seus esforços no TISAX. No portal ENX, oferecemos conselhos sobre como abordar as declarações públicas. Também fornecemos logotipos TISAX que você pode usar.

Após fazer login no portal ENX, você poderá acessar as informações aqui:
🇬🇧 enx.com/en-US/myenxportal/marketing/

Download direto de arquivo ZIP (documentos e logotipos):
enx.com/en-US/myenxportal/marketing/TISAX-Trademark-and-Logos-Terms-and-Conditions.zip

Se você estiver se perguntando se existe um certificado que você possa pendurar na parede: Devido ao processo de compartilhamento padronizado mencionado acima, não fornecemos esse certificado.

6.8.3. Compartilhamento com um parceiro que ainda não é participante TISAX

Se você desejar compartilhar o resultado da sua avaliação TISAX com um parceiro específico que a) ainda não seja participante TISAX e b) ainda não recebeu os selos TISAX (passando pelo processo de avaliação), você pode seguir estas etapas:

1. Oriente seu parceiro a realizar o cadastro como um participante TISAX.
   Ele só precisa se cadastrar como um participante TISAX. Ele não precisa continuar cadastrando um escopo da avaliação.
2. Oriente seu parceiro a entrar em contato conosco.
   Normalmente, iniciamos o processo de cadastro apenas se a empresa também estiver cadastrando um escopo da avaliação. A pedido do seu parceiro, processamos o seu cadastro. Assim, ele se tornará participante TISAX. Agora ele pode receber o resultado da sua avaliação TISAX através do processo regular de compartilhamento.

A finalidade dessa abordagem é garantir que seu parceiro concorde em aderir aos “Termos e Condições Gerais de Participação TISAX” que regulamentam o compartilhamento dos resultados da avaliação TISAX.

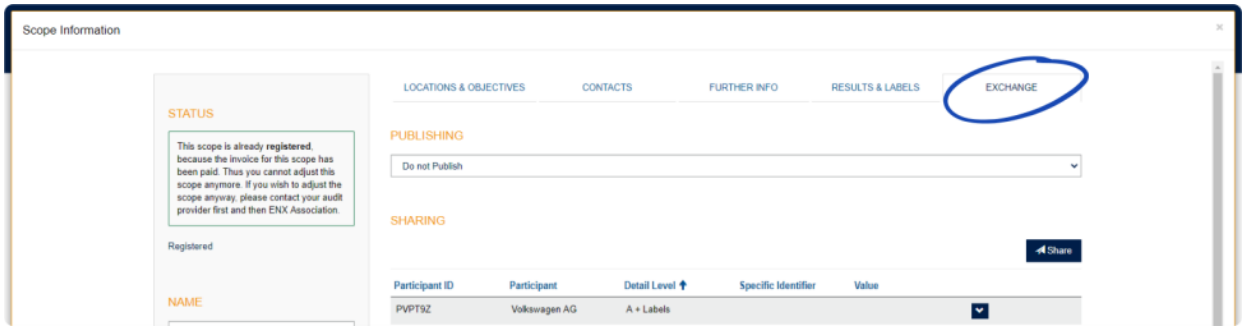
Apenas o cadastro de um escopo da avaliação acarreta custos. Como o cadastro como participante TISAX é gratuito, seu parceiro pode receber o resultado da avaliação sem nenhum custo. No entanto, sem um resultado de avaliação próprio, seu parceiro poderá receber apenas até cinco resultados de avaliação e não poderá ver nenhuma das publicações.

6.8.4. Compartilhamento com funcionários do seu parceiro que não têm acesso direto ao portal ENX

Apenas os funcionários do seu parceiro que tenham conta em nosso portal ENX poderão ver diretamente o seu resultado. Caso você precise comprovar seus selos TISAX para um funcionário do seu parceiro sem acesso ao portal, você pode utilizar um documento PDF especial para isso. Para obter o documento, siga estas etapas:

1. Compartilhe o resultado da sua avaliação com seu parceiro conforme descrito em Seção 6.7, “Compartilhar o resultado da sua avaliação com um participante específico”.
2. Faça login no portal ENX.

3. Acesse a barra de navegação principal e selecione “MY TISAX” (“MY TISAX” (MEU TISAX)).
4. No menu suspenso, selecione “SCOPES AND ASSESSMENTS” (“SCOPES AND ASSESSMENTS” (ESCOPOS E AVALIAÇÕES)).
5. Vá até a tabela e encontre a linha da tabela com o escopo da sua avaliação.
6. Verifique se o seu escopo da avaliação tem o status do escopo da avaliação “Active” (“Active” (Ativo)) (coluna “Scope Status” (“Scope Status” (Status do Escopo))).
7. Vá até o final da linha da tabela do seu escopo da avaliação e clique no botão com a seta para baixo .
8. Selecione “Scope Information” (“Informações do escopo”).
9. Na nova janela (“Scope Information” (“Scope Information” (Informações do escopo))), selecione a aba “EXCHANGE” (“EXCHANGE” (COMPARTILHAMENTO)).



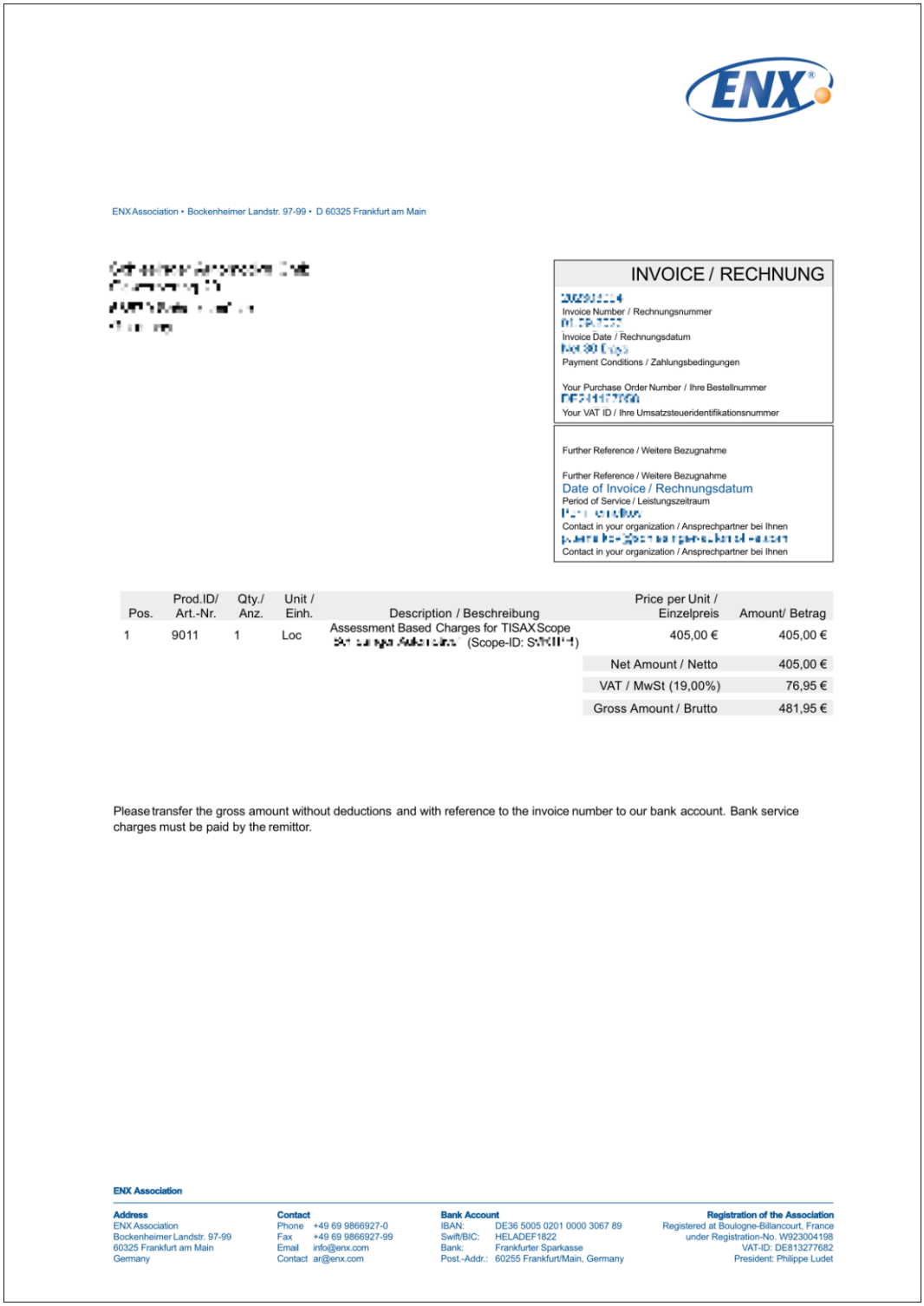
10. Vá para a seção “SHARING” (“SHARING” (COMPARTILHAMENTO)) e encontre a linha da tabela com a permissão de compartilhamento (conforme criado na etapa 1).
11. Vá até o final da linha da tabela da permissão de compartilhamento e clique no botão com a seta para baixo .
12. Selecione “Edit” (“Editar”)
13. Na nova janela (“SHARE THIS SCOPE” (“SHARE THIS SCOPE” (COMPARTILHAR ESSE ESCOPO))), role até o final e selecione “Request Shared Information as PDF” (“Request Shared Information as PDF” (Solicitar informações compartilhadas em PDF)).
14. Aguarde um momento até que o documento seja gerado.
15. Baixe o documento (“Copy of information shared with ACME.pdf (66.84 KB)” (“Cópia das informações compartilhadas com ACME.pdf (66,84 KB)”))

7. Anexos

7.1. Anexo: Exemplo de nota fiscal

Esse é um exemplo da fatura que enviamos.

Para obter mais informações, consulte a Seção 4.3.4, “Taxa”.



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. Anexo: Exemplo de e-mail de confirmação

Enviamos o e-mail de confirmação assim que você concluir todas as etapas obrigatórias durante o processo de cadastro on-line.

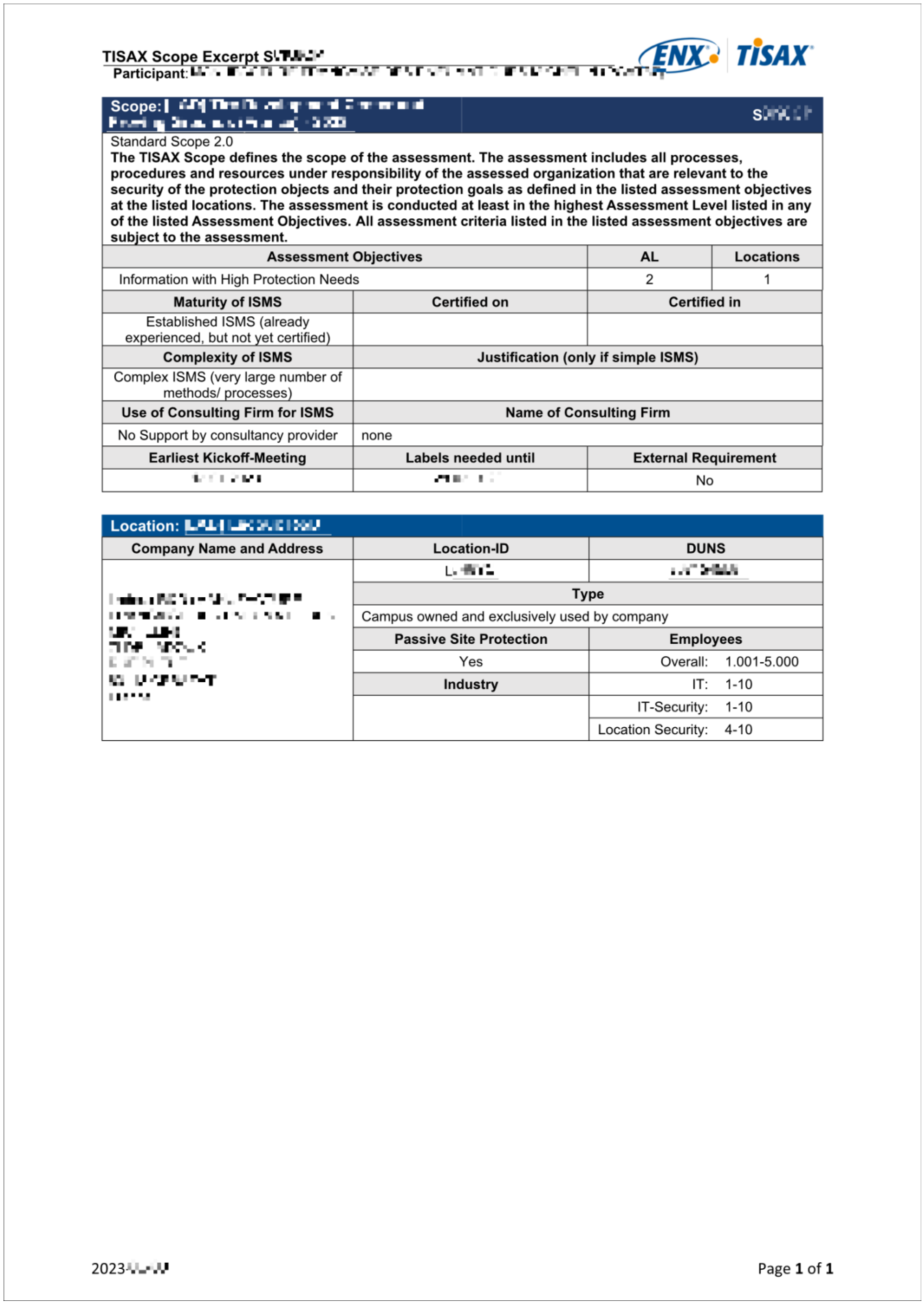
Para obter mais informações quando enviarmos esse e-mail de confirmação, consulte Seção 4.5.8, “E-mail de confirmação”.

```
f

Caro John Doe

Agradecemos pelo cadastro do escopo da avaliação TISAX. Realizei o cadastro do seu
escopo e aprovei o seu escopo. Em anexo você pode encontrar o extrato do escopo
TISAX incluindo todas as informações do escopo e a lista atual de provedores de
auditoria TISAX.

E agora?

Com o extrato do escopo TISAX anexado, agora você pode solicitar cotações de todos
os provedores de auditoria TISAX para o seu escopo.

Precisa de ajuda?

Para mais perguntas sobre o TISAX, leia as Perguntas frequentes do TISAX ou o
Manual do participante TISAX. Se precisar de mais assistência em relação ao TISAX,
não hesite em entrar em contato com a linha direta TISAX por e-mail (tisax@enx.com)
ou por telefone (+49 69 986692-777).

Atenciosamente,

Equipe TISAX
```

7.3. Anexo: Exemplo do extrato do escopo TISAX

Você receberá o “TISAX scope excerpt” (extrato do escopo TISAX) anexado ao e-mail de confirmação.

Para obter mais informações, consulte a Seção 4.5.8, “E-mail de confirmação”.



TISAX Scope Excerpt S[illegible]

Participant: [illegible]

Scope: [illegible] S[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]	L[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. Anexo: Participant status (Status do participante)

7.4.1. Visão geral: Participant status (Status do participante)

O “status do participante” define onde você (como empresa) está no processo TISAX.

Seu “status do participante” pode ser:

1. Incomplete (Incompleto)
2. Awaiting approval (Aguardando aprovação)
3. Preliminary (Provisório)
4. Registered (Cadastrado)
5. Expired (Vencido)

As tabelas na seção de cada status abaixo descrevem:

- sua situação
  (o que é verdade agora quando você está nesse status)
- sua próxima ação
  (o que você precisa fazer para avançar para o próximo status; se aplicável)
- nossa próxima ação
  (o que precisamos fazer para elevar seu status; se aplicável)
- o próximo status
  (se aplicável)

A ilustração a seguir mostra as ações que levam ao avanço de um status para o próximo:

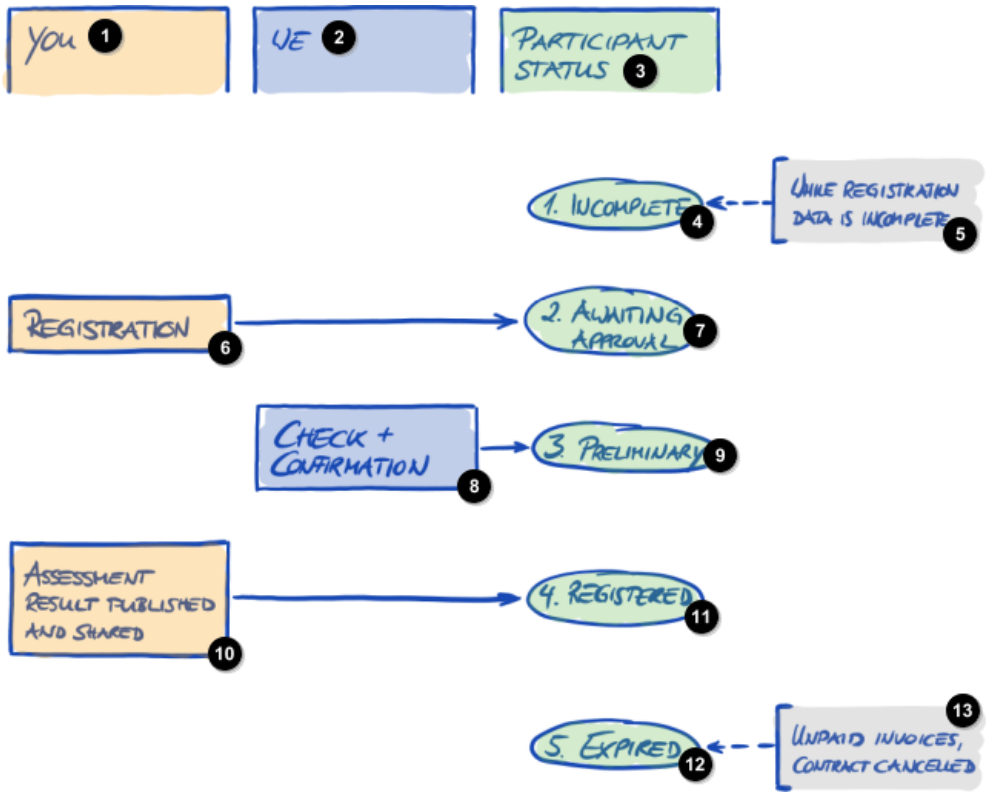


Figura 34. Visão geral do status do participante

1. Você
2. Nós
3. Status do participante
4. 1. Incompleto
5. Enquanto os dados do cadastro estejam incompletos
6. Cadastro
7. 2. Aguardando aprovação
8. Verificação + confirmação
9. 3. Provisório
10. Resultado da avaliação publicado e compartilhado
11. 4. Cadastrado
12. 5. Vencido
13. Faturas não pagas, contrato cancelado

7.4.2. Participant status “Incomplete” (Status do participante “Incomplete” (Incompleto))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Incompleto	Você não concluiu o cadastro TISAX. Ou você não aceitou os termos e condições gerais. Ou você não especificou a localização do participante principal. Ou você não atribuiu um contato de participante principal. Ou outras informações que necessitamos estão ausentes.	Continuar em enx.com/en-US/SignIn	Vamos enviar um lembrete por e-mail (normalmente dentro de alguns dias).	Aguardando aprovação

7.4.3. Participant status “Awaiting approval” (Status do participante “Awaiting approval” (Aguardando aprovação))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Aguardando aprovação	Seu cadastro TISAX está completo. Você pode ou não ter cadastrado um escopo de avaliação até o momento.	Aguarde nossa próxima ação.	Vamos verificar e normalmente aprovar sua inscrição. No entanto, normalmente você aciona nossa verificação ao cadastrar também um escopo de avaliação. Vamos atribuir um ID de participante e o(s) ID(s) do escopo. Enviaremos a você um e-mail de confirmação. O “TISAX scope excerpt” (extrato do escopo TISAX) (PDF) em anexo resume as informações que temos em nosso banco de dados.	Provisório

7.4.4. Participant status “Preliminary” (Status do participante “Preliminary” (Preliminar)

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Provisório	Você concluiu com sucesso o processo de cadastro TISAX.	Pagar a taxa (se aplicável). Passar pelo processo de avaliação TISAX. Publicar e compartilhar o resultado da sua avaliação.	Nenhuma	Cadastrado

7.4.5. Participant status “Registered” (Status do participante: “Cadastrado”)

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Cadastrado	Você concluiu com sucesso o processo de avaliação TISAX e recebeu os selos TISAX. Você publicou e compartilhou o resultado da sua avaliação. Você vai receber os selos TISAX apenas quando for aprovado no processo de avaliação TISAX. No portal ENX, isso se reflete em ter um escopo da avaliação com status do escopo da avaliação “Active” (Ativo).	Nenhuma	Nenhuma	(Vencido)

Observe:

Se desejar acessar os resultados da avaliação do(s) seu(s) parceiro(s):

O pré-requisito conceitual para poder receber os resultados da avaliação de outros participantes é:

- Você compartilhar o resultado da sua própria avaliação (isso “prova” que você é um participante TISAX sério e um membro da comunidade automotiva).
- Reconhecemos você com base em sua reputação no setor automotivo (como OEMs, fornecedores de primeiro nível).
- Você prova que tem um interesse legítimo em receber os resultados da avaliação de outros participantes. Precisamos verificar isso em um processo

> elaborado que pode incorrer em uma taxa substancial. Para obter mais informações, entre em contato conosco.

7.4.6. Participant status “Expired” (Status do participante “Expired” (Vencido))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Vencido	Você não pagou a taxa. Ou você ou nós cancelamos nosso contrato mútuo (os TCGs).	Nenhuma	Nenhuma	N/A

7.5. Anexo: Assessment scope status (Status do escopo da avaliação)

7.5.1. Visão geral: Assessment scope status (Status do escopo da avaliação)

O “status do escopo da avaliação” define onde está o escopo da sua avaliação em relação ao seu ciclo de vida.

Esteja ciente de que o “status do escopo da avaliação” é diferente do “status da avaliação”. Para obter mais informações sobre o “status da avaliação”, consulte Seção 7.6, “Anexo: Assessment status (Status da avaliação)”.

Seu “status do escopo da avaliação” pode ser:

1. Incomplete (Incompleto)
2. Awaiting your order (Aguardando seu pedido)
3. Awaiting ENX approval (Aguardando aprovação da ENX)
4. Awaiting your payment (Aguardando seu pagamento)
5. Registered (Cadastrado)
6. Active (Ativo)
7. Expired (Vencido)

As tabelas na seção de cada status abaixo descrevem:

- sua situação
  (o que é verdade agora quando você está nesse status)

- sua próxima ação
  (o que você precisa fazer para avançar para o próximo status; se aplicável)
- nossa próxima ação
  (o que precisamos fazer para elevar seu status; se aplicável)
- o próximo status
  (se aplicável)

A ilustração a seguir mostra as ações que levam ao avanço de um status para o próximo:

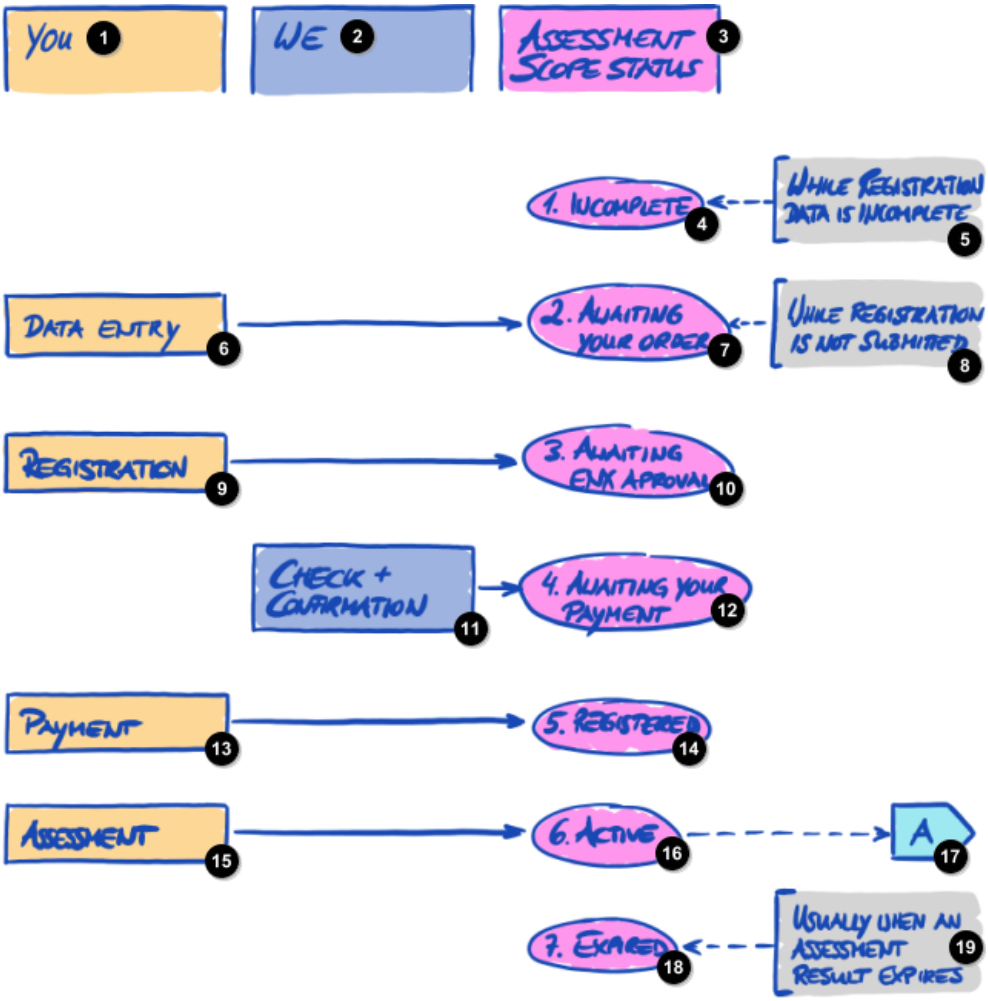


Figura 35. Visão geral do status do escopo da avaliação

1. Você
2. Nós
3. Status do escopo da avaliação
4. 1. Incompleto
5. Enquanto os dados do cadastro estejam incompletos

6. Entrada de dados
7. 2. Aguardando seu pedido
8. Enquanto o cadastro não for enviado
9. Cadastro
10. 3. Aguardando aprovação da ENX
11. Verificação + confirmação
12. 4. Aguardando seu pagamento
13. Pagamento
14. 5. Cadastrado
15. Avaliação
16. 6. Ativo
17. A
18. 7. Vencido
19. Normalmente, quando o resultado de uma avaliação vence

A referência fora da página “A” na figura acima vincula o status do escopo da avaliação “Active” (Ativo) com o “status da avaliação”. Para obter mais informações sobre o “status da avaliação”, consulte Seção 7.6, “Anexo: Assessment status (🇵🇹 Status da avaliação)”.

7.5.2. Assessment scope status “Incomplete” (🇵🇹 Status do escopo da avaliação “Incomplete” (Incompleto)

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Incompleto	Ou você não concluiu o cadastro do escopo da avaliação. Ou você não forneceu todas as informações necessárias.	Continuar em 🇬🇧 enx.com/en-US/SignIn	Vamos enviar um lembrete por e-mail (normalmente dentro de alguns dias).	Aguardando seu pedido

Para obter mais informações sobre onde esse status está desempenhando um papel, consulte Seção 4.5.7, “Cadastro do escopo da avaliação”.

7.5.3. Assessment scope status “Awaiting your order” (Status do escopo da avaliação “Awaiting your order” (Aguardando seu pedido))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Aguardando seu pedido	Você não concluiu o cadastro do seu escopo.	Continuar em enx.com/en-US/SignIn	Vamos enviar um lembrete por e-mail (normalmente dentro de alguns dias).	Aguardando aprovação da ENX

Para obter mais informações sobre onde esse status está desempenhando um papel, consulte Seção 4.5.7, “Cadastro do escopo da avaliação”.

7.5.4. Assessment scope status “Awaiting ENX approval” (Status do escopo da avaliação “Awaiting ENX approval” (Aguardando aprovação da ENX))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Aguardando aprovação da ENX	O cadastro do escopo da sua avaliação está completo.	Aguarde nossa próxima ação.	Vamos verificar e normalmente aprovar sua inscrição. Vamos atribuir o(s) ID(s) do escopo. Enviaremos a você um e-mail de confirmação. O “TISAX scope excerpt” (extrato do escopo TISAX) (PDF) em anexo resume as informações que temos em nosso banco de dados.	Aguardando seu pagamento

Para obter mais informações sobre onde esse status está desempenhando um papel, consulte Seção 4.5.7, “Cadastro do escopo da avaliação”.

7.5.5. Assessment scope status “Awaiting your payment” (Status do escopo da avaliação “Awaiting your payment” (Aguardando seu pagamento))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Aguardando seu pagamento	O cadastro do escopo da sua avaliação está completo e aprovado. Você recebeu nosso e-mail de confirmação e o “TISAX scope excerpt” (extrato do escopo TISAX).	Pagar a taxa (se aplicável). Solicite propostas dos nossos provedores de auditoria TISAX. A partir do status “Awaiting your payment” (Aguardando seu pagamento), você: ▪ pode começar compartilhando algumas informações relacionadas à avaliação com o seu parceiro.[34] ▪ pode configurar previamente a publicação do resultado da sua avaliação (isso só entrará em vigor quando o status do escopo da sua avaliação mudar para “Active” (Ativo).	Aguardando seu pagamento.	Cadastrado

Para obter mais informações sobre onde esse status está desempenhando um papel, consulte Seção 4.5.8, “E-mail de confirmação”.

7.5.6. Assessment scope status “Registered” (Status do escopo de avaliação “Registered” (Cadastrado)

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Cadastrado	Seu escopo de avaliação está cadastrado. Recebemos seu pagamento completo ou seu status comercial é “verde” devido a outras circunstâncias.	Passar pelo processo de avaliação TISAX.	Nenhuma	Ativo

7.5.7. Assessment scope status “Active” (Status do escopo da avaliação “Active” (Ativo))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Ativo	Você concluiu com sucesso o processo de avaliação TISAX e recebeu os selos TISAX.	Publicar e compartilhar o resultado da sua avaliação. Quaisquer publicações e permissões de compartilhamento configuradas previamente com um status inferior agora entrarão em vigor.	Nenhuma	Vencido

Para obter mais informações sobre como publicar e compartilhar, consulte Seção 6, “Compartilhamento (Etapa 3)”.

7.5.8. Assessment scope status “Expired” (Status do escopo da avaliação “Expired” (Vencido))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Vencido	Há as opções a seguir: ▪ você não concluiu o cadastro do escopo da avaliação em 90 dias,	Inicie um novo cadastro do escopo da avaliação.	Nenhuma	Incompleto ou Aguardando seu pedido ou Aguardando aprovação da ENX
	• ou houve um atraso indevido no pagamento da taxa,			
	• ou você saiu do processo TISAX,			
	• ou a validade do resultado da sua avaliação venceu (três anos),			
	• ou você teve grandes alterações no escopo da avaliação (exemplo: nenhuma das localizações no escopo da avaliação pertence mais à sua empresa).			

7.6. Anexo: Assessment status (🇵🇹 Status da avaliação)

7.6.1. Visão geral: Assessment status (🇵🇹 Status da avaliação)

O “status da avaliação” define onde você está no processo de avaliação. O status muda com a sua progressão de um tipo de avaliação para outro (como “avaliação inicial” para “avaliação do plano de ação corretiva”).

Esteja ciente de que o “status da avaliação” é diferente do “status do escopo da avaliação”. Para obter mais informações sobre o “status do escopo da avaliação”, consulte a Seção 7.5, “Anexo: Assessment scope status (🇵🇹 Status do escopo da avaliação)”.

Seu “status da avaliação” pode ser:

1. Initial assessment ordered (🇵🇹 Avaliação inicial solicitada)
2. Initial assessment ongoing (🇵🇹 Avaliação inicial em andamento)
3. Waiting for corrective action plan assessment (🇵🇹 Aguardando avaliação do plano de ação corretiva)
4. Waiting for follow-up (🇵🇹 Aguardando acompanhamento)
5. Finished (🇵🇹 Concluído)

As tabelas na seção de cada status abaixo descrevem:

- sua situação
  (o que é verdade agora quando você está nesse status)
- sua próxima ação
  (o que você precisa fazer para avançar para o próximo status; se aplicável)
- nossa próxima ação
  (o que precisamos fazer para elevar seu status; se aplicável)
- o próximo status
  (se aplicável)

A ilustração a seguir mostra as ações que levam ao avanço de um status para o próximo:

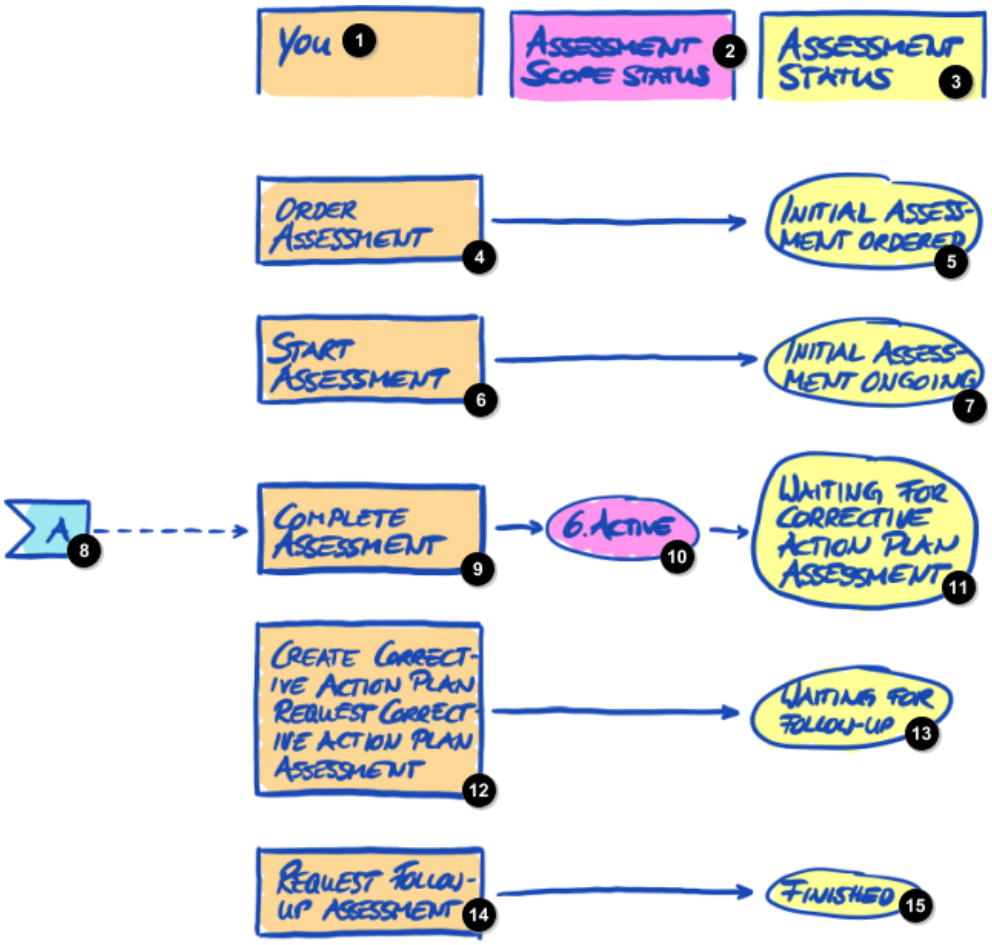


Figura 36. Visão geral do status da avaliação

1. Você
2. Status do escopo da avaliação
3. Status da avaliação
4. Avaliação do pedido
5. Avaliação inicial solicitada
6. Avaliação do pedido
7. Avaliação inicial em andamento
8. A
9. Avaliação incompleta
10. 6. Ativo
11. Aguardando avaliação do plano de ação corretiva
12. Criar um plano de ação corretiva
    Solicitar avaliação do plano de ação corretiva

13. Aguardando acompanhamento
14. Solicitar avaliação de acompanhamento
15. Finalizado

A referência fora da página “A” na figura acima vincula o status do escopo da avaliação “Active” (Ativo) com o status da avaliação “Waiting for corrective action plan assessment” (Aguardando avaliação do plano de ação corretiva). Para obter mais informações sobre o “status do escopo da avaliação”, consulte a Seção 7.5, “Anexo: Assessment scope status (Status do escopo da avaliação)”.

7.6.2. Assessment status “Initial assessment ordered” (Status da avaliação “Initial assessment ordered” (Avaliação inicial solicitada))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Avaliação inicial solicitada	Você selecionou um dos nossos provedores de auditoria TISAX e solicitou uma avaliação inicial.	Continue o processo de avaliação TISAX.	Nenhuma	Avaliação inicial em andamento

7.6.3. Assessment status “Initial assessment ongoing” (Status da avaliação “Initial assessment ongoing” (Avaliação inicial em andamento))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Avaliação inicial em andamento	Sua avaliação inicial: ▪ começou ▪ ou foi concluída, mas o seu provedor de auditoria ainda não enviou o relatório de avaliação TISAX	Nenhuma	Nenhuma	Aguardando avaliação do plano de ação corretiva (se aplicável)

7.6.4. Assessment status “Waiting for corrective action plan assessment” (Status da avaliação “Waiting for corrective action plan assessment” (Aguardando avaliação do plano de ação corretiva))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Aguardando avaliação do plano de ação corretiva	Seu provedor de auditoria realizou uma avaliação inicial. Seu provedor de auditoria nos enviou o relatório de avaliação TISAX. O resultado da avaliação é uma não conformidade (importante/menor).	Crie um plano de ação corretiva. Inicie as ações corretivas. Solicite uma avaliação do plano de ação corretiva.	Nenhuma	Aguardando acompanhamento (se aplicável)

O status da avaliação “Waiting for corrective action plan assessment” (Aguardando avaliação do plano de ação corretiva) é limitado a nove meses. Para obter mais informações, consulte a Seção 5.4.9.3, “Requisitos do plano de ação corretiva”.

7.6.5. Assessment status “Waiting for follow-up” (Status da avaliação “Waiting for follow-up” (Aguardando acompanhamento))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Aguardando acompanhamento	Seu provedor de auditoria aprovou seu plano de ação corretiva. Você implementou as ações corretivas.	Solicite uma avaliação de acompanhamento.	Nenhuma	Finalizado

O status da avaliação “Waiting for follow-up” (Aguardando acompanhamento) é limitado a nove meses. Para obter mais informações, consulte a Seção 5.4.9.3, “Requisitos do plano de ação corretiva”.

7.6.6. Assessment status “Finished” (Status da avaliação “Finished” (Concluído))

Status	Situação	Sua próxima ação	Nossa próxima ação	Próximo status
Finalizado	Seu provedor de auditoria realizou uma avaliação de acompanhamento. O resultado da avaliação não apresenta não conformidades. Seu provedor de auditoria nos enviou o relatório de avaliação TISAX.	Publicar e compartilhar o resultado da sua avaliação.	Nenhuma	N/A

7.7. Anexo: A lógica contra “avaliações prévias” e “análises de lacunas”

Geralmente desaconselhamos solicitar a um provedor de auditoria que realize uma “avaliação prévia” ou uma “análise de lacunas”. Em quase todos os casos, faz mais sentido iniciar imediatamente o processo de avaliação TISAX.

Nessa seção abordamos as preocupações mais comuns.

Você considera uma avaliação prévia porque:

1. Você está preocupado com a possibilidade do seu cliente ver um resultado de avaliação potencialmente desfavorável?

   Você tem controle total sobre quem vê os resultados da sua avaliação. É sua a decisão de autorizar o provedor de auditoria a carregar algo no portal ENX. Se ninguém deveria ver, ninguém vê (exceto o auditor, é claro).

   Além disso, o provedor de auditoria sempre carrega apenas as primeiras duas seções do relatório de avaliação TISAX e *nunca* carrega os resultados detalhados da avaliação de qualquer maneira.

2. Você acha que uma avaliação prévia pode ser econômica?
   - Com uma avaliação prévia, você:

- paga pela avaliação prévia
- pode ter os custos internos para corrigir quaisquer não conformidades
- paga pela avaliação TISAX completa (“avaliação inicial”)

Mesmo que *não* haja achados, você sempre paga por *duas* avaliações completas.

- Começando com uma avaliação TISAX, você:
  - pagar pela “avaliação inicial”
  - pode ter os custos internos de corrigir quaisquer achados
  - pode pagar muito menos (em comparação com a avaliação inicial) pela chamada “avaliação de acompanhamento”, onde o auditor se concentra apenas em saber se você corrigiu as não conformidades da avaliação inicial

  Mesmo *com* os achados, você paga apenas por uma avaliação completa mais a avaliação de acompanhamento concisa.

3. Você acha que pode ser reprovado na avaliação com consequências permanentes?

   Você não pode reprovado permanentemente, porque pode fazer quantas avaliações quiser. Se o resultado da avaliação não atender às suas expectativas ou se você não conseguir corrigir as não conformidades com ações corretivas dentro do período de nove meses exigido, basta considerar a tentativa com reprovação como a sua avaliação prévia e iniciar uma nova. E ninguém precisa ver os resultados da sua primeira tentativa. Você apenas compartilha o resultado da avaliação bem-sucedida.

Considerações adicionais:

- Se o resultado da avaliação for melhor que o esperado, você poderá receber os selos TISAX temporários. Você pode compartilhá-los diretamente com o seu parceiro. Isso não é possível com uma avaliação prévia.
- Se o provedor de auditoria que faz a avaliação prévia também realizar a avaliação TISAX, ele não poderá consultar você. Caso contrário, você precisa escolher outro provedor de auditoria para a avaliação TISAX.

Embora a maioria dos auditados não se beneficie de uma avaliação prévia, queremos mencionar as seguintes vantagens.

O auditor:

- pode se concentrar nos aspectos críticos que você não tem confiança em seu SGSI
- pode gastar mais tempo do que o normal e aumentar as informações
- pode documentar achados de maneira diferente

Após a leitura das seções sobre o processo de avaliação TISAX, ficará ainda mais fácil entender a nossa lógica.

7.8. Anexo: Escopos personalizados

Quase todos os participantes TISAX escolhem o escopo padrão. No entanto, em algumas e *raras* circunstâncias, pode ser necessário escolher um escopo personalizado.

Existem dois tipos de escopos personalizados:

7.8.1. Escopo ampliado personalizado

Você pode ampliar o escopo. Um escopo ampliado personalizado contém MAIS do que o escopo padrão. O provedor de auditoria vai realizar mais verificações.

Finalidade: um escopo ampliado personalizado pode ser relevante se você desejar usar sua avaliação TISAX para fins internos ou fora do setor automotivo.

Selos TISAX e compartilhamento dos resultados: um escopo ampliado personalizado sempre inclui o escopo padrão. Portanto, um escopo ampliado personalizado receberá selos TISAX[35]. Outros participantes TISAX também vão aceitar o resultado da avaliação.

Descrição: embora o escopo padrão tenha uma descrição predefinida, você vai precisar escrever sua própria descrição do escopo se precisar de um escopo ampliado personalizado.

7.8.2. Escopo personalizado completo

Você pode definir totalmente seu próprio escopo.

Finalidade: se você tiver localizações que pertencem a escopos da avaliação diferentes e que usam serviços em um local específico (como um centro de dados), você poderá usar um escopo personalizado completo para esses serviços. Assim, um provedor de auditoria TISAX pode reutilizar facilmente o resultado da avaliação de todo o escopo personalizado do serviço.

Exemplo: você tem muitas localizações (possivelmente fazendo parte de escopos diferentes) e um departamento central de TI em uma dessas localizações. Definir um escopo personalizado completo apenas para o departamento de TI pode facilitar a reutilização do respectivo resultado da avaliação nos demais escopos.

Selos TISAX e compartilhamento dos resultados: os escopos totalmente personalizados não recebem os selos TISAX. O resultado da sua avaliação é registrado no portal ENX com a data, prazo de validade e se o resultado geral da avaliação está conforme ou não conforme. Você pode compartilhar o resultado dessa avaliação. Mas compartilhar um resultado de avaliação sem selos TISAX parecerá uma avaliação “reprovada” para a maioria dos destinatários. Outros participantes TISAX geralmente não aceitam resultados da avaliação de escopos personalizados completos.

Descrição: como para o escopo ampliado personalizado, você precisa escrever sua própria descrição do escopo se precisar de um escopo personalizado completo.

Observação importante:

Para enfatizar como é raro o uso de escopos totalmente personalizados: há uma chance de 98% de que o seu provedor de auditoria reverta seu escopo totalmente personalizado para um escopo padrão. Nenhum participante *nunca* escolheu com sucesso um escopo personalizado completo sem aconselhamento de seu provedor de auditoria.

Uma avaliação com escopo totalmente personalizado não receberá os selos TISAX. Portanto, normalmente desaconselhamos a escolha de um escopo totalmente personalizado — principalmente porque outros participantes geralmente não aceitam resultados de avaliação com escopos totalmente personalizados.
Não escolha um escopo personalizado completo se não tiver a confirmação explícita de que seu parceiro vai aceitar o resultado e concordar com a sua descrição específica do escopo.

7.9. Anexo: Gerenciamento do ciclo de vida dos dados do participante

As seções a seguir descrevem o que você precisa fazer se algo relacionado aos seus dados como participante mudar.

7.9.1. Perda de acesso aos dados dos participantes (portal ENX)

Se ninguém em sua empresa teve acesso ao portal ENX e, portanto, seus dados de participante forem perdidos, entre em contato conosco. Vamos tentar ajudar você a recuperar o acesso aos dados dos participantes da sua empresa.

7.9.2. Administração dos contatos

Os principais contatos participantes da sua empresa e todos os demais “contatos administrativos” com contas no portal podem sempre acessar o portal ENX e:

- adicionar novos contatos
- excluir contatos existentes
- alterar os dados de contato dos contatos existentes

7.9.2.1. Como adicionar um novo contato

Para adicionar um novo contato, siga estas etapas:

1. Faça login no portal ENX.
2. Acesse a barra de navegação principal e selecione “MY TISAX” (“MY TISAX” (MEU TISAX)).
3. No menu suspenso, selecione “ADMINISTRATORS” (“ADMINISTRATORS” (ADMINISTRADORES)).
4. Clique no botão “Create new TISAX Administrator” (“Create new TISAX Administrator” (Criar novo administrador TISAX)).
5. Insira os dados do contato.
6. Clique no botão “Save Contact” (“Save Contact” (Salvar contato)).
7. Vá até a tabela e encontre a linha da tabela com o contato.
8. Vá até o final da linha da tabela do contato e clique no botão com a seta para baixo .
9. Selecione “Edit TISAX Administrator” (“Edit TISAX Administrator” (Editar Administrador TISAX)).
10. Na nova janela (“Edit TISAX Contact” (“Edit TISAX Contact” (Editar contato TISAX))), role para baixo até a seção “ENX PORTAL ACCESS” (“ENX PORTAL ACCESS” (ACESSO DO PORTAL ENX)).
11. Selecione “Yes” (“Yes” (Sim)).
12. Na seção que é exibida “WEB ROLES” (“WEB ROLES” (FUNÇÕES DA WEB)), clique no botão “Add Role” (“Add Role” (Adicionar função)).
13. Selecione a função que deseja atribuir (por exemplo, “TISAX Administrator” (“TISAX Administrator” (Administrador TISAX))).
14. Clique no botão “Add Role” (Adicionar função).
15. Clique no botão “Save Contact” (Salvar contato).

7.9.2.2. Como excluir os dados de um contato existente

Para excluir os dados de um contato existente, siga estas etapas:

1. Faça login no portal ENX.
2. Acesse a barra de navegação principal e selecione “MY TISAX” (“MY TISAX” (MEU TISAX)).
3. No menu suspenso, selecione “ADMINISTRATORS” (“ADMINISTRATORS” (ADMINISTRADORES)).
4. Vá até a tabela e encontre a linha da tabela com o contato.
5. Vá até o final da linha da tabela do contato e clique no botão com a seta para baixo .
6. Selecione “Delete TISAX Administrator” (“Delete TISAX Administrator” (Excluir Administrador TISAX).
7. Na solicitação de confirmação que é exibida, clique no botão “Delete” (“Delete” (Excluir)).

7.9.2.3. Como atualizar os dados de um contato existente

Para atualizar os dados de um contato existente, siga estas etapas:

1. Faça login no portal ENX.
2. Acesse a barra de navegação principal e selecione “MY TISAX” (“MY TISAX” (MEU TISAX)).
3. No menu suspenso, selecione “ADMINISTRATORS” (“ADMINISTRATORS” (ADMINISTRADORES)).
4. Vá até a tabela e encontre a linha da tabela com o contato.
5. Vá até o final da linha da tabela do contato e clique no botão com a seta para baixo .
6. Selecione “Edit TISAX Administrator” (“Edit TISAX Administrator” (Editar Administrador TISAX)).
7. Atualizar os dados.
8. Clique no botão “Save Contact” (“Save Contact” (Salvar contato)).

7.9.3. Administração das localizações

Os principais contatos participantes da sua empresa e todos os demais “contatos administrativos” com contas no portal podem sempre acessar o portal ENX e solicitar a:

- mudança do nome da empresa
- mudança de localização (mudança/relocalização)
- mudança do nome da rua
- adição de uma nova localização

Descrevemos as etapas necessárias nas seções a seguir.

Observe:

- No TISAX, a combinação do nome de uma empresa e de um endereço define uma “localização”.
- Cada localização tem um “ID da localização” (Os IDs da localização sempre começam com “L” e têm seis caracteres; Exemplo: L1L3XY).
- Se a sua empresa mudar do endereço atual para um novo endereço, a localização antiga não será mais uma localização válida.

Observação importante:

Depois de clicar no botão “Save Location” (Salvar localização) no portal ENX, não será mais possível alterá-lo por sua própria conta. Nas situações descritas

abaixo, você pode solicitar mudanças.

7.9.3.1. Como solicitar a mudança do nome da sua empresa

Sua situação:	Sua empresa mudou de nome.
Exemplo:	O nome antigo da empresa é “ACME Tires Corporation”. O novo nome da empresa é “ACME Corporation”.

Caso queira solicitar a mudança do nome da sua empresa, siga estas etapas:

1. Faça login no portal ENX.
2. Acesse a barra de navegação principal e selecione “MY TISAX” (“MY TISAX” (MEU TISAX)).
3. No menu suspenso, selecione “LOCATIONS” (“LOCATIONS” (LOCALIZAÇÕES)).
4. Vá até a tabela e encontre a linha da tabela com a sua localização.
5. Vá até o final da linha da tabela da sua localização e clique no botão com a seta para baixo .
6. Selecione “Request Change” (“Request Change” (Solicitar mudança)).
7. Na nova janela (“Request Change” (“Request Change” (Solicitar alteração)), acesse o campo do formulário “Subject of the change” (“Subject of the change” (Assunto da alteração), abra o menu suspenso e selecione “Company Name” (“Company Name” (Nome da Empresa)).
8. Continue preenchendo o formulário
9. Envie o formulário

Vamos verificar a sua solicitação, possivelmente aceitar a solicitação de mudança do nome da empresa e informar você assim que isso for feito.

7.9.3.2. Como solicitar a mudança de uma localização)

Sua situação:	Sua empresa mudou para uma nova localização.
Exemplo:	A localização antiga é “ACME Corporation, Bockenheimer Landstraße 97-99, 60325 Frankfurt, Alemanha”. A nova localização é “ACME Corporation, Behrenstraße 35, 10117 Berlim, Alemanha”.

Observação importante:

Se uma autoridade oficial mudou o nome da rua da sua localização, consulte Seção 7.9.3.3, “Como solicitar a mudança do nome da rua” para obter mais informações.

Se uma das suas localizações for transferida para um novo endereço, siga estas etapas:

1. Criar uma nova localização:
   a. Faça login no portal ENX.
   b. Acesse a barra de navegação principal e selecione “MY TISAX” (“MY TISAX” (MEU TISAX)).
   c. No menu suspenso, selecione “Locations” (“LOCATIONS” (LOCALIZAÇÕES)).
   d. Clique no botão “Create TISAX Location” (“Create TISAX Location” (Criar localização TISAX)).
   e. Na nova janela (“CREATE TISAX LOCATION” (“CREATE TISAX LOCATION” (CRIAR LOCALIZAÇÃO TISAX)), preencha o formulário com os dados da nova localização.
   f. Clique no botão “Save Location” (“Save Location” (Salvar localização)).
2. Lembre-se do “Location ID” (“ID da localização”) da localização recém-criada. Você pode encontrar o “ID da localização” na primeira coluna da tabela “MY LOCATIONS” (“MY LOCATIONS” (MINHAS LOCALIZAÇÕES)). Seu provedor de auditoria precisa do “ID da localização” para atualizar o escopo da sua avaliação no portal ENX.
3. Informe seu provedor de auditoria sobre a mudança (forneça o “ID da localização” da localização antiga, bem como da nova localização).
   Você já concluiu a avaliação?
   a. Se a resposta for NÃO, então não há mais nada a fazer em relação à mudança de localização.
   b. Se a resposta for SIM, você precisará solicitar uma “avaliação da ampliação do escopo” (“scope extension assessment”) ao seu provedor de auditoria. Para obter mais informações, consulte a Seção 7.10, “Anexo: Avaliação da ampliação do escopo”.

O provedor de auditoria verificará sua solicitação e atualizará o escopo da avaliação no portal ENX.

Observe:

Um provedor de auditoria só poderá atualizar o escopo da sua avaliação se você já tiver solicitado a avaliação desse provedor de auditoria.

7.9.3.3. Como solicitar a mudança do nome da rua

Sua situação: O nome da rua da sua localização mudou. Sua empresa ainda está no mesmo local físico.

Exemplo: A localização antiga é “ACME Corporation, Bockenheimer Landstraße 97-99, 60325 Frankfurt, Alemanha”.
A nova localização é “ACME Corporation, Behrenstraße 97-99, 60325 Frankfurt, Alemanha”.

Se uma autoridade oficial mudou o nome da rua da sua localização, siga estas etapas:

1. Faça login no portal ENX.
2. Acesse a barra de navegação principal e selecione “MY TISAX” (“MY TISAX” (MEU TISAX)).
3. No menu suspenso, selecione “Locations” (“Locations” (Localizações)).
4. Vá até a tabela e encontre a linha da tabela com a sua localização.
5. Vá até o final da linha da tabela da sua localização e clique no botão com a seta para baixo .
6. Selecione “Request Change” (“Request Change” (Solicitar mudança)).
7. Na nova janela (“Request Change” (“Request Change” (Solicitar alteração)), acesse o campo do formulário “Subject of the change” (“Subject of the change” (Assunto da alteração), abra o menu suspenso e selecione “Address” (“Address” (Endereço)).
8. Continue preenchendo o formulário
9. Envie o formulário

Vamos verificar a sua solicitação, possivelmente aceitar a solicitação de mudança do nome da rua e informar você assim que isso for feito.

Observação importante:

Essas etapas só são aplicadas quando sua empresa ainda está no mesmo local físico, mas uma autoridade oficial mudou o nome da rua.
Se você mudou para uma nova localização, consulte a Seção 7.9.3.2, “Como solicitar a mudança de uma localização)” para obter mais informações.

7.9.3.4. Como adicionar uma outra localização

Se você abrir uma localização adicional durante o período de validade de seus selos TISAX existentes, poderá solicitar uma “avaliação da ampliação do escopo” (“scope extension assessment”) ao seu provedor de auditoria.

Para obter mais informações, consulte a Seção 7.10, “Anexo: Avaliação da ampliação do escopo”.

7.10. Anexo: Avaliação da ampliação do escopo

Além dos tipos de avaliação padrão descritos em Seção 5.4.3, “Tipos de avaliação TISAX”, existe

outro tipo de avaliação especial: a “avaliação da ampliação do escopo” (“scope extension assessment”).

Você pode estender um escopo da avaliação TISAX existente se desejar adicionar um ou mais:

- objetivos da avaliação, ou
- localizações.

Você não pode selecionar outro provedor de auditoria para realizar uma “avaliação da ampliação do escopo”. A avaliação é semelhante aos tipos de avaliação padrão. No entanto, seu provedor de auditoria provavelmente vai considerar a reutilização dos resultados aplicáveis das avaliações anteriores.

Assim que a avaliação da ampliação do escopo for concluída sem não conformidades, seu provedor de auditoria vai:

- atualizar o escopo da sua avaliação no portal ENX.
- emitir o relatório da avaliação da ampliação do escopo.

Uma avaliação da ampliação do escopo não estende o período de validade original de seus selos TISAX existentes.

Observe:

Se o motivo da avaliação da ampliação do escopo for uma mudança ou uma localização adicional, será necessário criar a nova localização no portal ENX. Forneça o “Extrato da localização” ou pelo menos o “ID da localização” ao seu provedor de auditoria.
Cada localização tem um “ID da localização” (Os IDs da localização sempre começam com “L” e têm seis caracteres; Exemplo: L1L3XY). Seu provedor de auditoria precisa do ID da localização para atualizar o resultado da sua avaliação no portal ENX.

7.11. Anexo: Gerenciamento do ciclo de vida da ISA

Um grupo de trabalho ENX está mantendo a ISA.

Esses fatos podem ser do seu interesse:

- A VDA publica oficialmente novas versões.
- O provedor de auditoria vai usar a versão da ISA válida quando você *pedir* sua avaliação inicial
- Por acordo mútuo, você pode usar uma versão mais recente da ISA se alguma for publicada entre seu pedido e o início da avaliação inicial.

- Você pode encontrar a data de publicação de uma determinada versão da ISA na planilha Excel “Capa”.
  - Exemplo:
    Versão: 5.0 | Revisão 4 | 2021-04-16

7.12. Anexo: Documentos úteis

Essa seção lista os documentos que consideramos úteis.

- Artigo técnico “Harmonization of classification levels” (Harmonização dos níveis de classificação)

  “Esse Artigo técnico descreve a proposta do grupo de trabalho de segurança da informação para determinar um esquema com foco no objetivo de proteção da confidencialidade; isso significa que as informações não são acessíveis a pessoas, organizações ou processos não autorizados. Além disso, os objetivos de proteção como disponibilidade, integridade e confiabilidade não são o foco desse Artigo técnico.”

  Editora: Verband der Automobilindustrie e.V. (“Associação Alemã do Setor Automotivo”).

  Idiomas disponíveis: inglês, alemão

  https://www.vda.de/en/news/publications/publication/harmonization-of-classification-levels
  https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--harmonisierung-der-klassifizierungsstufen-

- Artigo técnico “Information Security Risk Management” (Gerenciamento de riscos de segurança da informação)

  “O objetivo desse Artigo técnico é informar as empresas do setor automotivo no que diz respeito ao gerenciamento de segurança da informação orientado aos riscos e permitir que elas estabeleçam um gerenciamento eficaz de riscos de segurança da informação. Tem como objetivo auxiliar as organizações na preparação ou realização de uma avaliação TISAX para atender aos requisitos da pergunta de controle 1.4.1 da VDA ISA. Seu conteúdo deve ser considerado como recomendações de implementação, não como requisitos obrigatórios.”

  Editora: Verband der Automobilindustrie e.V. (“Associação Alemã do Setor Automotivo”).

  Idiomas disponíveis: inglês, alemão

  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. Anexo: Gerenciamento de reclamações

7.13.1. Causas para reclamação

Nosso gerenciamento de reclamações diferencia estas duas áreas:

1. ENX Association — a organização que regulamenta o TISAX
2. Provedores de auditoria — as organizações que realizam as avaliações TISAX

7.13.1.1. Reclamações sobre a ENX Association

Se tiver uma reclamação sobre a ENX Association, entre em contato com nosso “gerente de plantão TISAX” (veja os dados de contato abaixo).

7.13.1.2. Reclamações sobre provedores de auditoria

Primeiro, você deve tentar solucionar o problema diretamente com o auditor.

A próxima etapa deve ser a pessoa responsável pelo TISAX diante do provedor de auditoria.

Posteriormente, seu próximo contato será a pessoa responsável pelo gerenciamento de qualidade do provedor de auditoria.

Se o problema ainda não for resolvido, você deve entrar em contato com nosso “gerente de plantão TISAX” (veja os dados de contato abaixo).

Existem até opções acima do “gerente de plantão TISAX”. Nesses casos, você conversaria com o diretor administrativo da ENX Association.

A VDA não tem qualquer papel no gerenciamento de reclamações.

Observe:

O provedor de auditoria deve informar você sobre o seu direito de reclamar durante a reunião inicial. Se ele não fizer isso, já seria motivo para uma reclamação.

7.13.1.3. Requisitos para reclamações

Se desejar nos envolver, precisamos das seguintes informações:

- Quem está reclamando?
  - Nome da empresa
  - ID de participante TISAX
  - Contato (nome, endereço de e-mail, número de telefone)

- Qual avaliação é essa?
  - ID da avaliação
  - Caso a avaliação ainda não esteja registrada no portal ENX: ID do escopo
- Quem é o provedor de auditoria?
  - Nome da empresa do provedor de auditoria
  - Nome do(s) auditor(es)
- Sobre o que você está reclamando?
  1. Reclamação geral sobre o desempenho do provedor de auditoria
  2. Reclamação sobre a abordagem do auditor
  3. Reclamação sobre a avaliação em relação ao conteúdo
- Em caso de reclamações sobre a avaliação em relação ao conteúdo: Qual achado você contesta?
  - Controle (por exemplo, 1.6.1 "Até que ponto os eventos de segurança da informação são processados?")
  - Achado (texto completo)
  - Objeção contra:
    - Interpretação do controle
    - Averiguação em relação ao conteúdo (as evidências disponíveis não foram avaliadas corretamente)
    - Avaliação do risco (adequação não considerada)
  - Explicação sobre o motivo pelo qual você avalia as coisas de forma diferente.

7.13.2. Contato para reclamações

Entre em contato com o “gerente de plantão TISAX”:

Envie um e-mail para ele no endereço:	tisax-complaints@enx.com
Ou ligue para ele no número:	+49 69 9866927-79

Você pode entrar em contato com ele durante o horário comercial normal na Alemanha (UTC+01:00).

Ele fala inglês e alemão.

8. Histórico do documento

Versão 2.7

- Mais quatro línguas (Japonês, Português do Brasil, Italiano, Coreano) incluídas
- Inclusão de um botão de mudança de idioma para versões HTML (no canto superior direito)
- Melhoria do layout das versões em PDF
- Atualização de várias seções com os dois novos objetivos de avaliação de confidencialidade
- Atualização da seção “List of assessment objectives” (Lista de objetivos da avaliação) (redação do objetivo da avaliação “Special data” corrigida; adição de uma nota a respeito da transição de selo)
- Correção dos erros de digitação

Versão 2.6

- Observação geral sobre os objetivos e selos da avaliação que adicionamos nesta versão: nas versões anteriores, os objetivos e selos da avaliação tinham um “nome oficial” completo e um “nome abreviado” (Exemplo: “tratamento de informações com necessidades de proteção elevadas” e “Informações elevadas”). Como a maioria das pessoas quase usava apenas o nome abreviado, a forma abreviada agora é o “nome oficial”. O antigo nome completo agora é denominado “Descrição”. Além disso, usamos *apenas* o nome oficial em inglês no portal ENX e em todas as traduções do manual do participante TISAX.
- Atualização da seção “List of assessment objectives” (Lista de objetivos da avaliação) com os dois objetivos da avaliação “High availability” (disponibilidade elevada) e “Very high availability” (disponibilidade muito elevada) e “Figura 6. Objetivos da avaliação TISAX (representação em tabela, formatos completos e abreviados)” removidos
- Atualização da seção “Assessment objectives and ISA” (Objetivos da avaliação e a ISA) para refletir o fato de que apenas um subconjunto da lista de critérios de Segurança da informação se aplica aos dois objetivos da avaliação “High availability” e “Very high availability”
- Remoção da seção “Assessment objectives and their dependencies” (Objetivos da avaliação e suas dependências)
- Atualização da seção “Assessment objective selection” (Seleção do objetivo da avaliação) com os dois objetivos d avaliação “High availability” e “Very high availability”
- Atualização da seção “Protection needs and assessment levels” (Necessidades de proteção e níveis da avaliação) com os dois objetivos da avaliação “High availability” e “Very high availability” e “Tabela 5. Mapeamento de listas de critérios da ISA e necessidades de proteção para os objetivos da avaliação TISAX” removido
- Atualização da seção “Criteria Catalogues” (Listas de critérios) com os dois objetivos da

avaliação “High availability” e “Very high availability”

- Atualização da seção “Requirements” (Requisitos) para refletir o fato de que apenas um subconjunto da lista de critérios de Segurança da informação se aplica aos dois objetivos da avaliação “High availability” e “Very high availability”
- Atualização da seção “TISAX label hierarchy” (Hierarquia dos selos TISAX) para refletir o fato de que uma hierarquia agora só existe em alguns casos e “Figura 36. Remoção dos objetivos da avaliação TISAX e dos selos TISAX (dependências e hierarquia)”
- Atualização da seção “Annex: Helpful documents” (Anexo: Documentos úteis) para refletir as alterações nos links
- Vários pequenos esclarecimentos e pequenas correções
- Correção dos erros de digitação

Versão 2.5.1

- Correção dos links quebrados

Versão 2.5

- Adição da seção “Administration of locations” (Administração das localizações)
- Atualização da seção “Annex: Helpful documents” (Anexo: Documentos úteis) para refletir as alterações nos links

Versão 2.4

- Declaração imprecisa sobre a duração máxima do processo de avaliação TISAX removida de Seção 3.1, “Visão geral”
- Mudança de nome do “Relatório TISAX” para “Relatório de avaliação TISAX”
- Atualização da observação em relação às diferenças entre ISO 27001 e TISAX
- Atualização da seção “Scope description” (Descrição do escopo); seção de escopo personalizado movida para o anexo
- “Standard scope description” (Descrição do escopo padrão) atualizada para a versão 2.0
- Atualização da seção “Publication and sharing” (Publicação e compartilhamento) com observação sobre o compartilhamento do status da avaliação
- Atualização da seção “Protection needs and assessment levels” (Necessidades de proteção e níveis de avaliação) com conteúdo sobre “nível de avaliação 2,5”, o “método de avaliação remota com suporte de vídeo”, as diferenças entre AL 2 e AL 3, verificação de plausibilidade versus verificação

- Atualização do link para início do processo de cadastro
- Atualização da seção “Portal account” (Conta do portal) para refletir a alteração do processo de convite
- Alteração dos links de download para o documento da ISA (agora também disponível em enx.com)
- Atualização da seção “Evaluating offers” (Avaliação das propostas) com uma base para as estimativas dos custos
- Adição da seção “Kick-off meeting” (Reunião inicial) (com conteúdo movido da seção “The first formal opening meeting” (A primeira reunião formal de abertura)
- Atualização da seção “About conformity” (Sobre a conformidade) com uma nova tabela sobre os quatro tipos de achados
- Atualização da seção “Initial assessment” (Avaliação inicial) com observação sobre as restrições de tempo
- Atualização da seção “TISAX assessment report” (Relatório de avaliação TISAX) com observação sobre um plano de ação corretiva proativo
- Atualização da seção “Corrective action plan preparation” (Preparação do plano de ação corretiva) com os requisitos “achado” e “causa raiz” e uma observação sobre os modelos do plano de ação corretiva
- Atualização da seção “Corrective action plan assessment” (Avaliação do plano de ação corretiva) com uma observação sobre o e-mail como único meio de comunicação
- Mudança de nome da seção “Prerequisites for a corrective action plan assessment” (Pré-requisitos para uma avaliação do plano de ação corretiva) para “Reasons for a corrective action plan assessment” (Motivos para uma avaliação do plano de ação corretiva) e adição de dois motivos
- Atualização da seção “Temporary TISAX labels” (Selos TISAX temporários) com exemplos e esclarecimentos sobre o período de validade
- Mudança de nome da seção “TISAX report” (Relatório TISAX) para “TISAX assessment report” (Relatório de avaliação TISAX)
- Atualização da seção “Renewal of TISAX labels” (Renovação de selos TISAX) com observação sobre a reutilização de cadastros da localização no portal ENX
- Adição da seção “Annex: The reasoning against “pre-assessments” and “gap analyses” (Anexo: a lógica contra “avaliações prévias” e “análises de lacunas”)”
- Adição da seção “Annex: Custom scopes” (Anexo: Escopos personalizados) (“Extended scope” (Escopo ampliado) e “Narrowed scope” (Escopo restrito) substituídos por “Customer extended scope” (Escopo ampliado do cliente) e “Full custom scope” (Escopo personalizado completo)
- Atualização da seção “Annex: Scope extension assessment” (Anexo: Avaliação da ampliação

do escopo) com os motivos e uma observação sobre a adição de registros da localização à conta do portal ENX do participante

- Atualização da seção “Annex: ISA life cycle management” (Anexo: Gerenciamento do ciclo de vida da ISA) para refletir a situação atual
- Atualização da seção “Annex: Helpful documents” (Anexo: Documentos úteis) para refletir as alterações nos links
- Adição da seção “Annex: Complaint management” (Anexo: Gerenciamento de reclamações)
- Os números de telefone agora podem ser clicados
- Vários pequenos esclarecimentos e pequenas correções
- Correção dos erros de digitação
- Observação para os provedores de auditoria TISAX: essa atualização é baseada no documento ENX ID 612 versão 2.1

Versão 2.3

- Reformulação da legenda
- Mudança de Word/PDF para HTML como formato principal do manual
- Outras traduções disponíveis (chinês e francês, veja o próximo item)
- Adição da seção “The TISAX participant handbook in other languages and formats” (Manual do participante TISAX em outros idiomas e formatos)
- Todos os links para a página inicial da ENX foram alterados de "https://portal.enx.com" para "https://enx.com" (os links antigos ainda funcionam)
- “VDA ISA” passa a ser “ISA”
- Atualização da seção Seção 5.2, “Autoavaliação baseada na ISA” para refletir as alterações introduzidas com a ISA versão 5
- Reordenação das linhas de todas as tabelas que listam os objetivos da avaliação para corresponder à ordem alterada das listas de critérios na ISA 5
- Atualização das figuras que listam os objetivos da avaliação para corresponder à ordem alterada das listas de critérios da ISA 5
- Atualização da seção “Scope tailoring” (Adaptação do escopo) (correção da figura 6, correção do erro de digitação, atualização dos objetivos da avaliação)
- Atualização da seção “Fee” (Taxa) com informações sobre os pagamentos com cartão de crédito
- Atualização da seção “TISAX assessment process diagram” (Diagrama do processo de avaliação TISAX) (figura 34, remoção da referência ao provedor de serviços gerenciados)

- Atualização da seção “Annex: Helpful documents” (Anexo: Documentos úteis) (adição do Artigo técnico “Information Security Risk Management” (Gerenciamento de riscos de segurança da informação))

Versão 2.2.1

- Correção dos erros de digitação

Versão 2.2

- Correção do problema de impressão da capa
- Alteração de todos os links para nossa página inicial e os downloads
- Agora também falamos italiano
- Ampliação da seção “Custom scope” (Escopo personalizado)
- Atualização da seção “Scope locations” (Localizações do escopo)
- Atualização dos objetivos da avaliação remoção da “Conexão com terceiros”; atualização das figuras 7, 9 e 38; atualização das tabelas 4, 5, 6 e 8
- A redação “*com* nível de avaliação” foi alterada para “*no* nível de avaliação”
- Remoção da referência à “lista de ativação TISAX” na seção “Protection needs and assessment levels” (Necessidades de proteção e níveis de avaliação)
(não é mais aplicável)
- Adição da seção “Assessment objectives and your own suppliers” (Objetivos de avaliação e seus próprios fornecedores)
- Atualização da seção “Participant contact” (Contato do participante) com informações sobre endereços de e-mail de grupo e contatos convidados para permitir que eles gerenciem os dados dos participantes no portal ENX
- Atualização da seção “Assessment scope registration” (Cadastro do escopo da avaliação) com informações sobre as alterações no escopo da avaliação
- Atualização da seção “Status information” (Informações de status) (figura 12)
- Atualização da seção “Address the self-assessment result” (Abordagem do resultado da autoavaliação) com informações sobre a ajuda externa de terceiros
- Atualização da seção “Coverage” (Abrangência) com link para a matriz de cobertura do provedor de auditoria
- Atualização da seção “Requesting offers” (Solicitação de propostas)
- Atualização da seção “Evaluating offers” (Avaliação das propostas) com informações sobre “avaliações prévias”

- Atualização da seção “Renewal of TISAX labels” (Renovação de selos TISAX) com informações sobre a necessidade de cadastrar um novo escopo
- Atualização de várias subseções da seção “Exchange (Step 3)” (Compartilhamento (Etapa 3)) para refletir as mudanças na interface do portal ENX
- Atualização da seção “Share your assessment result with a particular partner” (Compartilhe o resultado da sua avaliação com um parceiro específico) com recomendações sobre o nível de compartilhamento e observação sobre o processamento automatizado dos resultados de avaliações compartilhadas
- Adição da seção “Sharing your assessment result outside TISAX” (Compartilhamento do resultado da sua avaliação fora do TISAX)
- Adição da seção “ISA lifecycle management” (Gerenciamento do ciclo de vida da ISA)
- Atualização da seção “Annex: Assessment scope status” (Anexo: status do escopo da avaliação) (novo status “Awaiting your order” (Aguardando seu pedido), mudança de nome do status “Awaiting approval” (Aguardando aprovação) para “Awaiting ENX approval” (Aguardando aprovação da ENX), mudança de nome do status “Approved” (Aprovado) para “Awaiting your payment” (Aguardando seu pagamento), figura 40)
- Atualização da seção “Annex: Example confirmation email” (Anexo: Exemplo de e-mail de confirmação)
- Atualização da seção “Annex: Example TISAX Scope Excerpt” (Anexo: Exemplo do extrato do escopo TISAX)
- Atualização da seção “Annex: Assessment status” (Anexo: Status da avaliação) (novo status “Initial assessment ongoing” (Avaliação inicial em andamento), mudança de nome do status “Waiting for follow-up assessment” (Aguardando avaliação de acompanhamento) para “Waiting for follow-up” (Aguardando acompanhamento), figura 41)
- Remoção da seção “Annex: Volkswagen legacy assessments” (Anexo: Avaliações do legado da Volkswagen) (e referências) (não é mais relevante)

Versão 2.1.2

- Correção do limite formal da “distância” entre a “sua pontuação do resultado” e a “pontuação máxima do resultado” de 25% para 30%

Versão 2.1.1

- Correção dos erros de digitação

Versão 2.1

- Remoção da seção “Managed Service Providers” (Provedores de serviços gerenciados)
- Novos objetivos da avaliação TISAX/selos (selos de proteção de dados baseados no RGPD; quatro em vez de dois protótipos de selos; Renomeação: necessidades de proteção em vez de níveis de proteção; atualização dos conselhos de seleção)
- Atualizações devido a alterações na ISA (versão 4.0 a 4.1)
- Consulte o novo documento “TISAX Simplified Group Assessment” (Avaliação de grupo simplificada TISAX) (anexo a este manual)
- Adição de sugestões para atribuição de nomes das localizações e nomes do escopo
- Mudança de nome de “taxa de cadastro” para “taxa”
- Recomendação de adição de representantes para contato
- Remoção da seleção do modelo de cobrança

Voltar ao início.

[1] Você pode considerar passar pelo processo TISAX como uma etapa preventiva. Algumas empresas fazem isso para estarem mais bem preparadas. Já ter sido avaliado pelo TISAX pode significar um período de integração muito mais curto e, portanto, pode dar a você uma vantagem sobre concorrentes que ainda não passaram pela avaliação do TISAX.

[2] “Selos TISAX” são um conceito para resumir o resultado da sua avaliação e são o resultado do processo TISAX. Consulte a Seção 5.4.14, “Selos TISAX” para obter mais detalhes.

[3] Você só precisa realizar a maioria das etapas de cadastro uma vez quando começar como participante TISAX. Ao renovar o resultado da sua avaliação, você só precisa atualizar e confirmar seus dados de cadastro.

[4] Vamos publicar alterações em nossos TCGs no portal ENX e notificar os contatos cadastrados.

[5] Isso também se aplica a todos os outros acordos adicionais (por exemplo, códigos de conduta).

[6] Observe que atualmente seu parceiro não é informado automaticamente sobre novas permissões. Você pode notificar seu parceiro assim que o resultado da avaliação estiver disponível para ele.

[7] Se você quiser estar nessa lista, entre em contato conosco.

[8] Evidência é algo que apoie a afirmação de que você cumpre um determinado requisito. As evidências são principalmente documentos. Certamente você vai utilizar documentação interna como evidência.

[9] As entrevistas para avaliações com nível de avaliação 2 são geralmente realizadas via teleconferência. A seu pedido, as entrevistas podem ser realizadas no local

[10] O mínimo teórico para avaliações simplificadas em grupo é de três localizações.

[11] Se você já sabe que vai precisar melhorar seu sistema de gerenciamento de segurança da informação, o mínimo recomendado é de pelo menos doze localizações.

[12] Para evitar possíveis confusões entre números e letras (como 8 e B), algumas letras não são permitidas nos IDs de Participante. No entanto, alguns IDs de participante mais antigos podem conter a letra “G”.

[13] A ISA também se refere às listas de critérios como “módulos”.

[14] Você pode encontrar o recurso subjacente do Excel na faixa “Data” (Dados), seção “Outline” (Esboço).

[15] Você tem provedores de auditoria para sua empresa para avaliações semelhantes (como ISO 27001) que também estão interessados em realizar as avaliações TISAX? Em seguida, compartilhe este manual com eles e peça para entrarem em

contato conosco para saberem o que é necessário para se tornar um provedor de auditoria TISAX

[16] Os provedores de auditoria que não estão incluídos em nossa listagem não estão autorizados a realizar avaliações TISAX.

[17] Se você encerrar o processo de avaliação, não receberá os selos TISAX.

[18] Na verdade, existe um quarto tipo: A “avaliação da ampliação do escopo”. Por se tratar de um caso especial, está descrito detalhadamente no anexo na Seção 7.10, “Anexo: Avaliação da ampliação do escopo”.

[19] A reunião formal de *abertura* será descrita em detalhes apenas para a avaliação inicial. Para as outras avaliações TISAX, seu provedor de auditoria vai agendar e configurar essas reuniões.

[20] Alguns provedores de auditoria podem usar o termo “reunião inicial” como sinônimo de “reunião formal de abertura”.

[21] A reunião formal de *encerramento* será descrita em detalhes apenas para a avaliação inicial. Para as outras avaliações TISAX, seu provedor de auditoria vai agendar e configurar essas reuniões.

[22] Se uma divergência não puder ser resolvida, você poderá encaminhar o problema. Para obter mais informações, consulte Seção 7.13, “Anexo: Gerenciamento de reclamações” para obter mais detalhes.

[23] Para obter mais informações sobre os métodos e intensidades da auditoria, consulte Seção 4.3.3.5, “Necessidades de proteção e os níveis de avaliação”.

[24] Se uma divergência não puder ser resolvida, você poderá encaminhar o problema. Entre em contato conosco para obter mais detalhes.

[25] Observe que o resultado geral da sua avaliação ainda pode ser “não conformidade importante”, mesmo que você tenha definido as ações corretivas adequadas. Esse é o caso se suas medidas não entrarem em vigor imediatamente.

[26] Isso, é claro, é aplicável apenas a uma avaliação inicial que identificou não conformidades. Você não precisa de uma avaliação de acompanhamento para uma avaliação inicial com um resultado de avaliação de “conformidade”.

[27] Em teoria, isso pode ser nove meses após a conclusão da avaliação inicial.

[28] Na verdade, existe um quarto tipo: O “relatório da avaliação da ampliação do escopo”. Por se tratar de um caso especial, está descrito detalhadamente na Seção 7.10, “Anexo: Avaliação da ampliação do escopo”.

[29] O “relatório de avaliação TISAX” tem por base um modelo que todos os provedores de auditoria TISAX são obrigados a utilizar.

[30] A palavra “renovação” pode dar a entender algo errado. Para manter um selo TISAX por mais de três anos, você precisa realizar novamente o processo TISAX. Isso começa com o cadastro de um novo escopo de avaliação.

[31] Não mantemos uma lista “pública TISAX” de IDs de participantes. O motivo para isso é que queremos evitar o compartilhamento acidental com base em nomes de empresas com sons semelhantes ou outros “erros humanos”. Portanto, você sempre deverá obter o ID de participante do seu parceiro entrando em contato diretamente com ele.

[32] Seu parceiro deve fazer login no portal e procurar de forma ativa o resultado da avaliação compartilhada. Seu parceiro não recebe uma notificação automática sobre os novos resultados das avaliações compartilhadas.

[33] A regra está definida nos “Termos e Condições Gerais de Participação TISAX” (https://enx.com/tisaxgtcen.pdf).

[34] Enquanto estiver no status do escopo da avaliação “Awaiting your payment” (Aguardando seu pagamento) ou “Registered” (Cadastrado) “Assessment Related information” (Informações relacionadas à avaliação) inclui a(s) localização(ões) do escopo da avaliação, o status do escopo da avaliação e o(s) objetivo(s) da avaliação. Não inclui os resultados da avaliação ou os selos TISAX.

[35] “Selos TISAX” são um conceito para resumir o resultado da sua avaliação e são o resultado do processo TISAX. Consulte a Seção 5.4.14, “Selos TISAX” para obter mais detalhes.