Comunicado Externo – ERRATA
TÜV NORD Brasil

ISO 27001:2022 – Regras de Transição
Informações importantes sobre sua certificação ISO 27001

Prezados clientes,

Como vocês provavelmente já ouviram, a ISO/ IEC 27001 foi revisada e publicada como norma internacional ISO/ IEC 27001:2022 em outubro de 2022.

O IAF (International Accreditation Forum) definiu, através do documento IAF MD 26, datado de 15/02/2023, um período de transição de 3 anos e considerou algumas medidas transitórias. O que significa que depois do período de transição, qualquer certificação de acordo com a ISO 27001 deve ser baseada exclusivamente na Nova Edição e todos os certificados baseados na edição anterior se tornarão inválidos, independentemente da data de expiração do certificado.

Continuação da certificação ISO 27001 com a nova versão.
Por favor, note as seguintes condições gerais definidas pelo IAF:

Todo certificado ISO 27001:2013 se tornará inválido em 31/10/2025, se a transição não tiver sido completada antes.

Toda auditoria de certificação inicial e auditoria de recertificação iniciando em 01/05/2024 ou depois desta data devem ser conduzidas bom base na ISO 27001:2022. O ponto de partida é o primeiro dia da auditoria on-site (auditoria de fase 1).

Quaisquer decisões de certificação para atualizar a atual certificação ISO 27001:2013 deve ser completada até 31/05/2025. Caso contrário, deverá ser efetuada uma nova certificação inicial.

Auditorias de transição exigirão uma duração adicional de auditoria on-site. Esta duração extra será um evento único somente válido para esta transição de auditoria.

A transição pode ser realizada sob a forma de auditoria de recertificação, monitoração 12° mês, monitoração 24° mês ou como uma auditoria extraordinária.

Auditorias de acordo com a nova edição da ISO 27001 devem ser efetuadas somente por equipes de auditores que tenham sido treinados nos novos requisitos e tenham sido qualificados na nova norma.

Atividades das organizações que procuram uma transição da certificação ISO 27001

Para cada organização, a extensão da mudança requerida depende da maturidade e efetividade do atual Sistema de Gestão em Segurança da Informação (ISMS), estruturas e processos / procedimentos organizacionais. Portanto, a fim de identificar o impacto sobre os recursos e os prazos, é fortemente recomendada a análise/ avaliação dos impactos.

Para as organizações que estão usando um ISMS baseado na ISO 27001:2013, são recomendadas as seguintes ações:

- Identificar as lacunas organizacionais que precisam ser abordadas de forma a cumprir os novos requisitos;
- Preparação de um plano de transição;

- Providenciar treinamento apropriado e sensibilizar todas as partes que influenciam a efetividade da organização;
- Atualizar o ISMS existente para cumprir os requisitos revisados e apresentar provas de eficácia.

Por favor, tenha em conta que uma auditoria interna completa e uma evolução do sistema de gestão de acordo com a nova edição da ISO 27001:2022 deve ser demonstrada na auditoria de transição.

Regras de cálculo para duração da auditoria adicional

Nos requisitos de transição do documento IAF MD 26:2022, capítulo 4.2, contém um regulamento do tempo adicional de auditoria requerido nas auditorias de transição. O TÜV NORD decidiu adotar esta abordagem e modifica-la em relação ao tipo de auditoria (auditoria de site único ou auditoria multisite). Isso nos leva aos seguintes resultados:

Tipo	Auditoria site único	Auditoria multisite
Transição em auditoria de recertificação	0,5 manday adicional	0,5 manday adicional na função central + manday adicional por site da amostragem
Transição em uma auditoria regular de monitoração	1 manday adicional	1,0 manday adicional na função central + manday adicional por site da amostragem
Transição em uma auditoria extraordinária	1 manday adicional	1,0 manday adicional na função central + manday adicional por site da amostragem

Nota: Se a transição for efetuada em uma auditoria extraordinária, então esta deve ser calculada como uma auditoria de monitoração com uma duração adicional descrita aqui – isto definitivamente representa uma solução “mais cara”.

Uma auditoria inicial completa (fase 1 e fase 2) para ISO 27001:2022 não requer um tempo de auditoria adicional e pode substituir qualquer outra auditoria de transição.

Se uma transferência de um organismo de certificação para outro for pretendido, a transferência de certificação de acordo com a ISO 27001:2013 deve ser totalmente completada antes de iniciar o planejamento de uma auditoria de transição (como descrito acima).

Após a transição em forma de uma auditoria extraordinária, uma auditoria de monitoração ou auditoria de recertificação, um novo certificado será emitido contendo a mesma data de validade do certificado de ISO 27001:2013.

Um novo ciclo de certificação completo de 3 anos deve ser somente concedido depois de uma auditoria de recertificação.

Resumo

De forma a continuar com uma certificação bem-sucedida de acordo com a ISO 27001, é necessário adaptar o sistema de acordo com a norma atualizada. Isto requer trabalho, tempo e dinheiro – mas cria resistência contra influências não autorizadas.

Esperamos continuar nossa cooperação com você.

Em caso de dúvidas, entrar em contato com Guilherme Moutinho (gmoutinho@tuv-nord.com)