La certificación de un sistema de gestión (BCMS, SGSI, SMS) consiste en la fase de oferta y contrato, la preparación de la auditoría, el desempeño de la auditoría de la fase I con la evaluación de la documentación de la dirección, el desempeño de la auditoría de la fase II, la emisión del certificado y los seguimientos / recertificación.

Si es necesario, se puede agregar el procedimiento de certificación para los sistemas de gestión (BCMS, SGSI, SMS) con evaluaciones de los estándares específicos del sector ("sector-specific-standards" = 3S).

De la familia ISO 27001 están por ejemplo:

- ISO 27010 Gestión de la seguridad de la información para comunicaciones intersectoriales e interorganizacionales.
- ISO 27011 Directrices de gestión de la seguridad de la información para organizaciones de telecomunicaciones basadas en ISO / IEC 27002
- ISO 27015 Pautas de gestión de seguridad de la información para servicios financieros.
- Código de práctica ISO 27017 para controles de seguridad de la información basado en ISO / IEC 27002 para servicios en la nube
- Código de práctica ISO 27018 para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII
- Normas de gestión de la seguridad de la información ISO27019 basadas en ISO / IEC 27002 para sistemas de control de procesos específicos de la industria de servicios públicos de energía.
- ISO 27799 Gestión de la seguridad de la información en salud utilizando ISO / IEC 27000

Algunos de los 3S de TN CERT tienen una acreditación propia o están en un procedimiento de acreditación, por ejemplo.

- BNetzA § 11 Abs.1aEnWG / Requisitos específicos para los operadores de redes de energía.
- IEC 62443-2-1 - Seguridad de la información / Ciberseguridad - Requisitos para un sistema de administración de seguridad IACS
- IEC 62443-2-4 - Seguridad de la información / Ciberseguridad – Requisitos para los proveedores de soluciones IACS.
- IEC 62443-3-2 - Seguridad de la información / Ciberseguridad – Evaluación de riesgos de seguridad y diseño del sistema

Algunos de los 3S de TÜV NORD CERT están hechos para "infraestructuras críticas", por ejemplo:

- TN CERT Sector-Specific-Standard (3S): Energía
- TN CERT Sector-Specific-Standard (3S): Agua
- TN CERT Sector-Specific-Standard (3S): Alimentación
- TN CERT Sector-Specific-Standard (3S): Técnicas de la información y telecomunicaciones
- TN CERT Sector-Specific-Standard (3S): Salud
- TN CERT Sector-Specific-Standard (3S): Seguros y Finanzas

- TN CERT Sector-Specific-Standard (3S): Transporte y Tráfico
- TN CERT Sector-Specific-Standard (3S): Administración
- TN CERT Sector-Specific-Standard (3S): Medios y Cultura

La lista de los 3S se actualizará permanentemente. Se proporcionarán los 3S adicionales si se solicitan.

Los auditores son seleccionados por el Organismo de Certificación de TÜV NORD CERT GmbH de acuerdo con su calificación.

1.- Procedimiento de Certificación

1.1.- Preparación de la auditoría

Una vez firmado el contrato, el auditor prepara la auditoría basándose en el cuestionario completado por la organización y la hoja de cálculo, y discute y acuerda el procedimiento adicional con la organización a ser auditada.

En caso de que existan circunstancias particulares en la organización que hagan necesario mantener una seguridad o confidencialidad adicional, se puede firmar un acuerdo de confidencialidad adicional.
El organismo de certificación debe ser notificado con anticipación si el cliente tiene documentos confidenciales que no pueden ser accesibles a los auditores. Antes de la auditoría, el organismo de certificación debe determinar si el sistema de gestión puede ser auditado adecuadamente en ausencia de estos registros. Si el organismo de certificación concluye que no es posible auditar adecuadamente el sistema de gestión sin revisar los registros confidenciales o confidenciales identificados, deberá informar a la organización cliente que la auditoría de certificación no puede realizarse hasta que se otorguen los acuerdos de acceso apropiados.

Durante la preparación de la auditoría de seguimiento o recertificación, las organizaciones a ser auditadas tienen el deber de informar los cambios fundamentales en su estructura organizativa o los cambios en el procedimiento al organismo de certificación.

1.2.- Auditoría Fase I

La Auditoría Fase I se lleva a cabo con el fin de
- Obtener y revisar la documentación del sistema de gestión requerida por la norma.
- Proporcionar un enfoque para la planificación de la auditoría de la Fase II
- Obtención del estado de preparación de la organización para la auditoría de la Fase II (basada en la comprensión del sistema de gestión en el contexto de las políticas y objetivos de la organización).

El cliente hace todos los arreglos necesarios para llevar a cabo la auditoría de certificación, incluida la disposición para examinar la documentación y el acceso a todas las áreas, los registros (incluidos los informes de auditoría interna y los informes de revisiones) y el personal para los fines de auditoría de certificación, auditoría de recertificación y resolución de quejas. El cliente suministra todos los documentos

necesarios para la auditoría, en su versión válida actual, al menos 4 semanas antes de la auditoría.

La Auditoría Fase I incluye, pero no se limita a, la revisión del documento. El organismo de certificación está de acuerdo con la organización cliente cuando y donde se lleva a cabo la revisión del documento.

La documentación de gestión actual está evaluada y consiste en:

BCMS – ISO22301	**ISMS – ISO 27001**	**SMS – ISO 20000-1**
Política y objetivos BCM	Política y objetivos ISMS	Política y objetivos SMS
Alcance del BCMS	Área de aplicación / alcance del ISMS	Área de aplicación / alcance del SMS.
Procedimientos BCMS	Procedimiento (s) y actividades del ISMS	Plan de gestión de servicios
Análisis de Impacto del Negocio Evaluación de riesgos	Declaración de aplicabilidad	Acuerdos de nivel de servicio documentados.
Estrategia de continuidad de negocio	Cualquier otro documento / registro relevante relacionado con la norma en la que se basa la auditoría.	Procesos y procedimientos documentados requeridos por la Norma.
Estructura de respuesta a incidentes Planes de continuidad de negocio / Planes de gestión de incidencias. BCM ejerciendo récords	Gestión de riesgos que incluye Descripción de la metodología de evaluación de riesgos. Informe de evaluación de riesgos Plan de tratamiento de riesgos	Registros requeridos por la Norma

El cliente deberá completar un listado de verificación específico por estándar antes de la Fase I de auditoría en los casos de evaluaciones de los 3S. El cliente recibe el formato de verificación antes.

La organización recibe un informe por escrito sobre los resultados de la auditoría de la Fase I, incluida la evaluación de la documentación y la revisión de la dirección, y por lo tanto, también tiene la oportunidad de eliminar cualquier no conformidad antes de la auditoría de la Fase II. También es posible enviar declaraciones con respecto a cualquier elemento que no esté claro.

Si las no conformidades se identificaron en la auditoría de la Fase I, estas deben ser corregidas por la organización antes de la auditoría de la Fase II.

Si al final no se puede establecer de manera positiva que la organización esté lista para la auditoría de la Fase II, la auditoría se interrumpe después de la auditoría de la Fase I.

El Auditor Jefe es responsable de la coordinación de las actividades de la auditoría de la Fase I y, si es necesario, de la coordinación y la cooperación de los auditores interesados entre ellos.

1.3.- Auditoría de Certificación (Fase II)

La auditoría se realiza de acuerdo con el plan de auditoría que se acordó con la compañía antes del inicio de la auditoría. La organización tiene el derecho de rechazar a los auditores que han sido nombrados. La compañía demuestra el uso y la eficacia de los procedimientos que se han descrito y establecido en la auditoría.
La auditoría comienza con una reunión de apertura, en la que los participantes se presentan entre sí. Se explica el procedimiento a seguir en la auditoría. En el marco de la auditoría a las instalaciones de la organización, los auditores revisan y evalúan la efectividad del sistema de gestión que se ha instalado.

Durante la auditoría, la organización le permite al equipo auditor ver los registros que se refieren a las áreas que se encuentran dentro del alcance de la auditoría y le permite al equipo acceder a las unidades de negocios relevantes.

Durante la auditoría, se inspeccionan los siguientes ítems, entre otros:

- Los documentos en los que se basa la evaluación.
- Evidencia de que las acciones para las revisiones de la dirección y las auditorías internas se han implementado, son efectivos y se mantendrán.
- La efectividad del sistema de gestión en las áreas dentro del alcance de la auditoría.
- Uso correcto del certificado / marca de certificación (si corresponde)
- Objeciones al sistema de gestión.
- La efectividad de las acciones correctivas con respecto a las no conformidades de la auditoría anterior (si corresponde).

La organización tiene el deber de registrar todas las objeciones que se refieren al sistema de gestión y su rectificación, y presentarlas durante la auditoría.
En la reunión final, se muestra el resultado de la auditoría, así como cualquier no conformidad que haya sido registrada, y se comunican a la organización.
Las no conformidades son requisitos que no se han cumplido, donde la organización tiene que instigar las acciones correctivas apropiadas y verificar estas acciones. Se debe proporcionar prueba correspondiente.

Las no conformidades pueden llevar a la presentación de documentos / procedimientos nuevos / revisados y / o incluso a una nueva auditoría.
El auditor jefe decide sobre el alcance de la re-auditoría. Solo se auditan los aspectos relevantes para la no conformidad (procesos, procedimientos, áreas de la empresa).
Una vez implementadas todas las acciones correctivas y corregidas y aprobadas todas las no conformidades, se elabora el informe de auditoría.

1.4.- Expedición del certificado

El certificado se emite cuando el organismo de certificación ha revisado y aprobado el expediente de certificación. La persona que revisa y libera el expediente no puede haber participado en la auditoría.

El certificado solo puede emitirse cuando el equipo de auditoría haya aceptado o verificado las no conformidades.

Los certificados son válidos por 3 años.

2.- Auditorías de Seguimiento

Los siguientes ítems son revisados durante la Auditoría de Seguimiento:

- La efectividad del sistema de gestión dentro de toda la empresa mediante una muestra aleatoria más pequeña.
- Uso correcto del certificado / marca de certificación.
- Objeciones al sistema de gestión.
- Efectividad de las acciones correctivas con respecto a las no conformidades de la auditoría anterior (si corresponde)

En la reunión final, se comenta el resultado de la auditoría y se comunica a la empresa, incluidas las no conformidades documentadas.

El cliente recibe un informe tras la Auditoría de Seguimiento.

Las Auditorías de Seguimiento deben realizarse una vez al año durante el período de validez del certificado (3 años).

Nuevos clientes:

- La fecha relevante para la auditoría programada para la auditoría de Auditoría de Seguimiento, que sigue a la auditoría de certificación, no debe ser posterior a los 12 meses posteriores al último día de la auditoría de la Fase II.

Clientes existentes:

- La fecha relevante para la auditoría de la Auditoría de Seguimiento anual es la fecha de validez del certificado, que era válida el 01 de enero de 2008 (día y mes) menos 1 mes.

Clientes nuevos y existentes:

- La fecha relevante para la auditoría controla todas las auditorías siguientes (Auditoría de Seguimiento y recertificación).
- Cada Auditoría de Seguimiento, incluida la revisión y aceptación y verificación, si corresponde, de las medidas para corregir las no conformidades, la redacción del informe de auditoría y la publicación por parte del organismo de certificación, debe completarse a más tardar 2 meses después de la fecha relevante para la auditoría.
- En el marco de la vigilancia anual, una Auditoría de Seguimiento puede llevarse a cabo lo antes posible 3 meses antes de la fecha relevante para la auditoría.

La tolerancia permisible para realizar auditorías de las Auditorías de Seguimiento: último día de auditoría de Fase II -3 / +0 meses.

3.- Auditorías de Recertificación

Las auditorías de recertificación deben estar completas antes del final del período de validez del certificado, incluida la revisión de las medidas para la corrección de no conformidades.
En la auditoría de recertificación, se lleva a cabo una revisión de la documentación del sistema de gestión de la organización y se lleva a cabo una auditoría in situ, por lo que se deben tener en cuenta los resultados de los programas de seguimiento anteriores durante el período de certificación. Todos los requisitos de la norma son auditados.
Las actividades relacionadas con la auditoría de recertificación pueden incluir una auditoría de la fase I si hay cambios significativos en el sistema de gestión o en relación con las actividades de la organización (por ejemplo, cambios a la ley).

Los métodos de auditoría utilizados en la auditoría de recertificación corresponden a los utilizados en una auditoría de la fase II.

La tolerancia permisible para realizar auditorías de las Auditorías de Renovación: 3 meses antes de la caducidad del certificado.

4.- Auditoría de Extensión

Si se pretende ampliar el alcance de un certificado existente, esto puede implementarse mediante una auditoría de extensión. Una auditoría de extensión se puede realizar en el marco de una auditoría de seguimiento, una auditoría de recertificación o en un momento que se establece de forma independiente.

El período de validez de un certificado no cambia como resultado. Las excepciones deben justificarse por escrito.

5.- Transferencia de certificados de otros organismos de certificación

En general, solo los certificados de organismos de certificación acreditados pueden ser transferidos. Las organizaciones con certificados que se originan en organismos de certificación no acreditados se tratan como nuevos clientes.

Una persona competente del organismo de certificación se hace cargo en realizar una "Revisión previa a la transferencia". Esta revisión generalmente consiste en un examen de documentos importantes y una visita al cliente.

Los certificados que han sido suspendidos, o donde existe riesgo de suspensión, no pueden ser aceptados. Cualquier no conformidad que no haya sido corregida debe, en la medida de lo posible, aclararse con el Certificador anterior antes de la adquisición. De lo contrario, deben ser tratados en la auditoría.

El programa de seguimiento adicional se basa en el programa que se ha implementado hasta el momento de la adquisición del certificado.

6.- Certificación de organizaciones multi-emplazamiento

Si una organización que tiene varios sitios certificados, estos sitios también deben ser auditados. Por medio de un procedimiento de muestreo aleatorio, la certificación de organizaciones con varios sitios de producción / sucursales / ubicaciones, etc. con actividades similares y que operan bajo un único sistema de gestión.

7.- Gestión de no conformidades

Se debe realizar un análisis de las causas para cada no conformidad y se deben implementar las acciones correctivas correspondientes. La organización tiene el deber, dependiendo de la gravedad de la no conformidad, de informar al equipo de auditoría dentro de los 90 días, ya sea con respecto a las acciones correctivas que se han establecido y las fechas para su implementación o que se han implementado las acciones correctivas. Si no se observa este período, se considera que la auditoría no tiene éxito, es decir, no se pasa. No se puede emitir ningún certificado, o se retira un certificado existente.