ISO 27001 INTERNAL AUDITOR/LEAD AUDITOR (I27001IA/LA)

ISO 27001 INTERNAL AUDITOR
I27001IA

ISO 27001 LEAD AUDITOR
I27001LA

CertiProf®
Professional Knowledge

www.certiprof.com

(I27001IA/LA) VERSIÓN 092020

ISO 27001 Internal Auditor/Lead Auditor (I27001IA/LA)

Syllabus V092020

Introducción

Esta certificación está diseñada para evaluar conocimientos a nivel de auditor acerca del sistema de gestión de seguridad de la información (SDSI) y su aplicación en las organizaciones.

El entrenamiento constará de exposiciones de temas con uso de diapositivas y ejemplos de experiencia del facilitador. Se espera que los estudiantes durante el entrenamiento conozcan las prácticas para la implementación y gestión de un SDSI, así como la preparación como auditor.

Es altamente recomendable trabajar con la norma de traducción oficial de cada país.

Objetivos

- Entender y analizar la Norma ISO 27001 (Interpretación de Requisitos).
- Conocer hechos, términos y conceptos sobre la visión general, el alcance, los esquemas y lograr la certificación ISO/IEC 27001.
- Conocer hechos, términos y conceptos relacionados con los requisitos generales del sistema de gestión de seguridad de la información (SDSI) en ISO/IEC 27001.
- Identificación de mejoras posibles al SDSI.
- Desarrollar la capacidad de auditar los procesos de los requisitos de ISO/IEC 27001.

Formato y duración del examen

Este programa de estudios tiene un examen en el cual el candidato debe lograr alcanzar una puntuación para obtener la certificación de auditor en ISO/IEC 27001.

- Tipo: Opción múltiple, 40 Preguntas.
- Duración: Máximo 60 minutos para todos los candidatos en su respectivo lenguaje.
- Prerrequisito: Ninguno.
- Supervisado: Bajo requerimiento.
- Libro abierto: No.
- Puntaje de aprobación: 24/40 o 60 %.
- Entrega: Este examen está disponible en línea.

Elegibilidad para certificación

Presidentes de TI, Jefes Ejecutivos, Auditores de TI/IS, Auditores, Profesionales en Seguridad de la Información y de TI, Consultores, Gerentes de TI/IS, Profesionales o Estudiantes de Ingenierías afines a la gestión de servicios de TI.

La sección para obtener el Certificado de Auditor Líder es un examen complementario con libro abierto, diseñado para permitir a los estudiantes demostrar su comprensión del proceso de auditoría y las responsabilidades de ser un auditor líder.

Contenido

Introducción y Antecedentes
- Historia de la Norma
- ISO/IEC 27001:2013 – Estructura
- ISO 27000 Familia de Normas

Conceptos Claves
- Información y Principios Generales
- La Seguridad de la Información
- El Sistema de Gestión
- Factores Críticos de Éxito de una SGSI
- Beneficios de la Familia de Normas SGSI

Términos y Definiciones
- Control de Acceso
- Modelo Analítico
- Ataque
- Atributo
- Auditoría
- Alcance de la Auditoría
- Autenticación
- Autenticidad
- Disponibilidad
- Medida Básica
- Competencia
- Confidencialidad
- Conformidad
- Consecuencia
- Mejora Continua
- Control
- Objetivo de Control
- Corrección
- Acción Correctiva
- Datos
- Criterios de Decisión
- Medida Derivada
- Información Documentada
- Eficacia
- Evento
- Dirección Ejecutiva

Contexto Externo
Gobernanza de la Seguridad de la Información
Órgano de Gobierno
Indicador
Necesidades de Información
Recursos (instalaciones) de Tratamiento de Información
Seguridad de la Información
Continuidad de la Seguridad de la Información
Evento o Suceso de Seguridad de la Información
Incidente de Seguridad de la Información
Gestión de Incidentes de Seguridad de la Información
Colectivo que Comparte Información
Sistema de Información
Integridad
Parte Interesada
Contexto Interno
Proyecto del SGSI
Nivel de Riesgo
Probabilidad (likehood)
Sistema de Gestión
Medida
Medición
Función de Medición
Método de Medición
Resultados de las Mediciones
Supervisión, Seguimiento o Monitorización (monitoring)
No Conformidad
No Repudio
Objeto
Objetivo
Organización
Contratar Externamente (verbo)
Desempeño
Política
Proceso
Fiabilidad
Requisito
Riesgo Residual
Revisión
Objeto en Revisión
Objetivo de la Revisión
Riesgo
Aceptación del Riesgo
Análisis del Riesgo

- Apreciación del Riesgo
- Comunicación y Consulta del Riesgo
- Criterios de Riesgo
- Evaluación del Riesgo
- Identificación del Riesgo
- Gestión del Riesgo
- Proceso de Gestión del riesgo
- Dueño del Riesgo
- Tratamiento del Riesgo
- Escala
- Norma de Implementación de la Seguridad
- Parte Interesada
- Amenaza
- Alta Dirección
- Entidad de Confianza para la Comunicación de la Información
- Unidad de Medida
- Validación
- Verificación
- Vulnerabilidad

Contexto de la Organización

- Comprensión de la Organización y de su Contexto
- Comprensión de las Necesidades y Expectativas de las Partes Interesadas
- Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información
- Sistema de Gestión de la Seguridad de la Información

Liderazgo

- Liderazgo y Compromiso
- Política
- Roles, Responsabilidades y Autoridades en la Organización

Planificación

- Acciones para Tratar los Riesgos y Oportunidades
- Objetivos de Seguridad de la Información y Planificación para su Consecución

Soporte

- Recursos
- Competencia
- Concienciación
- Comunicación
- Información Documentada

Operación

- Planificación y Control Operacional
- Apreciación de los Riesgos de Seguridad de la Información
- Tratamiento de los Riesgos de Seguridad de la Información

Evaluación del Desempeño

- Seguimiento, Medición, Análisis y Evaluación
- Auditoría Interna

Revisión por la Dirección

Mejora

No Conformidad y Acciones Correctivas
Mejora Continua

Auditoría

Auditor
Términos y Definiciones ISO 19011:2011
Tipos
Criterios de Auditoría
Evidencia de la Auditoría
Hallazgos de la Auditoría
Conclusiones de la Auditoría
Cliente de la Auditoría
Auditado
Auditor
Equipo Auditor
Experto Técnico
Observador
Guía
Programa de Auditoría
Alcance de la Auditoría
Plan de Auditoría
Riesgo
Competencia
Conformidad
No Conformidad
Sistema de Gestión

Taller

Programa de Auditoría
Principios de Auditoría
Atributos de los Auditores
Auditoría y Evidencia
Reunión de Apertura

Taller

Establecer un Programa de Auditoría
Competencias de los Auditores
Métodos de Auditoría Aplicables
Objetivos de la Auditoría Interna
Auditoría Interna Evidencia Objetiva
Actividades de Auditoría
Preparación de las Actividades Auditoría en Sitio
Responsabilidades del Auditor Líder
Responsabilidades del Co-Auditor

Taller

- Preparación Individual del Auditor
- Plan de Auditoría
- Listas de Chequeo o Verificación
- Preguntas Claves del Auditor
- Tipo de Preguntas
- Recolección de Evidencia Objetiva
- Ejecutando la Auditoría
- Fuentes de Información
- Realización de Entrevistas
- Técnicas de Entrevista del Auditor
- Actitudes a Tomar para Controlar la Auditoría
- ¿Cómo entorpecer la Auditoría (Auditado)?
- Administración del Tiempo
- Manejo de Situaciones Difíciles
- Resultados de la Auditoría
- Tipos de Hallazgos
- Incumplimientos más Comunes

Taller

- La Reunión de Cierre
- Dirigida por el Auditor Líder
- Informe de Auditoría
- ¿Qué no incluir en el informe de auditoría?
- Plantilla de Informe
- Acciones Correctivas
- Las Auditorías de Seguimiento
- Redacción de las No Conformidades
- Fórmula de Redacción de No Conformidades
- Fases de la Auditoría

Conclusiones