Formulario de Verificación de Experiencia para CRISC

Solicitantes que aprobaron el examen CRISC de 2015 y posteriores

Por favor use Adobe Reader cuando cumplimente esta solicitud electrónicamente.

DETALLES DEL SOLICITANTE

NOMBRE DEL SOLICITANTE: _____ N°. DE ID DE ISACA: _____

INSTRUCCIONES DEL FORMULARIO PARA EL VERIFICADOR

El solicitante (mencionado arriba) realiza la solicitud de la certificación CRISC a través de ISACA. ISACA requiere que la experiencia laboral del solicitante sea verificada de forma independiente por parte de un supervisor o gerente con quien haya trabajado. Los verificadores no pueden ser familia inmediata o lejana, ni pueden trabajar en el Departamento de Recursos Humanos.

Al completar el formulario, usted avala la experiencia laboral del solicitante, tal como éste declara en su solicitud adjunta (página A-1), en conformidad con las áreas de dominio de práctica laboral de CRISC y sus declaraciones de tareas (página V-2).

Por favor, devuelva el presente formulario de verificación al solicitante, para su remisión a ISACA por parte de éste. Si tiene alguna pregunta, comuníquese con ISACA en https://support.isaca.org o +1.847.660.5505.

INFORMACIÓN SOBRE EL VERIFICADOR

NOMBRE DEL VERIFICADOR: _____

NOMBRE DE LA EMPRESA: _____ CARGO: _____

CORREO ELECTRÓNICO: _____ N°. DE TELÉFONO: _____

PREGUNTAS DEL VERIFICADOR

1. Avalo la siguiente experiencia laboral obtenida por el solicitante, como se indica en la página A-1 (*marque todas las opciones que correspondan*):

☐ Sección A: Empresa 1 ☐ Sección A: Empresa 3

☐ Sección A: Empresa 2 ☐ Sección A: Empresa 4

2. He desempeñado las siguientes funciones en relación con el solicitante:

☐ Supervisor ☐ Gerente ☐ Colega ☐ Cliente

3. Avalo también que las tareas realizadas por el aspirante, según lo declarado en la página V-2 de este formulario, son correctas a mi leal saber y entender.

☐ Sí ☐ No

ACUERDO DEL VERIFICADOR:

Por la presente confirmo que la información en la página V-1 y V-2 es correcta a mi leal saber y entender y no hay razón para que este solicitante no esté certificado en Control de Riesgos y Sistemas de Información. También estoy dispuesto a responder preguntas de ISACA sobre la información proporcionada, en caso de ser requerido a ello.

FIRMA DEL VERIFICADOR: _____ FECHA: _____

Formulario de Verificación de Experiencia para CRISC

Solicitantes que aprobaron el examen CRISC de 2015 y posteriores

Por favor use Adobe Reader cuando cumplimente esta solicitud electrónicamente.

INSTRUCCIONES PARA EL DOMINIO DE PRÁCTICA LABORAL

Es obligatorio que el solicitante marque todos los dominios en los que ha completado tareas, a confirmar por parte del verificador.

☐ DOMINIO 1 - Identificación de riesgos de TI

Identificar el universo de riesgos de TI para contribuir a la ejecución de la estrategia de gestión de riesgos de TI y respaldar los objetivos de negocio y mantenerse alineado con la estrategia de gestión de riesgo empresarial (ERM).

Declaraciones de tareas:

- Recopilar y revisar información, incluyendo la documentación existente sobre los entornos de TI y los negocios internos y externos de la organización para identificar los impactos potenciales de los riesgos de TI en los objetivos y las operaciones de la organización.
- Identifique amenazas y vulnerabilidades potenciales relativas al personal, los procesos y la tecnología de la organización para permitir el análisis de riesgo de TI.
- Desarrollar un conjunto integral de escenarios de riesgo de TI con base en la información disponible para determinar el impacto potencial a las operaciones y los objetivos del negocio.
- Identificar a las partes interesadas clave en los escenarios de riesgo de TI para ayudar a establecer las responsabilidades.
- Establecer un registro de riesgo de TI para ayudar a garantizar que los escenarios de riesgo de TI identificados se tengan en cuenta y se incorporen al perfil de riesgo de toda la organización.
- Identificar el apetito y la tolerancia al riesgo definidos por la alta Dirección y las partes interesadas claves para garantizar la alineación con los objetivos de negocio.
- Colaborar en el desarrollo del programa de concienciación de riesgos y llevar a cabo capacitaciones con el fin de garantizar que las partes interesadas comprendan los riesgos y fomenten una cultura de conciencia de riesgos.

☐ DOMINIO 2 - Evaluación de riesgos de TI

Analizar y evaluar los riesgos de TI para determinar la probabilidad y el impacto en los objetivos de negocio para que se tomen decisiones basadas en el riesgo.

Declaraciones de tareas:

- Analizar los escenarios de riesgo de acuerdo con los criterios organizacionales (p. ej., estructura organizacional, políticas, estándares, tecnología, arquitectura, controles) para determinar la probabilidad y el impacto de un riesgo identificado.
- Identificar el estado actual de los controles existentes y evaluar su eficacia para la mitigación de riesgos de TI.
- Revisar los resultados del análisis de riesgo y controles para evaluar las brechas que existan entre los estados actual y deseado del entorno de riesgo de TI.
- Garantizar que se asigne la propiedad de riesgos en el nivel correspondiente para establecer líneas claras de responsabilidad.
- Comunicar los resultados de evaluaciones de riesgo a la alta gerencia y a las partes interesadas correspondientes para permitir la toma de decisiones en función de los riesgos.
- Actualizar el registro de riesgos con los resultados de la evaluación del riesgo.

☐ DOMINIO 3 - Mitigación y respuesta al riesgo

Determinar las opciones de respuesta al riesgo, y evaluar su eficiencia y eficacia al momento de gestionar el riesgo de manera alineada con los objetivos del negocio.

Declaraciones de tareas:

- Consultar con los propietarios del riesgo para seleccionar y alinear las respuestas ante riesgos recomendadas con los objetivos del negocio y permitir decisiones informadas sobre el riesgo.
- Consultar con los propietarios del riesgo, o asistirlos, al momento del desarrollo de planes de acción ante riesgos para garantizar que los planes incluyan elementos clave (por ejemplo, respuesta, coste, fecha prevista).
- Consultar sobre el diseño y la implementación de ajustes de los controles de mitigación para garantizar que el riesgo se gestione a un nivel aceptable.
- Garantizar que la propiedad del control es asignada para establecer líneas claras de responsabilidad.
- Asistir a los propietarios de control para desarrollar documentación y procedimientos de desarrollo de controles, a fin de permitir la ejecución eficaz y efectiva del control.
- Actualizar el registro de riesgos a fin de reflejar los cambios en el riesgo y la correspondiente respuesta por parte de la gerencia.
- Validar que las respuestas al riesgo se hayan ejecutado de acuerdo con los planes de acción ante riesgos.

☐ DOMINIO 4 - Monitoreo y Reporte de Riesgos y Controles

Monitorear continuamente el riesgo y los controles de TI, e informar sobre estos a las partes interesadas pertinentes para garantizar la eficiencia y la eficacia constantes de la estrategia de gestión del riesgo de TI y su adecuación a los objetivos de negocio.

Declaraciones de tareas:

- Definir y establecer indicadores clave de riesgo (KRI) y umbrales sobre la base de los datos disponibles para permitir el monitoreo de los cambios en los riesgos.
- Monitorear y analizar los indicadores clave de riesgo (KRI) para identificar cambios o tendencias en el perfil de riesgos de TI.
- Informar sobre cambios o tendencias relacionadas con el perfil de riesgos de TI para asistir a la gerencia y a las partes interesadas pertinentes en la toma de decisiones.
- Facilitar la identificación de métricas y de indicadores clave de desempeño (KPI) que permitan medir el desempeño de los controles.
- Monitorear y analizar los indicadores clave de desempeño (KPI) para identificar cambios o tendencias relacionadas con el ambiente de control y determinar la eficiencia y la eficacia de los controles.
- Revisar los resultados de evaluación de control para determinar la eficacia del ambiente de control.
- Informar sobre el desempeño o los cambios o tendencias en el perfil de riesgo general y el ambiente de control para partes interesadas pertinentes que permitan la toma de decisiones.