Escenario

Este escenario se basa en una empresa ficticia: Botium Toys es una pequeña empresa estadounidense que desarrolla y vende juguetes. La empresa tiene una sola sede física. Sin embargo, su presencia en línea ha crecido, atrayendo a clientes de Estados Unidos y del extranjero. Su departamento de tecnología de la información (TI) está sometido a una presión cada vez mayor para dar soporte a su mercado en línea en todo el mundo. La gerente del departamento de TI ha decidido que es necesario realizar una auditoría interna de TI. Expresa su preocupación por no tener un plan de acción consolidado para garantizar la continuidad del negocio y el cumplimiento de la normativa, a medida que la empresa crece.Cree que una auditoría interna puede ayudar a asegurar mejor la infraestructura de la empresa y ayudar a identificar y mitigar los posibles riesgos, amenazas o vulnerabilidades de los activos críticos.

La gerente también está interesada en asegurarse de que cumplen con la normativa relacionada con la aceptación de pagos en línea y la realización de negocios en la Unión Europea (UE). La gerente de TI comienza aplicando el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST), estableciendo un alcance y unos objetivos de auditoría y completando una evaluación de riesgos. El objetivo de la auditoría es proporcionar una visión general de los riesgos que la empresa podría experimentar debido al estado actual de su postura de seguridad. La gerente de TI quiere utilizar los resultados de la auditoría como prueba para obtener la aprobación para ampliar su departamento.

Tu tarea consiste en revisar el alcance, los objetivos y la evaluación de riesgos de la gerente de TI. Luego, realiza una auditoría interna para completar una evaluación de los controles y una lista de verificación de cumplimiento.