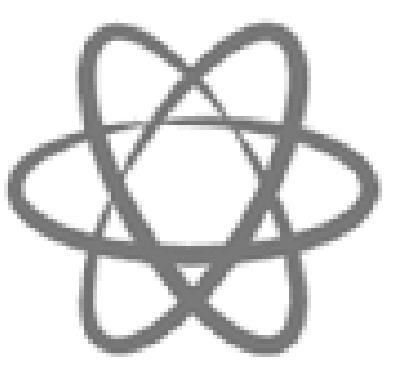




RESEARCH  
SCHOLARS  
PROGRAM



# Business Information Security Officer (BISO) Responsibilities and Role Development



## Authors

Kaung Myat Thu and Hudda Siddique

Mentor: Professor Patrick Slattery (CST)

Department of Computer systems technology (CST)

## Abstract

As technology develops in the 21st century, everything is connected through a network. Enterprises are highly dependent on that network connectivity to develop and succeed. The Information security role has become critical to protect sensitive information from threats such as cyber-attack, and other information incidents to ensure the success of the business. We cannot rely on technology every time because one mistake could compromise the organization's reputation, financial impact and value. This research project is to study the Business Information Security Officer (BISO) role: its responsibility, strategy, and how BISOs handle threats. We will look at what knowledge a BISO should have and what skills required to be a BISO. BISOs need to have a combination of technical and business knowledge to maintain and improve information security in important aspects of a business. Whether a BISO needs to have an ISC<sup>2</sup> CISSP (Information Systems Security Professional), ISACA CRISC (Information Technology Risk Management), CISM (Information Security Management) or other certifications will be explored. In addition an understanding of risk management, and CompTIA Security+ qualifications will be studied. The role of a BISO is new and evolving – this study aims to contribute to the maturity of the role.



## Introduction

Business Information Security Officer (BISO) is the senior information security officer (CISO) who is in charge of all services and core platforms; accountable for prioritizing security risks across business units (BUs), technology, and serving as the CISO's representative in local security issues. Some of BISO responsibility are creating and sustaining a program for business information security including standards, guidelines and regulations directing the regulations directing the reaction to an incident involving a security breach or other occurrence.

## What are BISO responsibilities?

The BISO is one of the few roles that supports the priorities of both the business and the information security function. That's why organizations need BISOs to align business and information security priorities. They support both the core security function and help business units improve the cybersecurity program's maturity by encouraging collaboration, ensuring relevance and driving results.



## What value do BISOs provide?

- Developing and maintaining the business such as technologies, customers, partners, alliances, systems, processes, consumers, data, and customers.
- Offer guidance for cybersecurity across regions and functions.
- Implementation of the information security policies and procedures across all assigned regions or units.
- Participating in company/region related meetings and conferences and industry forums associated as part of the cybersecurity program.
- Offer reporting on a regular basis on cybersecurity status across the company/region/unit of responsibility.
- Act as the main contact for inquiries, security issues, and security issues.
- Coordinate with Crisis Management and Security Incident Response teams to help resolutions for incidents and assist with investigations.
- Work with the Information Risk Management and Compliance team for policy development and regulatory compliance.

## What knowledge do BISOs need ?

BISO has the combination of technical and business knowledge to improve information security in all aspects of a business. They understand the processes, identify and evaluate controls and risks, and suggest controls and risk management strategies so that the company is complying with Information Security Policies and Standards.

The BISO's responsibilities has a variety of tasks and include supporting core security functions with the following:

- **Risk management:** This includes risk identification, risk acceptance, solution development and risk mitigation implementation support.
- **Education:** This includes educating business and functional leaders on operationalization of policies, standards and baselines.
- **Collaboration:** This includes collaborating on key security tasks, such as incident management, threat modeling, vulnerability management, third party assessments, etc.

## How do you become a BISO?

One of the most common ways to become a BISO is through a mix of information science and business management study. This includes degrees in information technology management, cybersecurity policy and management, and business administration with an information security focus.

## Required certifications to be BISO :

- (ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP) demonstrates a broad understanding of existing and emerging cybersecurity threats and how to prevent them from impacting an organization.
- ISACA CRISC and CISM certifications validate a strong understanding of risk management and skills in assessing and overseeing an enterprise's information security.
- CompTIA Security+ validates baseline skills required to perform core security functions and pursue a career in information security.



## Citations

- Written by Larisa Redins - Published: April 11. "Business Information Security Officer: A Complete Career Guide." Cybersecurity Guide. 11 Apr. 2022. [cybersecurityguide.org/careers/business-information-security-officer/](https://cybersecurityguide.org/careers/business-information-security-officer/).
- Soto, Myrna, et al. "How Bisos Bridge the Gap between Corporate Boards and Cybersecurity." SC Media, 23 June 2022. <https://www.scmagazine.com/news/content/how-bisos-bridge-the-gap-between-corporate-boards-and-cybersecurity>.
- "Business Information Security Officer (BISO) - Health Services." ClearedJobs.Net. <https://clearedjobs.net/job/business-information-security-officer-biso-health-services-orlando-florida-446206>.
- 14, October, et al. "What Does a Business Information Security Officer Do?" Infosec Resources, 8 Oct. 2021. <https://resources.infosecinstitute.com/topic/what-does-a-business-information-security-officer-do/>.

