Structuring a BISO Role for Success

Responsibilities, Organizational Approaches, and Performance Indicators for Business Information Security Officers

© 2025 FS-ISAC, Inc. | All rights reserved

Contributors

Aaron Kirby, Senior Vice President, Security Business Solutions, Mastercard

Alok Nigam, Director, Technology Risk & Cybersecurity, American Express

Amit Khosla, Business Information Security Officer, Fannie Mae

Ann Hines, Business Information Security Officer, USAA

Barbara Verde, Business Security Advisory, Ahold Delhaize Group

Carlos Gonzalez, Business Information Security Officer, Wells Fargo

Chiheb El Ouekdi, Business Information Security Officer, Industrielle Alliance, Assurance et services financiers

Carly Miller, Business Unit Risk Lead Vice President, Comerica

Donald Schmidt, Business Information Security Officer, Fannie Mae

Ian McNiff, Business Information Security Officer, Lowes

Irina Singh, Business Information Security Officer, Baxter International Inc.

Jackie Deloplaine, Manager – Cyber Intelligence Engagement, RH-ISAC

Jocelyn Anderson, Assistant Vice President, Information Security, HarborOne Bank

John Mracek, Business Information Security Officer, Target

Joseph Millevolte, Business Information Security Officer, BNP Paribas

Michael Leking, former Business Information Security Officer, U.S. Bank

Nicholas Kelley-Ossey, Business Information Security Officer, The Travelers Companies

Owen Barton, Business Information Security Officer, The Vanguard Group

Patricia DiGiacomo, Sr. Director, Global Business Information Security Office, Kenvue

Renee Kimble, Business Information Security Officer, Toyota

Ryan Bowling, Business Information Security Officer, Lowes

Segun Yayi, former Business Information Security Officer

Seido Afia, Business Security and Risk Analyst Lead, Comerica

Vishwas Gadgil, Business Information Security Officer, Merck

Michael Petrik, Community of Interest Manager, FS-ISAC

© 2025 FS-ISAC, Inc. | All rights reserved |

Contents

Contributors 1
Executive Summary 3
Role Responsibilities 4
BISO Alignment Model 6
Titles Used for the BISO 7
Structure of the BISO Role 8
BISO Reporting Structure 9
Key Challenges and Solutions 10
Assessing the Success of a BISO Program/Role 12
How to Measure Success 13
Cultural Support for BISO Programs 15

This white paper and its companion documents, The Business Information Security Officer: An Overview; Actionable Advice from Practitioners in Four Industries and *Mapping the BISO Career: The Development of an Effective Business Information Security Officer, offer insight into the role design, value proposition, organization, responsibilities, and challenges of the Business Information Security Officer role.*

This series was written collaboratively by members of the Financial Services, Health, and Retail and Hospitality Information Sharing and Analysis Centers, all of them leaders and expert practitioners.

The partnership across companies and industries demonstrates the value of collaboration on cyber defense. Threats cross departments, industries, and borders. Strengthening one sector's cybersecurity and resilience ultimately strengthens all of them.

© 2025 FS-ISAC, Inc. | All rights reserved |

Executive Summary

From large multinational corporations to smaller, more local firms, the Business Information Security Officer (BISO) role is becoming increasingly common in multiple industries.

The BISO is a liaison between business and cybersecurity, ensuring the security of the enterprise's information and technology assets, building trust between business, technology, and cybersecurity teams, and translating business requirements and cyber risks to various functions.

While the role of BISO has become familiar in many organizations' cybersecurity programs, the structure of the BISO function varies. To some extent, the lack of standardization reflects the differing needs of companies and industries, but **a common understanding of the role would help businesses better implement BISO programs, determine the scope of the role, and evaluate success in it.**

To that end, experts in over a dozen companies in four industries developed this series of three papers. The documents **detail the BISO function, define its responsibilities and evaluation criteria, and provide considerations** for companies navigating a changing business and regulatory environment.

This is the second white paper in the series. Written for executives, leaders, and cybersecurity professionals, it examines:

- The responsibilities of the role and areas of BISOs' particular focus
- Approaches to organizational alignment and role structure
- Obstacles to success in the role
- Guidance on performance measurement
- The cultural attributes that support BISO performance

Though companies should mold the role according to their sector, business needs, and risk appetite, aspects of the BISO role are universal: **all BISOs must understand the cyber risks their business faces, translate those risks to leaders and teams, and implement risk management strategies that work.** The experience of experts can help companies achieve those aims – and maximize the benefit of this vital function.

© 2025 FS-ISAC, Inc. | All rights reserved |

The Business Information Security Officer: An Overview; Actionable Advice from Practitioners in Four Industries for a high-level look at the role, and *Mapping the BISO Career: The Development of an Effective Business Information Security Officer* to learn more about the qualities of effective BISOs.

The Responsibilities of a BISO

BISOs' specific areas of focus may differ between organizations in some regards, but the BISO's agenda is fundamentally the same across institutions and industries: steering the organization's information security agenda, fostering collaboration between business units and IT departments, ensuring compliance with regulatory requirements, and helping the business manage risks.

Therefore, the BISO's remit typically includes:

- **Mitigating cybersecurity threats.** BISOs must stay informed of evolving cybersecurity threats and the threat landscape as it relates to their business sector. In addition to ensuring that these threats are properly mitigated by the cybersecurity teams, BISOs identify and facilitate the resolution, where practicable, of issues or areas that suffer control weaknesses.
- **Ensuring information security.** By definition, BISOs are responsible for the breadth of information security domains. They are accountable for providing consultation and/or oversight on controls, determining exemptions to controls or standards, and reviewing loss information to prevent incidents in the future.

When cybersecurity processes and/or technology changes are created with BISO involvement, the changes are more likely to align with business processes and experiences, reduce delays to adoption, and have a postive impact on the business and customers.

- **Maintaining regulatory compliance.** Many BISOs collaborate with legal counsel to ensure that the organization's cybersecurity program complies with various industry-specific regulations and data protection laws, such as the New York Department of Financial Services Part 500 (PCI-DSS, NYDFS), the Health Insurance Portability and Accountability Act (HIPAA), the Office of the

© 2025 FS-ISAC, Inc. | All rights reserved |

Comptroller of the Currency Gramm-Leach-Bliley Act Appendix B (OCC GLBA), the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and more. BISOs must stay abreast of changing regulations, ensure the implementation of necessary controls to maintain compliance, and collaborate with organizational compliance teams.

- **Partnering on security training.** BISOs often partner with training and awareness staff to help educate employees about effective security practices and potential threats. Some BISOs conduct regular training sessions to ensure that employees understand their roles and responsibilities in maintaining information security.

- **Managing third-party risk.** Many organizations work with external vendors, partners, or suppliers that have access to the institution's sensitive data or systems. BISOs support business and cybersecurity teams — and third-party risk management teams, in organizations that have them — in the assessment and management of risks associated with third-party relationships, helping ensure that these partners maintain a high level of security to protect shared information.

- **Analyzing emerging technologies.** BISOs must understand emerging technologies to forecast security implications and support the development of strategies to mitigate associated risks. In many cases, BISOs help the organization prepare for and capitalize on emerging technologies and regulations around them.

- **Establishing cybersecurity strategies and priorities.** BISOs are in a unique position to influence how cybersecurity is aligned to a business' critical processes. Their collaboration can help technology implementations align with business strategy and risk appetite.

- **Communication and relationship building.** The BISO acts as a trusted advisor to both the business and cybersecurity leadership, often as a single point of contact for cybersecurity communication across lines of business. By leveraging those relationships, BISOs can articulate cyber issues and their impact on the business. While BISOs cannot be involved in every security decision, change, or proposed Gramm-Leach-Bliley Act Appendix B initiative, BISOs partner with cybersecurity leaders to convey information in a timely manner for business response and adoption.

© 2025 FS-ISAC, Inc. | All rights reserved |

BISO Alignment Model

The specific alignment and reporting structure of a BISO program depends on the institution's size, industry, culture, and the risk that the BISO is tasked to address.

The number of BISOs in a business is a factor of its size and complexity. A smaller company may employ only one BISO, while bigger organizations, those with operations in many geographies, or those with stringent compliance requirements — such as healthcare or financial services — may have several BISOs, each assigned to a different business unit.

In the latter hierarchy, close alignment to the team that the BISO supports is foundational to the BISO's success. That alignment can relate to one or a combination of the following:

- Functional (i.e., consumer banking, HR, consumer retail, IT, manufacturing, corporate, investments, insurance, payments, etc.)
    - In organizations with multiple business functions, BISOs may be aligned with specific functions rather than business units. In such structures, the BISO is responsible for providing cybersecurity subject matter expertise and risk evaluation within their respective functional areas.
- Geographic
    - In global enterprises with a multinational presence, BISOs may be aligned geographically. These BISOs are "local specialists" responsible for ensuring cybersecurity compliance and conventions within specific areas, according to local regulations and risks.
- Technical
    - Some BISOs are aligned to products (i.e., cloud, merger and acquisition assessments, computer network, application development, etc.). These BISOs have an in-depth understanding of the product or specialize in a technical competency and liaise with business-aligned BISOs to drive the right solutions for the business.
- Hybrid models
    - Many organizations combine elements of the above structures to best fit their needs. In these hybrid arrangements, BISOs may have a functional or technical alignment but still report to the Chief Information Security Officer (CISO) for

© 2025 FS-ISAC, Inc. | All rights reserved |

overarching security strategy and coordination. This often requires the BISO to have a wide range of security expertise rather than expertise in any one security or domain. Nonetheless, BISOs in hybrid models must understand how to best bridge cyber policy, align other cyber subject matter experts, and provide high-level architecture support to direct their internal partners to the best security outcome.

Ultimately, the alignment of BISOs in an enterprise should strike a balance between providing specialized security expertise and ensuring that security measures are closely aligned with the business's overall objectives and success.

The Use of *Officer* in the BISO Title

The term *officer* in the title "Business Information Security Officer" carries significant weight and connotes the role's seniority, decision-making authority, responsibility, and alignment with organizational governance. The use of *officer* emphasizes that the BISO position is not merely a technical or advisory one but a leadership role that integrates business strategy with cybersecurity principles.

BISOs Are Not Project Managers

While a project management skillset helps BISOs succeed in the role, BISOs are not project or program managers for cybersecurity or other teams. BISOs can conduct oversight over projects and programs, and provide portfolio oversight at a strategic level, but project management is not a dedicated function of the role. There may be times when there is a gap and the BISO must assume duties as a project manager, but this should be a temporary task.

The title also aligns the role with other high-ranking positions such as Chief Information Officer (CIO) or CISO. Though BISO roles are not necessarily equivalent to those roles in organizational hierarchies – many BISOs report to CISOs or CIOs – the use of *officer* signals the BISO's strategic importance with a level of autonomy and accountability akin to these other leadership roles. Moreover, the term *officer* underscores the BISO's role in managing risk at an enterprise level, making it clear to stakeholders that the position is central to protecting critical business information assets.

However, some organizations choose not to use the term *officer* in such titles, often due to concerns about hierarchy, perception, regulatory implications, or internal culture. In highly structured organizations, *officer* may be reserved for only the most senior executive roles, such as those reporting directly to the Board. In such cases, using *officer* for roles that may be perceived as middle management could dilute the word's

© 2025 FS-ISAC, Inc. | All rights reserved |

significance and authority, its clear association with cybersecurity and information security, or create internal tensions. Additionally, in regulated industries, *officer* could imply legal or fiduciary responsibilities, which executives might choose to avoid to limit liability or clarify the scope of the position.

The functional and corporate titles of the BISO role are influenced by areas of focus, reporting structure, business alignment (i.e. regional BISO or segmentation of BISO), responsibilities, and the organization's title conventions. Some organizations may prefer alternative titles to reflect a more collaborative or less formal approach to security leadership. Titles like "Business Information Security Manager" or "Cybersecurity Liaison" may emphasize partnership and integration over hierarchy, aligning with corporate cultures that prioritize inclusivity and teamwork over rigid structures.

Ultimately, the decision to use *officer* depends on how the organization balances these cultural, hierarchical, and regulatory considerations with the need to communicate the strategic importance of the role. Whatever the title, the responsibilities should be clearly defined to clarify that the role is equivalent to a BISO.

Structure of the BISO Role

The ideal structure for a BISO role depends on the firm's business, market, organizational structure, regulatory environment, and risk appetite. The structure should:

- Be tailored to the organization's unique needs, risk profile, and culture
- Manage cybersecurity risks effectively
- Provide a "check and balance" to the CIO

This can be done by building hard approval requirements into policy language. The goal is not to slow the business down, but to ensure cybersecurity is built into technology and\or business objectives.

Regardless of the total number of BISOs in the company — and there may be several levels of BISO within the same organization – the BISO is the chief cybersecurity and cyber risk advisor to the business, so logically reports directly to the CISO, the CIO/Chief Executive Officer (CEO), or both, dotted-lined to their business leader.

That approach enables BISOs to be part of the leadership team of the business unit and cyber operations, and ensures better alignment with enterprise-wide security strategies.

© 2025 FS-ISAC, Inc. | All rights reserved |

Ideally, the BISO is viewed as a "mini CISO," with the autonomy to act within the bounds of the approved cybersecurity policy and standards.

BISOs Aren't Technology Owners

The BISO should be independent – not a technology owner – so they can provide accurate risk-based advice to the business without conflict of interest.

If the BISO is aligned with a business or division — depending on the breadth and scope of the alignment — the BISO may require a staff or a federated security team (i.e., information security analysts or business\divisional employees with separate managers). That team could either report directly to the BISO or be matrixed to the BISO for operational execution. The composition of the BISO's support team depends greatly on the BISO's responsibilities, accountabilities, and goals. A strong data analytics role on the team is typical, however, as the BISO program's success depends on accurate reports of cybersecurity risk and activities.

Common BISO Reporting Structures

Regardless of the reporting structure, successful BISOs must establish strong partnerships with the business units or functions they support. They must have open lines of communication to their aligned risk owners and work closely with business leaders to understand the business' objectives, identify security risks, and develop security strategies that align with the organization's overall business goals. Examples of reporting structures include:

- **Report to the CISO or CIO:** In this structure, BISOs provide specialized security guidance and support for specific business units or functions and report directly to the CISO, who is responsible for the overall cybersecurity strategy and program.

  In some reporting structures, the BISO reports to a Regional Information Security Officer, who then reports to the Cyber Information Security Office.

  In organizations with only one region, a Senior BISO — who serves the CISO — may have one or more direct reports. This model focuses on strong adherence to cybersecurity governance and consistency in applying security controls and reducing cyber risk.

  Though reporting to the CISO ensures better alignment with enterprise-wide security strategies, it may limit the BISO's ability to advocate for unique business unit needs.

- **Report to the risk organization:** In this structure, BISOs report to the risk organization, which can include enterprise risk or technology risk.

© 2025 FS-ISAC, Inc. | All rights reserved |

- **Report to business unit leaders:** In this structure, BISOs report to the leaders of the business units they support, such as a Product Manager (i.e., cloud, merger and acquisition, computer network, etc.), Product Security Manager, or their respective technology division. This reporting structure is more common in larger enterprises with decentralized structures, where each business unit has its own security needs and priorities. Reporting directly to a business unit leader integrates the BISO into the team, allowing the BISO to prioritize business agility and innovation while providing localized security risk management. This arrangement ensures that security considerations are tightly aligned with the business' goals and operations. It can, however, create silos and limit centralized security oversight.

Compliance

It is important to note that in some industries, regulators have a say in the BISO's reporting structure as well as the BISO's remit and responsibilities.

- **Matrix reporting:** In this structure, BISOs report to both the CISO for security expertise and guidance and to the leaders of their respective business units for operational alignment. This dual reporting structure allows BISOs to balance the needs of the business with security requirements. Matrix reporting may layer BISOs under a Vice President (VP) — as can other structures — which may be appropriate for the business. However, this structure can direct activity toward the VP's focus areas, rather than the full scope of the cybersecurity organization.

Challenges of the Role and Solutions to Them

The way the BISO is positioned in the organization can create challenges for those in the role. The following issues are common to BISO programs.

Challenge: Ambiguity and crossover between BISOs. This issue often stems from overlapping roles, reporting structures, and responsibilities across various business units and departments. BISOs are typically positioned between business functions and the cybersecurity team, but the specific scope of their authority and responsibilities can vary greatly depending on the organization's structure.

- Solution: Define the BISO role and communicate — to all stakeholders — that the role is not a catch-all for miscellaneous cybersecurity administrative tasks.

© 2025 FS-ISAC, Inc. | All rights reserved |

Challenge: Shifting responsibilities. The BISO role contains an element of variety, which can cause "scope creep" and confusion about whether the BISO's primary focus is enforcing security policies or acting as a business enabler.

- Solution: Thoroughly document the scope and purpose of the BISO role. Though BISOs typically engage on topics across cybersecurity domains and leverage subject matter expertise as necessary, the BISO is not typically responsible for the implementation of recommended security guidance and controls.

Challenge: Poorly understood purpose. When the purpose of the BISO role is not communicated enterprise-wide, employees may fail to understand the role's function and pull BISOs into processes so late that the BISO can only course correct, escalate, or expedite.

For example, consider a business team implementing an AI project under the assumption that AI is a data quality solution outside the purview of cybersecurity (in fact, AI can impose significant cybersecurity risks). A BISO's input would enable the team to implement the AI solution within the business' risk tolerance, prevent remediation issues, and ensure the business impact of the technology.

- Solution: BISOs should be aware of evolving organizational needs and adapt accordingly. Such awareness results from continuously engaging with cybersecurity and business leadership at cybersecurity and business unit staff meetings, business-line compliance and risk routines, one-on-ones with key relationship partners, presentations, industry engagement, and mentoring.

Challenge: Navigating internal politics. The cross-functional nature of the role magnifies its susceptibility to internal politics.

- Solution: BISOs should prioritize understanding their organization's corporate culture and creating positive relationships, especially with the CISO, cybersecurity teams and leaders, and their business executives and stakeholders. Relationships with these partners can help BISOs navigate internal politics and set expectations for everyone involved.

© 2025 FS-ISAC, Inc. | All rights reserved |

Challenge: Lack of authority. BISOs need the ability to advise and direct teams but some structures and reporting lines give BISOs responsibility without authority. Where BISOs are asked to obtain results in their lines of business but lack authority or relationships with stakeholders, it can be difficult to drive security initiatives or influence business leaders to adopt secure practices.

RACI Framework: A project management tool that clarifies who is Responsible, Accountable, Consulted, and Informed for tasks.

- Solution: Empower the BISO to make decisions within pre-defined risk tolerance thresholds. In such structures, decision frameworks like RACI are recommended to support business-specific risk acceptance while ensuring enterprise-wide compliance.

Assessing the Success of a BISO Program/Role

Evaluating the success of a BISO program and/or role has proven difficult in every sector. Success is often subjective and defined by the BISO's engagement with the key stakeholders of their aligned business/function/region (BFR). The difficulty of a project might influence the perception of the BISO, for example, as might the BISO's support for more controls – a BISO who does not advocate for more security may be viewed as a partner; one who does may be seen as a barrier.

When measuring the subjective review of a BISO program/role, consider the following questions:

- Are BISOs involved in the right meetings to engage the BFR?
- How do their key stakeholders view them?
- How many connections does each BISO have with their partners? Where are they missing out?
- Do senior leaders have a positive view of the BISO?
- Since establishing the role, have unexpected issues or surprises been minimized and more insights provided to senior leaders?

Business/function/region

See *The Business Information Security Officer: An Overview; Actionable Advice from Practitioners in Four Industries* for insight on BFRs.

© 2025 FS-ISAC, Inc. | All rights reserved |

It's important to understand that these engagements may change over time or when the portfolios of the BISO or business units do. It may be difficult to determine where the BISO might be excluded.

Understanding the maturity of a BISO program will help determine how to measure its success. Various frameworks and models – such as the Capability Maturity Model Integration (CMMI) or the Gartner BI Maturity Model – can help gauge the program's maturity and the extent to which the BISO is achieving his or her mission.

CMMI defines five levels of maturity for any process or program:

1. Initial
2. Managed
3. Defined
4. Quantitatively managed
5. Optimizing

The **Gartner BI Maturity Model** focuses on the maturity of business intelligence:

- Unaware
- Reactive
- Proactive
- Managed
- Optimized
- Pervasive

How to Measure Success

There are no performance metrics defined specifically for the BISO role and they originate few projects or initiatives, making it hard to determine whether the completed work is the effort of the BISO or the project team.

However, given that the BISO is the chief cybersecurity advisor to the business, the BISO is critical in enabling the success of the business by helping to manage operational and cybersecurity risks. As a result, the BISO's (and cybersecurity's) strategic objectives should be aligned to the business' strategic objectives. The BISO's success could therefore be defined in terms of meeting business objectives in a secure and compliant way. What is measurable will depend on the maturity of the program and the BFR's metrics.

Methods of evaluating and measuring a BISO's performance and the subjectiveness of the role can include the following:

- The number of audits supported/engaged on (in organizations in which the BISO is responsible for supporting technology audits). Similarly, "low cyber findings"

© 2025 FS-ISAC, Inc. | All rights reserved |

could be a performance goal, if it conforms to the business leader's goals and is within the BISO's scope of responsibility.

- Rate of past-due security issues — 0% would indicate that identified security risks are well managed.
- Remediation status of penetration test findings by line of business.
- Degree of involvement in supporting the line of business (e.g., relationship building), such as the level of engagement in the appropriate meetings, working with the stakeholders, consulting on risk exceptions or acceptances, advising on regulatory alignment or proposed technology solutions, etc.
- A key stakeholder survey to create a net promoter score and collect feedback on BISOs, their program, and the quality of their work.
- A key stakeholder map to track the BISO's influence and the number and importance of their engagements. Some maps include how frequently the BISO should be engaged based on what that stakeholder values, how much interest they have in the BISO, and how many critical assets the BISO must support. See *Mapping the BISO Career: The Development of an Effective Business Information Security Office* for an example of a stakeholder map.
- A cyber health dashboard to follow contributions to/outcomes from agreed-upon objectives, projects (cybersecurity- or business-driven), and other initiatives where the BISO added value. Include how often a BISO is asked to help complete an out-of-scope task — many tasks are easily but erroneously attributable to the BISO's work.
- A Kanban board to capture the BISO's engagements and their solutions to the business. Break out strategic vs. tactical work completed by the BISO.
- Participation in training and development for themselves and extended to others (speaking, presenting, panelists, papers, and mentoring).
- Demonstrated decision-making maturity and the ability to take on new and varied projects.

Kanban Board

A visual presentation of task flow – i.e., To Do, In Progress, Review, Done – through different stages of a workflow.

© 2025 FS-ISAC, Inc. | All rights reserved |

- Contributions regarding Objectives and Key Results (OKRs) and Key Risk Indicators (KRIs) for cybersecurity teams and the lines of business related to cybersecurity, where appropriate.

Cultural Support for BISO Programs

Certain cultural attributes provide foundational support that helps BISOs succeed.

A clear objective. Define the responsibilities of the BISO, keeping in mind alignment to the needs of the business and security. For instance, what problem(s) or challenge(s) is the BISO program meant to address? What is the BISO intended to accomplish? Establish KPIs and/or KRIs at the business unit level to measure security posture (e.g., policy adherence) and business impact (e.g., reduced downtime due to security incidents).

Commitment to the team's success. Address the BISO's challenges, efforts, and values beyond greenlighting personnel or funding. A senior-level champion (i.e., CISO/cybersecurity and business leadership) is key, and support from the CIO and/or the executive leadership team is paramount. Ensure the BISO has decision-making scope and authority.

Effective communication channels. Choose appropriate channels, methods, and styles for the target audience within the organization. Choosing the right channel and receiving feedback are fundamental to starting and running a BISO program.

Diversity and teamwork. Recognize and appreciate the differences and similarities among team members to capitalize on the value of a variety of backgrounds, perspectives, experiences, and talents within the cybersecurity profession. An environment that values individuality *and* promotes teamwork and sharing information will be better equipped to address challenges that inevitably arise.

Cross-functional collaboration. Foster communication between BISOs, CISOs, and business leaders to align security with business objectives. Implement periodic BISO/CISO briefings to discuss emerging threats and align on strategic goals. Encourage cross-functional working groups and stakeholder briefings to promote knowledge sharing between security and business teams. Form a BISO Council chaired by the CISO to coordinate cybersecurity initiatives across business units, and use the council to drive security standards while addressing business-specific challenges.

© 2025 FS-ISAC, Inc. | All rights reserved |

Clarify role ownership. Aid the BISO's collaboration or engagement model by clarifying ownership for incident response, compliance, and risk management among the appropriate cybersecurity leaders.

Ensure consistent reporting. Provide security leadership and business stakeholders information with transparency. This can include reporting on business unit-aligned security risk assessments, control effectiveness, internal assessments on the cybersecurity program by risk (second line) and audit (third line), and business unit-specific security impacts and vulnerabilities.

© 2025 FS-ISAC, Inc. | All rights reserved |