Information Security Officer 1

Job summary

The Information Security Officer role will be the focal point for effective engagement between business areas and the Security Team. This role will be a trusted adviser to senior business and technology stakeholders and provide a broad knowledge of security strategies, policies, processes, architecture, and road maps to enable divisions/businesses to understand and meet security requirements.

The Information Security Officer role will report to the Head of Business Information Security Officer and work closely with the business, supporting to operate within the information security risk appetite. The Information Security Officer will be an essential business partner and will take responsibility for assessing and managing information security risks for the business.

This role will focus on ensuring that Information Security is considered in respect of all elements of Business. The Information Security Officer will be required to support business units with the design and implementation of central security strategies.

Responsibilities

Build and maintain effective relationships with a division’s Business and Technology stakeholders. Be the voice of information security in the division/business area and the voice of the business within the information security

Raise the profile of security within the organization by being pro-actively involved with stakeholders and customers

Own and communicate the divisional roadmap for information security aligned with risk appetite and overall security roadmap. Align information security responsibilities and working practices of divisions and security teams. Identify and resolve risks and issues

Facilitate planning, introduction, and delivery of information security services and initiatives e.g

Security capability / maturity improvement

Delivery of point services such as vulnerability assessments, project risk assessments, vendor assessments

Divisional security awareness and educations

Delivering targeted security and risk briefing

Collate demand for security and collaborate across the security team to balance the supply and demand of security and divisional resources

Contribution to the development and implementation of security architecture, and the design of security service and processes

Ensure that policy compliance is appropriate to the organizational and Business Unit’s level of risk acceptance

Demonstrate to stakeholders that appropriate security controls are in place and own/create actions plans to manage improvement or change where necessary

Advise stakeholders on how to achieve the relevant controls and assist with solutions to support them

Where necessary ensure that processes are documented and communicated in language that is relevant and understandable to international and /or non-technical audiences

Ensure all proposed technical solutions uphold security requirements

Support and deliver security initiatives as needed and be able to demonstrate and track progress to stakeholders

Manage divisional security incidents, working closely with the group and divisional stakeholders

Any other duties relating to the remit of a role of this standing as required by the needs of the business

Requirements

Experience managing multi-function relationships throughout major transformation;

Understanding of security technology;

Experience in a role balanced between business stakeholders and a central service organization;

Navigating a multifaceted, matrix organization; and

Collaborating with multiple stakeholders across functional and technical skillsets

Analytical: Inquisitive nature and intuition regarding what questions to ask, when, and their relative significance

Technical: Broad understanding of security technology

Business: High-level understanding of utility/energy sector business model, service offerings, and business operating environment as it pertains to the firm's threat landscape. Ability to frame threats and exposures in a business context recognized by non-technical staff and executives

Domain landscape: Knowledge of technical security operating principles

Communication: Ability to leverage business communication skills to inform, persuade, and teach stakeholders across a global network of member firms' staff and leadership to enable effective information security activities and processes in line with the cyber readiness program

The ability to build good relationships at all levels and across all business units and organizations, and the ability to influence stakeholders of all levels

Excellent verbal, written, and interpersonal communication skills. Listens and communicates technical subjects to both technical and non-technical audiences, flexes style to suit the needs of the audience

Ability to work with others effectively, with 3rd parties, internal teams, and international business units, promoting knowledge sharing within and across teams

Highly self-motivated and directed, with keen attention to detail

Information Security Officer 2

Job summary

We are looking for an Information Security Officer to take ownership of our information security program. From the development to maintenance of our policies and procedures to communication and stakeholder management both

externally and across the organization, this role is responsible for leading information security at the Company.

The ideal candidate for this role will have a deep knowledge of HIPAA and HITRUST requirements and will have been responsible for owning and implementing information security policies and procedures in compliance with these requirements. You will also have owned the third-party audit relationship, and be ready to take over our ongoing compliance requirements.

This role has the opportunity to progress into the leadership of the Quit Genius information security team as the company grows. Any previous leadership or mentoring experience is desirable, as the company is rapidly expanding and we have a lot of plans to improve upon our information security program across the board we will need to build out a team to execute this.

Responsibilities

Lead information security efforts

Develop and maintain our information security program

Ensure internal and external compliance

Manage client security assessments

Work with external audit firms to achieve and maintain compliance accreditations

Requirements

Extensive experience as an information security professional

Experience implementing an internal information security program preferred

HITRUST CCSFP certification

Proven ability to lead information security compliance and foster a culture of awareness and adherence

HIPAA compliance experience

Information Security Officer 3

Job summary

The Information Security Officer is responsible for establishing and maintaining the enterprise, vision, strategy, and program to ensure information assets and technologies are protected. This position reports to the Chief Information Officer.

Responsibilities

In conjunction with the Chief Information Officer, develop and manage information and organizational security policies, standards, and procedures to protect the Company from internal and external threats and vulnerabilities

Provide methodology for assessing organizational and information risks, gap analysis based on current controls

Develop repeatable processes for risk tolerance, risk prioritization, and mitigation

Guide Security practices with 3rd party providers such as cloud services, technology vendors, or any other services outsource to a 3rd party to ensure compliance with Company policies and standards

Identify information assets and categorizes them according to criticality and sensitivity

Formalize processes to catalog and maintain inventory of all software and hardware assets.

Develop internal security training programs and maintain materials for end users

Standardize subject access control to digital and physical assets, including data storage, applications, and services, physical and network infrastructure

Provide management and support of infrastructure planning and acceptance, malware protection, cryptography, PKI, backup and recovery, network and media management

Assist business units in the secure development of new and existing business systems

In conjunction with the Chief Information Officer, develop and implement plans to protect technology physical assets, including data centers and other controlled areas and controls for securing assets and equipment.

In conjunction with the Chief Information Officer, develop an incident management Lifecycle process that includes detection and analysis, containment, eradication, recovery, and post-incident activity

Collaborate with the business units at Company, assist in the development of a business continuity plan, continuity of operations plan, and disaster recovery plan

Guide compliance and regulatory requirements

Stay current on security practices, threat landscape, laws, and regulations

Requirements

Bachelor’s Degree in the field of Business Administration, Information Systems, Computer Science, or a related field is required

At least 5 years of experience, specifically in information security of multiple platforms, operating systems, software, and network protocols

CISSP or CISM Certifications are preferred

Knowledge of cyber security requirements of the following: HIPAA, FERPA, DSRIP

Knowledge of ITIL-based Service Management, Change Management, Problem Management, and Incident Management best practices

Ability to present complex technical concepts to a variety of audiences

Communicate clearly and effectively – orally and in writing

Information Security Officer 4

Job summary

The Information Security Officer (ISO) is responsible for providing strategic directions during the cloud migration and establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. The ISO performs security management and technical administration to provide security assurance for the agency's information resources. Work involves implementing information security measures and establishing and maintaining an agency-wide information security management program that protects information assets against both external and internal threats.

Manages security assurance activities related to the availability, integrity, and confidentiality of agency information in compliance with the state and the agency's information security policies. Works closely with executive management to determine acceptable levels of risk for the agency and creates and maintains a robust security role-based training program. Works under minimal supervision, with extensive latitude for the use of initiative and independent judgment. This position reports to the Chief Information Officer/Assistant Commissioner, Information Solutions and Services.

Responsibilities

Develops, implements, and monitors a strategic, comprehensive enterprise information security and IT risk management program to ensure that the integrity, confidentiality, and availability of information are owned, controlled, or processed.

Advises management and users regarding security policies, procedures, and best practices.

Acts as subject matter expert (SME) on cloud security issues; Designs, develops, reviews, and builds security architectures for public, private, and hybrid Cloud-based systems within Microsoft Azure, or other cloud providers.

Reviews guidelines, procedures, rules, and regulations and monitors compliance to ensure the agency remains in compliance with Texas Administrative Code Section 202.

Provides strategic risk guidance for IT projects, including the evaluation and recommendation of technical controls, and conducts risk pre-screening reviews and security sign-offs as appropriate for all application development projects.

Participates in Data Center Services (DCS) activities related to security assessment of data centers including Disaster Recovery (DR).

Oversees and completes Department of Information Resources (DIR) reviews and reports about information security.

Proactively works with Information Solutions and Services (ISS) staff and business units to develop security policies and implement practices that meet defined standards for information security. Develops and implements information and cybersecurity policies, standards, guidelines, and procedures to ensure information security capabilities cover current threat capabilities.

Develops security architecture and policies based on business needs, risk assessments, and regulatory requirements; and conducts information security risk analysis and system audits. Reviews and responds to special investigations, internal and external audits, and related reviews about information security issues and provide direction and guidance, and take ownership of required implementation.

Coordinates the use of external resources involved in the information security program, including, but not limited to, determining needs, recommending, and assisting with negotiating contracts and fees, and managing external resources.

Identifies evaluates, and reports on information security risks in a manner that meets compliance and regulatory

requirements, and aligns with and supports the risk posture of the agency.
Manages responses to security incidents and events to prevent unauthorized modification, destruction, or disclosure of information.
Performs internal scan/penetration analysis and testing; and researches and evaluates emerging security related technologies.
Plans, assigns, and supervises staff; and provides training and evaluations.
Maintains effective working relationships with all agency staff and representatives of other agencies and stakeholder organizations.
Represents ISS at meetings, conferences, seminars, or on panels and committees.
Perform other duties as assigned.

Requirements

Knowledge of local, state, and federal laws and regulations relevant to information security, privacy, and computer crime.
Knowledge of network security threats and ability to implement preventative controls including firewalls, access controls, authentication systems, intrusion detection systems, VPNs, and cryptography.
Knowledge of secure application programming guidelines; system development life cycles and limitations and capabilities of information systems.
Knowledge of cloud security concepts, technologies, and best practices, including but not limited to, automation frameworks, securing containers and container orchestration frameworks, Active Directory, LDAP, Federated SSO, One-Time Password (OTP) technology, SSL, encryption, IDS/IPS, SIEM, malware detection, forensics in a cloud environment, network and web app firewalls.
Knowledge of principles, practices, and techniques of management controls and information resources management.
Knowledge of network operating systems and client-server hardware and software and have demonstrated the ability to implement and maintain them in a production environment.
Knowledge of operational support of networks, operating systems, Internet technologies, databases, and security applications.
Skills in the use of vulnerability assessment and penetration testing tools with in-depth knowledge of network components such as bridges, routers, concentrators, cabling systems, and Ethernet in switched environments.
Skill in identifying, analyzing, and mitigating security-related issues.
Skill in configuring, deploying, and monitoring security infrastructure.
Ability to perform software installation, configuration, and maintenance of servers, routers, switches, firewalls, and other network security devices and complete project assignments within the allocated time frame, demonstrating patience and meticulousness in the implementation of information security solutions.
Ability to develop and interpret standards, policies, and procedures and analyze systems and procedures, write and

review standards and procedures, and handle multiple projects.

Ability to communicate effectively in a variety of forms.

Ability to establish and maintain effective working relationships with others.

Ability to work well under pressure and maintain flexibility.

Ability to plan, assign, and supervise the work of others.

Ability to identify problems, evaluate alternatives, and implement effective solutions.

Ability to resolve advanced security issues in diverse and decentralized environments.

Ability to proactively direct and organize program activities.

Bachelor’s degree from an accredited college or university with major coursework in computer science, management information systems, or equivalent.

3+ years of supervisory, management, or lead experience.

Must possess Certified Information Systems Security Professional (CISSP)

Must possess or be in the process of obtaining the Certified Cloud Security Professional (CCSP) certification.

3+ years of hands-on experience with Cloud platforms (Azure, AWS, etc.) required.

3+ years of hands-on experience implementing and managing cloud security tools required.

3+ years of experience with implementing and enforcing policies, procedures, and guidelines in a complex environment.

Information Security Officer 5

Job summary

The Information Security Officer position is to design and enforce policies and procedures that protect the university’s computing infrastructure from all forms of security breaches.

The primary responsibilities of Information Security Officer will be responsible for identifying vulnerabilities and working with our IT department to resolve them, ensuring that our network and data remain secure. To be successful as an Information Security Officer, you should have expert analytical skills and in-depth knowledge of best practices to prevent a wide range of security threats. Top candidates will also be excellent communicators, able to train and educate our staff on various information security topics.

Responsibilities

Provides the vision and strategies necessary to ensure the confidentiality, integrity, and availability of University electronic information

Communicating risk to senior administration

Creating and maintaining enforceable policies and supporting processes

Ensuring compliance with regulatory requirements

Coordinates activities with other departments, including the evaluation, procurement, and deployment of security-related

products

Develops and coordinates information security awareness and education programs

Requirements

Professional information security certification.

Experience in an information security role.

Solid knowledge of various information security frameworks.

Excellent problem-solving and analytical skills.

Ability to educate a non-technical audience about various security measures.

Effective verbal and written communication skills.

Associate degree or at least sixty hours of college credit are required.

A Bachelor’s degree is preferred

Professional certification (CISSP, GIAC, CISA, CISM, etc.) is preferred

The ability to understand hardware and software systems is required

The ability to maintain confidentiality regarding the information processed, stored, or accessed by the systems is required

The ability to manage multiple concurrent projects and to reason analytically is required

The ability to work with and train people possessing differing levels of technical knowledge is required

Effective verbal and written communication skills and proficiency in writing technical specifications are required

The ability to develop knowledge of, respect for, and skills to engage with those of other cultures or backgrounds is required

Information Security Officer 6

Job summary

The Information Security Officer is responsible for the oversight and implementation of the Bank’s Information Security Program.

Responsibilities

Responsible and accountable for implementing and monitoring the Bank’s formal Information Security Program including periodic reports on the state of Information Security to the Board of Directors and Senior Management.

Responsible for reviewing and updating the Bank’s Information Security (IT) Risk Assessment. This includes incorporating new systems/processes into the risk assessment. Ensures controls assessments are assigned and completed promptly.

Engages independent third parties to conduct testing of key controls and systems. Monitors progress on the remediation of findings. Provides updates to the Information Security Committee, the Audit Committee, and the Board of Directors.
Conducts internal assurance reviews to ensure that policies, procedures, and controls are operating effectively. Provides reports to the Information Security Committee and the Audit Committee.
Monitors cyber security threats and vulnerabilities. Communicates and discuss relevant information with the Information Technology Department and the Information Security Committee.
Responsible for maintaining the Bank's Information Security Incident Response Plan. Coordinates incident response activities as needed.
Assists management to evaluate the security controls of third-party service providers.
Reviews daily reports to provide oversight regarding changes to configurations and/or user changes on the network.
Ensures change management procedures are adhered to.
Works closely with project owners throughout the project to identify potential project risks and threats, including cybersecurity, and validates that testing results are consistent with predefined measurements of success.
Assists in the preparation for external audits, regulatory exams, and third-party vulnerability assessments and penetration testing.
Assists with Information Security training to support employee and customer awareness.
Chairs the Bank's Information Security Committee. Serves as a member of the Risk Management and Technology Steering Committees.
Provides professional, courteous, and efficient service to all internal and external customers.
Attends all required meetings and training.
Performs other miscellaneous duties or special assignments as required or assigned.
Complies with federal and state banking regulations, as well as with all bank and department policies and procedures.

Requirements

Bachelor of Science Degree preferred.
Five to seven years of Information Security and IT experience, preferably in a financial institution.
Proficiency in understanding information systems and risk management theory, standards, procedures, and techniques.
Good interpersonal skills with the ability to maintain satisfactory relationships with all employees.
A solid knowledge of banking regulations.
Proven ability to deliver quality work during times of increased volumes.
Excellent customer service skills.
Ability to adapt to changes in priorities quickly.
Interacts harmoniously, professionally, cordially, and effectively with others, focusing on the attainment of bank goals and objectives through a commitment to teamwork.
Strong written and verbal communication, interpersonal, time management, and organizational skills.

Operational competency using Microsoft Office suite; Proficient in Outlook, Word and Excel, and other Windows-based applications; comfortable learning new software.

Strong attention to detail.

Commitment to ongoing learning.

Ability to work independently and as a team player.

Ability to read/see documents and computer screens, to communicate in person and via the telephone and to operate a computer and other office equipment.

Is dependable and conforms to punctuality and attendance standards.

Information Security Officer 7

Job summary

The Chief Information Security Officer works closely with the CIO and Deputy CIO to maintain the security of the IT Network at all County locations. This position will develop, implement, analyze, and manage security policy, assist in strategic planning, research, recommend and implement security solutions, and develop and oversee a Countywide security & HIPAA awareness and training program. The position will also be responsible for creating and maintaining the County's Business Continuity plan for IT and coordinating the creation of plans by County departments.

This position is deemed essential and may be required to work during inclement weather, natural disaster, other emergencies, and/or when the County offices are officially closed due to inclement weather, natural disaster, or other emergencies, etc.

Responsibilities

Develop, Implement, analyze, and manage the County's security policy

Serve as mentor and coach to senior staff members

Ensure that the mix of technology services offered by the department is appropriate to help in fulfilling the department's strategic plan; proactively review and modify services offered to meet the changing needs of business Countywide

Develop, implement and maintain a Countywide Security & HIPAA awareness and training program

Develop departmental policies, procedures, and strategic planning based on the direction set forth by the CIO

Produce innovative ideas and keep tabs on the latest trends, applying as necessary to fulfill business needs Countywide

Ensure current and new operations plans and procedures are consistent with departmental goals and objectives

Appropriately set division budgetary constraints and oversee purchases and budget usage

Requirements

Bachelor's degree in Computer Science, Information Systems, or a related field

Five (5) or more years of experience in a technical field working with computer hardware and software, including applications and networking with at least one (1) year of management/leadership experience that included strategic planning, resource allocation, production methods, and coordination of people and resources, or;

Any equivalent combination of education and experience

Knowledge of data security and control measures

Knowledge of strategic computing and disaster recovery methods

Knowledge of current technology advances

Knowledge of networking fundamentals

Strong skills in analyzing information and using logic to address work-related issues and problems

Proper handling of the most confidential information/materials

Ability to communicate orally and written in a professional manner

Ability to work well both alone and in a team setting

Valid driver’s license and acceptable driving record by County policy

Acceptable pre-employment criminal background check

CISM (or equivalent – Preferred after 1 year of employment)

Information Security Officer 8

Job summary

The Information Security Officer is responsible for assisting the Security and Information Security Officer (and other employees within the department) in all duties as needed related to Security, Information Security, and Business Continuity.

Responsibilities

Update alarm access as needed

Assist in alarm monitoring, video surveillance monitoring, and research for fraud events.

Assist in the production and submission of subpoenas, IRS summons, Garnishments, and Interrogatories o Serve as a point of contact for alarm notifications and alerts

Assist in law enforcement requests on fraud cases

Assist in updating policies, procedures, and risk assessments

Research equipment for security needs

Assist in managing ATM/AHD lighting surveys, distribute test results to BCs twice annually, and help track the clearing of deficiencies

Assist with Fraud Packets and Fraud related Account Closure Letters

Assist with Without Entry claims

Help with robbery and security training

Requirements

Three to five years of banking or security experience

Self-starter, highly motivated, and attention to detail is necessary (ability to multitask)

Ability to research banking and security-related regulations and interpret them to enhance the Bank’s policies and procedures

Excellent verbal and written communication skills

Proficient in Microsoft Word, Powerpoint, Excel, etc.

Information Security Officer 9

Job summary

The Information Security Officer (ISO) is a senior-level professional responsible for driving efforts to prevent, monitor and respond to information/data breaches and cyber-attacks. The overall objective of this role is to ensure the execution of Information Security directives and activities in alignment with the Company's data security policy.

Responsibilities

Demonstrates understanding of the Company’s IS standards and best practices. Communicates relevant updates and changes to Citi’s IS standards and processes with the business.

Communicates with the Sector and Regional IS Heads and business managers; escalates issues as needed.

Establishes relationships with business managers and is consulted as a subject matter expert in IS. Influences decisions through recommendations and strong interpersonal skills.

Performs ISO-related tasks across the Company’s IS programs and ensures that deliverables are completed per the programs’ timelines.

Documents all suspected, identified, and reported security incidents (SIRTs). When needed, assists security incident response teams’ investigators triage and/or responding to crises or urgent situations to mitigate immediate and potential threats.

Establishes working relationships or networks with cross-sector ISOs, to strengthen relationships to efficiently tackle security issues that may impact multiple businesses. Leverages the ISO network to seek out best practices and create efficiencies. May participate in IS program working groups.

As needed, partners with stakeholders in other risk management disciplines; e.g. MCA, CoB, Records Management, Fraud Management, etc.

Assists in documenting Corrective Action Plans (CAPs) for all IS-related gaps and reviews evidence before submitting

issues for closure to ensure they meet Company’s requirements.

Works with the business to manage IS risk by analyzing the root cause, impact, and likelihood of issues, and then supports the business in implementing CAPs, Risk Exceptions, and/or compensating controls where appropriate.

Partners with TISOs and Application Managers to ensure vulnerability assessments are completed and issues are remediated by Company’s System Security Testing Standards (SSTS).

As required by local in-country regulators, ISOs may serve as the first point of contact for IS related topics and provide IS deliverables during regulatory audits.

Requirements

6-10 years of relevant experience

CISA, CISM, and/or CISSP certification is desired

Proficient in interpreting and applying policies, standards, and procedures

Consistently demonstrates clear and concise written and verbal communication

Proven influencing and relationship management skills

Proven analytical skills

Bachelor’s degree/University degree or equivalent experience

Master’s degree preferred

Information Security Officer 10

Job summary

The Information Security Officer may manage multiple related teams of managers and/or professional staff responsible for developing, implementing, and maintaining information security and identity management policies, procedures, and systems. Manages the deployment of security defense and identity management technologies, the management of existing infrastructure, and the response to cyber security incidents. Determines risks to the organization by directing security testing.

Responsibilities

Aligning with the University Information Security Office, execute a risk-based information security program for the BSD, including items such as access management, device security, incident response, policies, training, risk management, security architecture, vulnerability management, PCI/HIPPA compliance, support data governance, data stewardship, and technical architecture review programs.

Guide and counsel the Assistant Dean BSD Information Technology Services and organizational leaders on information security and its role in enabling mission activities and managing IT Security risk, in both strategic and tactical contexts.

Review hardware, software, and services being considered for purchase or implementation by BSDIS and other campus

departments to assess security issues (strengths/risks) and assure proper information security features are incorporated to support university business needs; provide security requirements to be included in RFPs for software and services.
Review Data Use Agreements and Procurement Contracts for the BSD to ensure security measures are appropriately identified and managed.
Establish annual and long-range security and compliance goals. Define security strategies, metrics, reporting mechanisms, and program services. Create maturity models and a roadmap for continual program improvements.
Engage with external communities and activities to maintain a good perspective on information security practices at peer organizations and the threat environment, and to promote and increase the inter-organizational ability to address common problems.
Oversee the management and administration of all security systems and their corresponding software, including firewalls, VPNs, intrusion detection, cryptography, content filters, and anti-malware systems.
Determine baseline security configuration standards for operating systems (e.g., OS hardening), network segmentation, and identity and access management (IAM).
Manage teams that research security alerts and anomalies and develop remediation plans. Regularly develop advanced hunt techniques for the identification of threat actors across the internal network. Create penetration testing plans, and execute and remediate findings.
Assume responsibility for digital forensics and eDiscovery tools, as well as perform data gathering to support internal and external litigation. Summarize and report results.
Lead the development and implementation of effective and reasonable policies and practices to secure protected and sensitive data and ensure information security and compliance with relevant legislation and legal interpretation.
Lead efforts to assess, evaluate and make recommendations regarding the adequacy of security controls for the BSD's information and technology systems, and establish a process that guarantees rigorous and appropriate vetting and risk assessment.

Requirements

Minimum requirements include a college or university degree in a related field.
Minimum requirements include knowledge and skills developed through 7+ years of work experience in a related job discipline.
Bachelor's Degree in Information Technology, Information Systems Security, Cybersecurity, or related field.
Must be an intelligent, articulate, consensus-building, and persuasive leader who can serve as an effective member of the senior management team and communicate information security-related concepts to a broad range of technical and non-technical team members at all levels of the organization.
Seven to ten years in a leadership role of combined IT and security work experience, with broad exposure to infrastructure/network, cloud, endpoint, and multiplatform environments.