ICT Security Specialist

Summary statement

Ensures the implementation of the organizations security policy.

Mission

Proposes and implements necessary security updates. Advises, supports, informs and provides training and security awareness. Takes direct action on all or part of a network or system. Is recognized as the ICT technical security expert by peers. Focus on protecting an organisation's data.

Accountable	Responsible	Contributor
▪ Knowledge or Information base (Security)	▪ New technology integration proposal (Security)	▪ Risk Management policy ▪ Risk Management Plan ▪ Information security policy

Main task/s

- Ensure security and appropriate use of ICT resources
- Evaluate risks, threats and consequences
- Provide security training and education
- Provide technical validation of security tools
- Contribute to definition of security standards
- Audit security vulnerability
- Monitor security developments to ensure data and physical security of the ICT resources

KPI area

Security measures in place

C - Run

C.2. Change Support

Implements and guides the evolution of an ICT solution. Ensures efficient control and scheduling of software or hardware modifications to prevent multiple upgrades creating unpredictable outcomes. Minimises service disruption as a consequence of changes and adheres to defined

service level agreement (SLA). Ensures consideration and compliance with information security procedures.

Proficiency Levels

Proficiency Level 3 - Ensures the integrity of the system by controlling the application of functional updates, software or hardware additions and maintenance activities. Complies with budget requirements.

C.3. Service Delivery
Ensures service delivery in accordance with established service level agreements (SLA's). Takes proactive action to ensure stable and secure applications and ICT infrastructure to avoid potential service disruptions, attending to capacity planning and to information security. Updates operational document library and logs all service incidents. Maintains monitoring and management tools (i.e. scripts, procedures). Maintains IS services. Takes proactive measures.

Proficiency Levels

Proficiency Level 3 - Programmes the schedule of operational tasks. Manages costs and budget according to the internal procedures and external constraints. Identifies the optimum number of people required to resource the operational management of the IS infrastructure.

D - Enable

D.9. Personnel Development
Diagnoses individual and group competence, identifying skill needs and skill gaps. Reviews training and development options and selects appropriate methodology taking into account the individual, project and business requirements. Coaches and/ or mentors individuals and teams to address learning needs.

Proficiency Levels

Proficiency Level 3 - Monitors and addressees the development needs of individuals and teams.

D.10. Information and Knowledge Management
Identifies and manages structured and unstructured information and considers information distribution policies. Creates information structure to enable exploitation and optimisation of information. Understands appropriate tools to be deployed to create, extract, maintain, renew and propagate business knowledge in order to capitalise from the information asset.

Proficiency Levels

Proficiency Level 3 - Analyses business processes and associated information requirements and provides the most appropriate information structure.

E - Manage

E.8. Information Security Management
Implements information security policy. Monitors and takes action against intrusion, fraud and security breaches or leaks. Ensures that security risks are analysed and managed with respect to enterprise data and information. Reviews security incidents, makes recommendations for security policy and strategy to ensure continuous improvement of security provision.

Proficiency Levels

Proficiency Level 3 - Evaluates security management measures and indicators and decides if compliant to information security policy. Investigates and instigates remedial measures to address any security breaches.

Proficiency Level 4 - Provides leadership for the integrity, confidentiality and availability of data stored on information systems and complies with all legal requirements.

Responsibilities:

- Develop and maintain security architecture artifacts (e.g. models, templates, standards, and procedures) that can be used to leverage security capabilities in projects and operations
- Ensure a complete, accurate, and valid inventory of all systems that should be logged by the an tool
- Responsible for ensuring that the Information Security policies and controls remain current and compliant within financial organizations
- Participate in formal hardware, software and project assessments to validate secure deployment and compliance.
- Perform Risk Assessments for proposed new technologies, infrastructure architecture changes, third party applications, vendor solutions
- Reporting to the head of ICT Finance
- Provide monthly status reports about the goals to be achieved

Qualifications:

- Bachelor degree based on a completed education in IT;
- At least 5-10 years of proven IT experience in an enterprise network environment, of which at least 3 years in the field of IT Security in financial organizations.;
- Demonstrable strategic insight and have a good conceptual thinking ability;
- Proven knowledge in the field of information security, preferably through the CISSP & CISA certification;
- Knowledge of and experience with applied products within the ICT infrastructure;

- Knowledge of and experience with
  - Relevant market standards in the field of information security: ISO / NEN 27001 and 27002 and BIR;
  - Relevant laws and regulations (such as the Protection of Personal Data Act);
  - Knowledge of ITILv3 and PRINCE2;

- Required English and Dutch oral and written