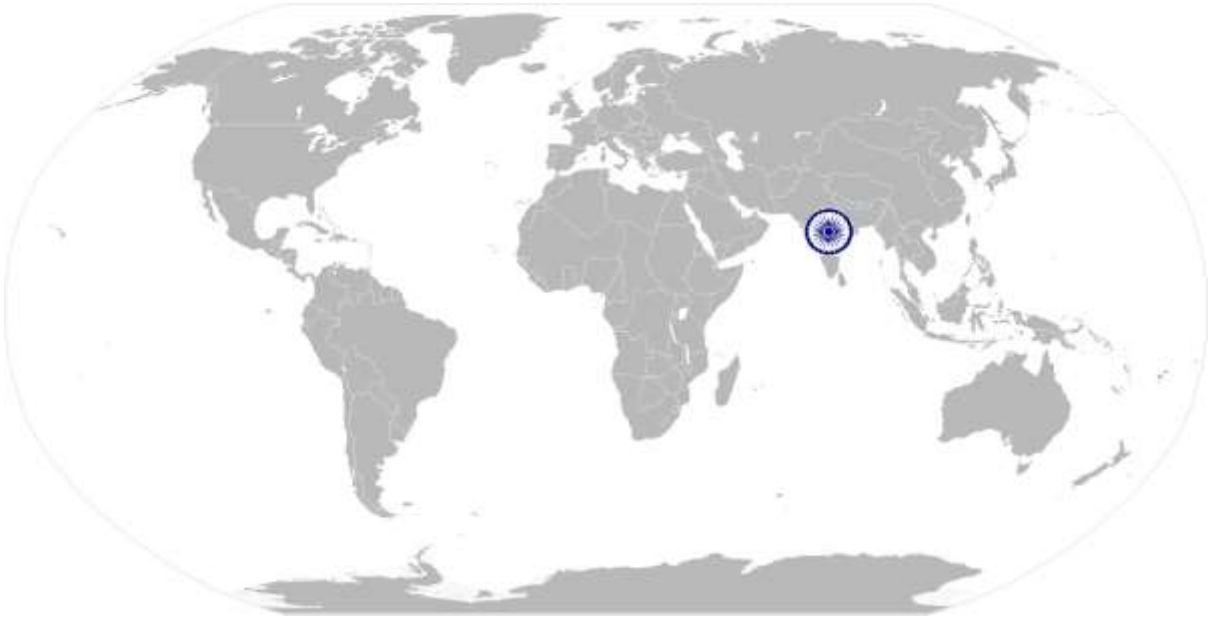
SSC/ N 0902 Co-ordinate responses to information security incidents

National Occupational Standard



Overview

This unit is about playing a co-ordinating role in responding to information security incidents, liaising with members of the security team who carry out investigations and other stakeholders or business users.

SSC/ N 0902 Co-ordinate responses to information security incidents

Applicable NOS Unit

Unit Code	**SSC/ N 0902**
Unit Title (Task)	**Co-ordinate responses to information security incidents**
Description	This unit is about playing a co-ordinating role in responding to information security incidents, liaising with members of the security team who carry out investigations and other stakeholders or business users.
Scope	This unit/task covers the following: **Information security incidents** may cover: • Identify and Access Management (IdAM) • physical security • networks (wired and wireless) • devices • endpoints/edge devices • storage devices • servers • software • applications security • content management • messaging • web security • security of infrastructure • infrastructure devices (eg routers, firewall services) • computer assets, server s and storage networks • messaging • intrusion detection/prevention • security incident management • third party security management • personnel security requirements **Information security incidents**: • automatically by tools and systems • manually by employees or business users **Appropriate people**: • line manager • members of the security team • incident management group • subject matter experts
Performance Criteria (PC) w.r.t. the Scope	

SSC/ N 0902 Co-ordinate responses to information security incidents

	To be competent, you must be able to: PC1. establish your role and responsibilities in co-ordinating responses to **information security incidents** PC2. record, classify and prioritize **information security incidents** using standard templates and tools PC3. access your organization's knowledge base for information on previous **information security incidents** and how these were managed PC4. assign **information security incidents** promptly to **appropriate people** for investigation/action PC5. liaise with stakeholders to gather, validate and provide information related to **information security incidents**, where required PC6. track progress of investigations into **information security incidents** and escalate to **appropriate people** where progress does not comply with standards or service level agreements (SLAs) PC7. prepare accurate preliminary reports on **information security incidents** using standard templates and tools PC8. submit preliminary reports promptly to **appropriate people** for action PC9. update the status of **information security incidents** following investigation/action using standard templates and tools PC10. obtain advice and guidance on co-ordinating **information security incidents** from **appropriate people**, where required PC11. update your organization's knowledge base promptly and accurately with **information security incidents** and how they were managed PC12. comply with your organization's policies, standards, procedures, guidelines and service level agreements (SLAs) when co-ordinating responses to **information security incidents**
Knowledge and Understanding (K)	
A. Organizational Context (Knowledge of the company/ organization and its processes)	You need to know and understand: KA1. your organization's policies, procedures, standards, guidelines and service level agreements for responding to information security incidents KA2. the day-to-day operations, procedures and tasks relating to your area of work KA3. your organization's knowledge base and how to access and update this KA4. limits of your role and responsibilities and who to seek guidance from where required KA5. the purpose of managing information security incident s KA6. who to involve when investigating and co-ordinating responses to information security incidents and how to contact them KA7. the importance of tracking progress and corrective and preventative actions for information security incidents

SSC/ N 0902 Co-ordinate responses to information security incidents

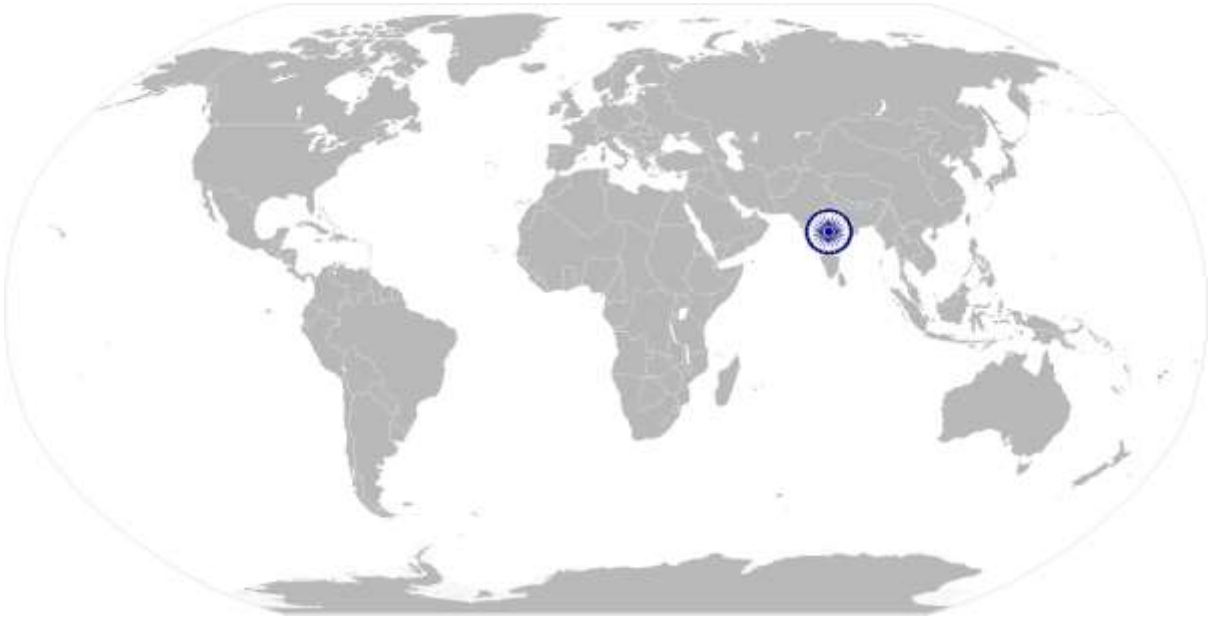
	KA8. the importance of keeping records and evidence relating to information security incidents KA9. the impact information security incidents can have on your organization KA10. different types of information security incidents and how to deal with these KA11. how to assign and escalate information on information security incidents KA12. different methods and techniques used when working with others KA13. standard tools and templates available and how to use these KA14. your organization's policies and procedures for sharing information on security incidents and the importance of complying with these KA15. how to classify and priorities information security incidents
B. Technical Knowledge	You need to know and understand: KB1. fundamentals of information security and how to apply these, including: • networks • communication • application security KB2. routine operational procedures and tasks required to co-ordinate and respond to information security incidents KB3. different stages of incident management and your role in relation to these, including: • identify • contain • cleanse • recover • close KB4. how to identify and resolve information security vulnerabilities and incidents KB5. common issues and incidents of information security that may require action and who to report these to KB6. how to obtain and validate information related to information security issues KB7. how to prepare and submit information security reports and who to share these with
Skills (S)	
A. Core Skills/ Generic Skills	**Writing Skills**
	You need to know and understand how to: SA1. complete accurate well written work with attention to detail SA2. communicate with others in writing
	Reading Skills
	You need to know and understand how to: SA3. follow guidelines, procedures, rules and service level agreements

SSC/ N 0902 Co-ordinate responses to information security incidents

	Oral Communication (Listening and Speaking skills)
	You need to know and understand how to: SA4. listen effectively and orally communicate information accurately SA5. ask for clarification and advice from others
B. Professional Skills	**Decision Making**
	You need to know and understand how to: SB1. follow rule-based decision-making processes SB2. make decisions on suitable courses of action
	Plan and Organize
	You need to know and understand how to: SB3. plan and organize your work to achieve targets and deadlines
	Customer Centricity
	You need to know and understand how to: SB4. build and maintain positive and effective relationships with customers SB5. check your own work meets customer requirements
	Problem Solving
	You need to know and understand how to: SB6. apply problem solving approaches in different situations SB7. seek clarification on problems from others SB8. refer anomalies to the line manager
	Analytical Thinking
	You need to know and understand how to: SB9. analyze data and activities SB10. configure data and disseminate relevant information to others SB11. pass on relevant information to others
	Critical Thinking
	You need to know and understand how to: SB12. provide opinions on work in a detailed and constructive way SB13. apply balanced judgments to different situations
	Attention to Detail
	You need to know and understand how to: SB14. apply good attention to details SB15. check your work is complete and free from errors
	Team Working
	You need to know and understand how to: SB16. work effectively in a team environment SB17. contribute to the quality of team working SB18. work independently and collaboratively

SSC/ N 0902 Co-ordinate responses to information security incidents

C. Technical Skills	You need to know and understand how to: SC1. use information technology effectively to input and/or extract data accurately SC2. identify and refer anomalies in data SC3. store and retrieve information SC4. agree objectives and work requirements SC5. keep up to date with changes, procedures and practices in your role



SSC/ N 0902 Co-ordinate responses to information security incidents

NOS Version Control

NOS Code	SSC/ N 0902		
Credits(NVEQF/NVQF/NSQF) [*OPTIONAL*]		Version number	0.1
Industry	IT-ITeS	Drafted on	30/04/2013
Industry Sub-sector	IT Services	Last reviewed on	31/03/2018
		Next review date	31/03/2019