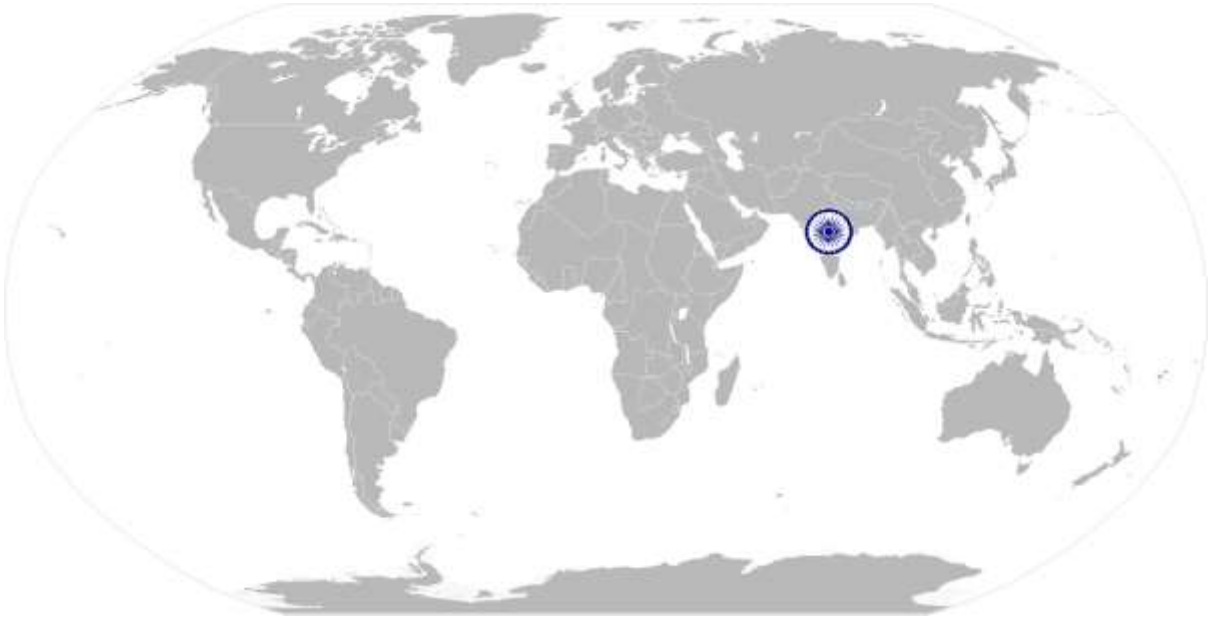
National Occupational Standard



Overview

This unit is about carrying out specified tasks as part of a team working to ensure information security.

SSC/ N 0901 **Contribute to managing information security**

Applicable NOS Unit

Unit Code	SSC/ N 0901
Unit Title (Task)	**Contribute to managing information security**
Description	This unit is about carrying out specified tasks as part of a team working to ensure information security.
Scope	This unit/task covers the following: **Information security** includes: • 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 **Backups** includes: • validation • tracking • consolidation • replication • configuration • logs • devices • applications • software

SSC/ N 0901 **Contribute to managing information security**

	Appropriate people: • line manager • members of the security team • subject matter experts
Performance Criteria (PC) w.r.t. the Scope	
	To be competent, you must be able to: PC1. establish your role and responsibilities in contributing to managing **information security** PC2. monitor systems and apply controls in line with **information security** policies, procedures and guidelines PC3. carry out security assessment of **information security** systems using automated tools PC4. carry out configuration reviews of **information security** systems using automated tools, where required PC5. carry out **backups** of security devices and applications in line with **information security** policies, procedures and guidelines, where required PC6. maintain accurate daily records/logs of **information security** performance parameters using standard templates and tools PC7. analyze **information security** performance metrics to highlight variances and issues for action by **appropriate people** PC8. provide inputs to root cause analysis and the resolution of **information security** issues, where required PC9. update your organization's knowledge base promptly and accurately with **information security** issues and their resolution PC10. obtain advice and guidance on **information security** issues from **appropriate people**, where required PC11. comply with your organization's policies, standards, procedures and guidelines when contributing to managing **information security**
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 and guidelines for managing information security KA2. your organization's knowledge base and how to access and update this KA3. limits of your role and responsibilities and who to seek guidance from KA4. the organizational systems, procedures and tasks/checklists within the domain and how to use these KA5. how to analyze root causes of information security issues KA6. how to carry out information security assessments

	KA7. how to carry out configuration reviews KA8. how to correlate devices and logs KA9. different types of automation tools and how to use these KA10. how to access and analyze information security performance metrics KA11. who to involve when managing information security KA12. your organization's information security systems and tools and how to access and maintain these KA13. standard tools and templates available and how to use these
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. different types of backups for security devices and applications and how to carry out backups KB3. common issues and variances of performance metrics that require action and who to report these to KB4. how to identify and resolve information security vulnerabilities and issues
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
	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. carry out rule-based transactions in line with customer-specific guidelines, procedures, rules and service level agreements SB5. check your own and/or your peers 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
	Analytical Thinking
	You need to know and understand how to: SB8. analyze data and activities SB9. configure data and disseminate relevant information to others SB10. pass on relevant information to others
	Critical Thinking
	You need to know and understand how to: SB11. provide opinions on work in a detailed and constructive way SB12. apply balanced judgments to different situations
	Attention to Detail
	You need to know and understand how to: SB13. check your work is complete and free from errors
	Team Working
	You need to know and understand how to: SB14. work effectively in a team environment SB15. work independently and collaboratively
C. Technical Skills	You need to know and understand how to: SC1. use information technology effectively to input and/or extract data accurately SC2. store and retrieve information SC3. identify and refer anomalies in data SC4. keep up to date with changes, procedures and practices in your field of expertise

SSC/ N 0901 **Contribute to managing information security**

NOS Version Control

NOS Code	SSC/ N 0901		
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