TECIS60553

Manage information security identity and access management activities

Overview

Identity and access management (IAM) deals with how users within an organisation are given an identity and how it is protected. It also included protecting critical applications, data and systems from unauthorised access, and managing access rights of people both inside and outside the organisation. This is especially important in the light of recent trends towards bring-your-own-device, cloud computing, mobile apps and an increasingly mobile workforce. Identity and access management involves protecting our data assets and implementing processes and procurement standards to run organisations more intelligently.

This standard defines the competencies associated with managing identity and access management activities. This includes setting policies and standards and ensuring that identity and access management processes are dynamic and respond to changing security status of data and information systems and also ensure that intruders cannot gain access to systems or to user accounts, especially those with excessive privileges to prevent data loss or theft.

Performance criteria

You must be able to:

1. implement information security policies, controls and standards for identity and access management in line with organisational requirements
2. develop the identity and access management aspects of information security architecture to support large user communities with complex information authorisation rules and requirements
3. identify and review all information security identity and access management compliance mandates (including privacy regulations) to which the organisation is subject in a timely manner
4. regularly review organisational compliance with internal and external standards and regulations in relation to information security identity and access management
5. evaluate and recommend new identity and access management security technologies, processes and methodologies in line with organisational requirements
6. identify and implement training and development programmes for information security identity and access management in line with organisational requirements
7. monitor adherence of identity and access management activities to identity and access management controls in line with organisational standards

Knowledge and understanding

You need to know and understand:

1. how to define the identity and access management aspects of the information security architecture
2. the importance of aligning identity and access management initiatives to business processes
3. the need to monitor identity and access management controls and ensure regulatory compliance to required standards
4. how to apply performance metrics to identity and access management activities and their deliverables
5. how to select and acquire technologies and vendors/service providers for identity and access management
6. how to audit access rights and modify these as appropriate
7. the current identity and access management capabilities of the organisation
8. how to identify technology and service gaps needing functional improvement
9. the need to keep up to date on the shifting compliance landscape
10. the importance of gaining management agreement on the vision and mandate behind the strategy and policies for identity and access management
11. the need to establish appropriate resources, budget and governance systems for identity and access management

TECIS60553

Manage information security identity and access management activities

Developed by	e-skills
Version Number	1
Date Approved	March 2016
Indicative Review Date	April 2019
Validity	Current
Status	Original
Originating Organisation	The Tech Partnership
Original URN	TECIS60553
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, identity and access management