Reporting e comunicazione del rischio

Traccia

Un'azienda ha richiesto la raccolta di informazione per la conduzione di un risk assessment. Lo scenario da valutare è la gestione dei controlli di accesso.

- Prepara un elenco di persone chiave da intervistare nell'azienda e i potenziali argomenti di discussione per ciascuna di esse.
- Identifica i tipi di documentazione che dovresti rivedere per raccogliere informazioni su processi, sistemi e controlli di sicurezza.
- Descrivi i test che potresti eseguire per raccogliere dati sulla configurazione dei sistemi IT e sulla sicurezza delle reti.

Ricordatevi delle risorse utilizzate nell'esercizio di ieri e del materiale relativo ai controlli.

Elenco di persone chiave da intervistare

B. Component: Organizational Structures									
Key Management Practice	**Chief Information Officer**	**Chief Information Security Officer**	**Business Process Owners**	**Head Human Resources**	**Head Development**	**Head IT Operations**	**Information Security Manager**	**Privacy Officer**
DSS05.01 Protect against malicious software.		A	R	R	R	R	R	
DSS05.02 Manage network and connectivity security.		A			R	R	R	
DSS05.03 Manage endpoint security.		A			R	R	R	
DSS05.04 Manage user identity and logical access.		A	R			R	R	R
DSS05.05 Manage physical access to I&T assets.		A				R	R	R

Argomenti di discussione

DSS05.04 Manage user identity and logical access.	APO01.05	Definition of I&T-related roles and responsibilities	Results of reviews of user accounts and privileges	Internal
	APO03.02	Information architecture model	Approved user access rights	Internal

Componenti su cui raccogliere informazioni

G. Component: Services, Infrastructure and Applications
• Directory services • Email filtering systems • Identity and access management system • Security awareness services • Security information and event management (SIEM) tools • Security operations center (SOC) services • Third-party security assessment services • URL filtering systems

Test da effettuare per raccolta dati

Activities	Capability Level
1. Continually use a portfolio of supported technologies, services and assets (e.g., vulnerability scanners, fuzzers and sniffers, protocol analyzers) to identify information security vulnerabilities.	2
2. Define and communicate risk scenarios, so they can be easily recognized, and the likelihood and impact understood.	
3. Regularly review the event logs for potential incidents.	
4. Ensure that security--related incident tickets are created in a timely manner when monitoring identifies potential incidents.	
5. Log security-related events and retain records for appropriate period.	3