




Example Sample Questions

IPSec Cyber Breach Capability Survey Sample Questions

Incident Tracking

Is an Incident Management Tool maintained to track incidents from escalation, closure to reporting impacting agreed Service Levels of the application in production?

- ☐ No formal incident management.
- ☐ Some incidents managed formally.
- ☐ Incident management implemented through a centralised tool.
- ☐ Incident management implemented in a centralised tool with monitored resolution KPIs.
- ☐ Tool based incident management with incident analytics to predict incident load.
- ☐ Not applicable.




Add explanation:  Ask a question about this control:  Evidence: 

Control ID: C0024

DLP Monitoring

Is the Security Operations Centre responsible for reviewing the rule exceptions and security events raised by the Data Loss Prevention solution and actioning accordingly?

- ☐ No DLP team.
- ☐ Ad-hoc actioning of DLP alerts.
- ☐ Defined process for analysing and reacting to DLP alerts.
- ☐ Defined processes with monitored SLAs for actioning alerts.
- ☐ Established DLP response team as part of Security Operations Centre / SIEM.
- ☐ Not applicable.




Add explanation:  Ask a question about this control:  Evidence: 

Control ID: C0205

Breach Evaluation

Does the Data Privacy Officer evaluate the severity of each data breach and assess the impact to customers, employees, third parties and the company?

- ☐ No management of data breaches.
- ☐ Reactive approach to data breaches.
- ☐ Formally defined approach for handling data breaches.
- ☐ DLP and IDS systems in place to detect data breaches.
- ☐ Data breach process fully integrated with legal, IT, Business Continuity Management and SIEM processes.
- ☐ Not applicable.

Add explanation:  Ask a question about this control:  Evidence: 




Control ID: C0272

Logging Requirements

Do all systems with authentication functions log at least

- user logins,
- timestamp of last login,
- failed login attempts,
- logins with privileged access accounts, and
- changes to user entitlements?

-
- ☐ No logging requirement.
 - ☐ Most data fields logged.
 - ☐ Formal logging requirements defined.
 - ☐ Formal logging requirements defined and monitored.
 - ☐ Formal logging requirements defined, monitored and integrated with SIEM.
 - ☐ Not applicable.




Add explanation:  Ask a question about this control:  Evidence: 

Control ID: C0366

Security Monitoring

Are all devices used within the bring your own device program equipped with the organisation's security monitoring solutions as applicable such as anti malware and data loss prevention software?

-
- ☐ No security monitoring.
 - ☐ Some monitoring depending on user diligence.
 - ☐ Formal requirement for monitoring defined.
 - ☐ Security monitoring implemented on all devices.
 - ☐ Security monitoring implemented and integrated with SIEM.
 - ☐ Not applicable.

Add explanation:  Ask a question about this control:  Evidence: 




Control ID: C0672

IPSec Cloud Security Preparedness Survey Example Questions

Cloud Service Management

Is the CIO responsible for managing all cloud services for the organisation?

- ☐ No person nominated.
- ☐ Task mostly executed ad-hoc.
- ☐ Accountability formally assigned.
- ☐ Accountability assigned and KPIs established.
- ☐ Accountability assigned with KPIs and tasks regularly reviewed and adapted.
- ☐ Not applicable.



Add explanation:  Ask a question about this control:  Evidence: 

Control ID: C0158

Procurement

Are all cloud services sourced through the Procurement Team?

- ☐ No restriction for procuring cloud services.
- ☐ Most cloud services procured centrally.
- ☐ All cloud services procured centrally.
- ☐ All cloud services procured centrally and monitoring for other cloud services used.
- ☐ All cloud services procured centrally and other procurement channels actively prevented.
- ☐ Not applicable.




Add explanation:  Ask a question about this control:  Evidence: 

Control ID: C0159

Authentication

Are all cloud services integrated with the organisation's directory services and identity management to avoid separate credentials for cloud services as much as possible?

- ☐ No integration.
- ☐ Some cloud services integrated or logins limited to the organisation's domain.
- ☐ All cloud services integrated with directory.
- ☐ All cloud services managed through the organisation's identity directory.
- ☐ All cloud services integrated with directory and single sign-on enabled.
- ☐ Not applicable.




Add explanation:  Ask a question about this control:  Evidence: 

Control ID: C0164

Preferred Suppliers

Does the Procurement Team define preferred suppliers from a list of all current vendors for the organisation's goods and services based on financial optimisation (e.g. volume discounts), strategic sourcing priorities and vendor risk minimisation?

- ☐ No preferred suppliers defined.
- ☐ Informal procurement from small number of suppliers.
- ☐ Preferred suppliers defined.
- ☐ Preferred suppliers defined and frame contracts established.
- ☐ Preferred suppliers with frame contracts defined and implemented in purchasing system.
- ☐ Not applicable.




Add explanation:  Ask a question about this control:  Evidence: 

Control ID: C0629

Independence

Are employees prohibited from accepting inappropriate material benefits from a vendor and required to maintain their independence?

- ☐ No restriction.
- ☐ Ethical behaviour expected.
- ☐ Conflict of interest management defined.
- ☐ Conflict of interest check performed for each person with purchasing power.
- ☐ Conflict of interest checks performed and regular mandatory independence trainings.
- ☐ Not applicable.




Add explanation:  Ask a question about this control:  Evidence: 

Control ID: C0641

Linkage to Control Statements

Is each risk aligned to a defined control statement where applicable?

- ☐ No alignment.
- ☐ Some risks aligned.
- ☐ Formal alignment to internal controls.
- ☐ Risk management system linked to Internal Controls System.
- ☐ Linkage to control statements regularly reviewed.
- ☐ Not applicable.

Add explanation:  Ask a question about this control:  Evidence: 

Control ID: C0716