G4. Review information security policies regarding strategic partners and other third-parties

Metrics	*0-100*
B Percentage of strategic partner and other third-party relationships for which information security requirements have been implemented in the agreements with these parties	

G5. Strive to ensure business continuity

Metrics	*0-100*
B Percentage of organizational units with an established business continuity plan	

G6. Review provisions for internal and external audits of the Information security program

Metrics	*0-100*
B Percentage of required internal and external audits completed and reviewed by the Board	
B Percentage of audit findings that have been resolved	

G7. Collaborate with management to specify the information security metrics to be reported to the board

No metrics are yet associated with this area.

7.3.2.7.2 Management

M8. Establish information security management policies and controls and monitor compliance

Metrics	*0-100*
B Percentage of Information Security Program Elements for which approved policies and controls are currently operational	
BS Percentage of staff assigned responsibilities for information security policies and controls who have acknowledged accountability for their responsibilities in connection with those policies and controls	
B Percentage of information security policy compliance reviews with no violations noted	
Percentage of business unit heads and senior managers who have implemented operational procedures to ensure compliance with approved information security policies and controls	

M9. Assign information security roles, responsibilities, required skills, and enforce role-based information access privileges

Metrics	*0-100*
BS Percentage of new employees hired this reporting period who satisfactorily completed security awareness training before being granted network access	
BS Percentage of employees who have satisfactorily completed periodic security awareness refresher training as required by policy	
Percentage of position descriptions that define the information security roles, responsibilities, skills, and certifications for Security Managers and Administrators	
Percentage of position descriptions that define the information security roles, responsibilities, skills, and certifications for IT personnel	
Percentage of position descriptions that define the information security roles, responsibilities, skills, and certifications for general staff system users	
Percentage of job performance reviews that include evaluation of information security responsibilities and information security policy compliance	
BS Percentage of user roles, systems, and applications that comply with the separation of duties principle	
B Percentage of individuals with access to security software who are trained and authorized security administrators	
B Percentage of individuals who are able to assign security privileges for systems and applications who are trained and authorized security administrators	
B Percentage of employees with high level system and application privileges whose access privileges have been reviewed this reporting period	
BS Percentage of terminated employees whose access privileges have been reviewed this reporting period	
Percentage of users who have undergone background checks	

M10. Assess information risks, establish risk thresholds and actively manage risk mitigation

Metrics	*0-100*
BS Percentage of critical information assets and information-dependent functions for which some form of risk assessment has been performed and documented as required by policy	

Metrics	***0-100***
Percentage of critical assets and functions for which the cost of compromise (loss, damage, disclosure, disruption in access to) has been quantified	
BS Percentage of identified risks that have a defined risk mitigation plan against which status is reported in accordance with policy	

M11. Ensure implementation of information security requirements for strategic partners and other third-parties

Metrics	***0-100***
Percentage of known information security risks that are related to third-party relationships	
BS Percentage of critical information assets or functions for which access by third-party personnel is not allowed	
BS Percentage of third-party personnel with current information access privileges who have been reviewed by designated authority to have continued need for access in accordance with policy	
BS Percentage of systems with critical information assets or functions for which electronic connection by third-party systems is not allowed	
Percentage of security incidents that involved third-party personnel	
Percentage of third-party agreements that include/demonstrate external verification of policies and procedures	
BS Percentage of third-party relationships that have been reviewed for compliance with information security requirements	
Percentage of out-of-compliance review findings that have been corrected since the last review	

M12. Identify and classify information assets

Metrics	***0-100***
BS Percentage of information assets that have been reviewed and classified by the designated owner in accordance with the classification scheme established by policy	
Percentage of information assets with defined access privileges that have been assigned based on role and in accordance with policy	
Percentage of scheduled asset inventories that occurred on time according to policy	

M13. Implement and test business continuity plans

Metrics	***0-100***
B Percentage of organizational units with a documented business continuity plan for which specific responsibilities have been assigned	
B Percentage of business continuity plans that have been reviewed, exercised/tested, and updated in accordance with policy	

M14. Approve information systems architecture during acquisition, development, operations, and maintenance

Metrics	***0-100***
Percentage of information security risks related to systems architecture identified in the most recent risk assessment that have been adequately mitigated.	
B Percentage of system architecture changes (additions, modifications, or deletions) that were reviewed for security impacts, approved by appropriate authority, and documented via change request forms	
Percentage of critical information assets or functions residing on systems that are currently in compliance with the approved systems architecture	

M15. Protect the physical environment

Metrics	***0-100***
BS Percentage of critical organizational information assets and functions that have been reviewed from the perspective of physical risks such as controlling physical access and physical protection of backup media	
Percentage of critical organizational information assets and functions exposed to physical risks for which risk mitigation actions have been implemented	
BS Percentage of critical assets that have been reviewed from the perspective of environmental risks such as temperature, fire, flooding, etc.	
Percentage of servers in locations with controlled physical access	

M16. Ensure internal and external audits of the information security program with timely follow-up

Metrics	***0-100***
B Percentage of information security requirements from applicable laws and regulations that are included in the internal/external audit program and schedule	

Metrics	*0-100*
B Percentage of information security audits conducted in compliance with the approved internal/external audit program and schedule	
B Percentage of management actions in response to audit findings / recommendations that were implemented as agreed as to timeliness and completeness	

M17. Collaborate with security staff to specify the information security metrics to be reported to management

No metrics are provided for this area.

7.3.2.7.3 Technical

T18. User identification and authentication

Metrics	*0-100*
BS Number of active user IDs assigned to only one person	
BS Percentage of systems and applications that perform password policy verification	
BS Percentage of active user passwords that are set to expire in accordance with policy	
Percentage of systems with critical information assets that use stronger authentication than IDs and passwords in accordance with policy	

T19. Account management

Metrics	*0-100*
BS Percentage of systems where vendor-supplied accounts and passwords have been disabled or reset	
BS Percentage of computer user accounts assigned to personnel who have left the organization or no longer have need for access that have been closed	
B Percentage of systems with account lockout parameters set in accordance with policy	
Percentage of inactive user accounts that have been disabled in accordance with policy	
BS Percentage of workstations with session time-out/automatic logout controls set in accordance with policy	

T20. User privileges

Metrics	*0-100*
B Percentage of active computer accounts that have been reviewed for justification of current access privileges in accordance with policy	

Metrics	***0-100***
BS Percentage of systems where permission to install non-standard software is limited in accordance with policy	
Percentage of systems and applications where assignment of user privileges is in compliance with the policy that specifies role-based information access privileges	

T21. Configuration management

Metrics	***0-100***
Percentage of systems for which approved configuration settings have been implemented as required by policy	
BS Percentage of systems with configurations that do not deviate from approved standards	
BS Percentage of systems that are continuously monitored for configuration policy compliance with out-of-compliance alarms or reports	
Percentage of systems whose configuration is compared with a previously established trusted baseline in accordance with policy	
B Percentage of systems where the authority to make configuration changes is limited in accordance with policy	

T22. Event and activity logging and monitoring

Metrics	***0-100***
B Percentage of systems for which event and activity logging has been implemented in accordance with policy	
BS Percentage of systems for which event and activity logs are monitored and reviewed in accordance with policy	
Percentage of systems for which log size and retention duration have been implemented in accordance with policy	
B Percentage of systems that generate warnings about anomalous or potentially unauthorized activity	

T23. Communications, email, and remote access security

Metrics	***0-100***
BS Percentage of notebooks and mobile devices that are required to verify compliance with approved configuration policy prior to being granted network access	
Percentage of communications channels controlled by the organization that have been secured in accordance with policy	

Metrics	***0-100***
Percentage of host servers that are protected from becoming relay hosts	
Percentage of mobile users who access enterprise facilities using secure communications methods	

T24. Malicious code protection, including viruses, worms, and Trojans

Metrics	***0-100***
BS Percentage of workstations (including notebooks) with automatic protection in accordance with policy	
BS Percentage of servers with automatic protection in accordance with policy	
BS Percentage of mobile devices with automatic protection in accordance with policy	

T25. Software change management, including patching

Metrics	***0-100***
BS Percentage of systems with the latest approved patches installed	
Mean time from vendor patch availability to patch installation by type of technology environment Note: A lower value is desirable.	
B Percentage of software changes that were reviewed for security impacts in advance of installation	

T26. Firewalls

Metrics	***0-100***
BS Percentage of workstation firewalls, host firewalls, sub-network firewalls, and perimeter firewalls configured in accordance with policy	

T27. Data encryption

Metrics	***0-100***
B Percentage of critical information assets stored on network accessible devices that are encrypted with widely tested and published cryptographic algorithms	
BS Percentage of mobile computing devices using encryption for critical information assets in accordance with policy	
Percentage of passwords and PINS that are encrypted (cryptographically one-way hashed) in accordance with policy	

T28. Backup and recovery

Metrics	*0-100*
BS Percentage of systems with critical information assets or functions that have been backed up in accordance with policy	
BS Percentage of systems with critical information assets or functions where restoration from a stored backup has been successfully demonstrated	
BS Percentage of backup media stored off-site in secure storage	
Percentage of used backup media sanitized prior to reuse or disposal	

T29. Incident and vulnerability detection and response

Metrics	*0-100*
B Percentage of operational time that critical services were unavailable (as seen by users and customers) due to security incidents. A lower value is desirable.	
BS Percentage of security incidents that exploited existing vulnerabilities with known solutions, patches, or workarounds. A lower value is desirable.	
Percentage of systems affected by security incidents that exploited existing vulnerabilities with known solutions, patches, or workarounds. A lower value is desirable.	
BS Percentage of security incidents that were managed in accordance with established policies, procedures, and processes	
BS Percentage of systems with critical information assets or functions that have been assessed for vulnerabilities in accordance with policy	
BS Percentage of vulnerability assessment findings that have been addressed since the last reporting period	

T30. Collaborate with management to specify the technical metrics to be reported to management

No metrics are specified for this area.

There are no baselines for this metric because it was only just created.