ISO 27001 Metrics

MINISTRY OF SECURITY

Chief Information Security Officer (CISO) plays a crucial role in ensuring the effectiveness of an information security program. To achieve this, they can track several key metrics that provide insights into the program's performance and its alignment with business goals.

Metric	Objective	Measurement Criteria
Patch Management	To ensure timely patching of critical vulnerabilities to minimize the risk of exploitation.	(Number of critical vulnerabilities patched on time / Total number of critical vulnerabilities) * 100.
Phishing Resilience	To assess the effectiveness of security awareness training and employee awareness.	(Number of employees not clicking on simulated phishing emails / Total number of employees) * 100.
Incident Response	To minimize the impact of security incidents by responding swiftly.	Total time taken to respond to incidents / Number of incidents.
User Access Review	To ensure timely review and revocation of unnecessary access rights.	(Number of user access reviews completed on time / Total number of user access reviews) * 100.
Security Awareness	To ensure all employees receive essential security education.	(Number of employees completing training / Total number of employees) * 100.
Vulnerability Management	To reduce the window of opportunity for attackers to exploit vulnerabilities.	Total time taken to remediate vulnerabilities / Number of vulnerabilities.

ISO 27001 Metrics

MINISTRY OF SECURITY

Remember that these metrics should be tailored to the specific goals and needs of your organization. Regularly reviewing and analyzing these metrics will provide insights into the effectiveness of your information security program and help you to enhance your organization's security posture.

Metric	Objective	Measurement Criteria
Risk Assessment	To identify and prioritize security risks and track the progress of risk mitigation efforts.	(Number of risks treated / Total number of risks identified) * 100
Firewall Rule Review	To determine how often firewall rules are reviewed and updated to ensure alignment with security	(Number of Firewall Rule Reviews) / (Time Period, e.g., Quarterly)
Antivirus Management	To measures the proportion of systems protected by the antivirus software out of the total systems.	(Number of Systems Protected by Antivirus / Total Number of Systems) * 100
Change Management	Measure the effectiveness of changes to the organization's IT environment.	(Number of successful changes / Total number of changes) * 100
Legal Compliance	Ensure the organization's adherence to relevant laws, regulations, and industry standards.	(Number of compliant controls / Total number of applicable controls) * 100
InfoSec Program	Measure the progress and success of various security initiatives and projects.	(Number of completed projects / Total number of projects) * 100