ISO 27001:2022 KPI Metrics

DOCUMENT CLASSIFICATION	Internal
VERISON	1.0
DATE	
DOCUMENT AUTHOR	**Ayaz Sabir**
DOCUMENT OWNER	

REVISION HISTORY

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES

DISTRIBUTION LIST

NAME	SUMMARY OF CHANGE

APPROVAL

NAME	POSITION	SIGN

Contents

1. Introduction

1.1 Purpose

This KPI framework is designed to help organizations measure the effectiveness of their ISMS and demonstrate continuous improvement in information security performance. The metrics align with ISO/IEC 27001:2022 requirements for monitoring, measurement, analysis, and evaluation.

1.2 Scope

This framework covers KPIs for all aspects of the ISMS including:

- Security control effectiveness
- Risk management performance
- Incident management efficiency
- Compliance and audit results
- Training and awareness effectiveness
- Business continuity and resilience
- Supplier and third-party security

1.3 KPI Categories

The KPIs are organized into the following categories:

1. **Strategic KPIs** - High-level organizational security performance
2. **Operational KPIs** - Day-to-day security operations effectiveness
3. **Tactical KPIs** - Specific security control and process performance
4. **Compliance KPIs** - Regulatory and standard compliance metrics

2. Strategic KPIs

2.1 ISMS Effectiveness Metrics

KPI Name	Description	Formula	Target	Frequency	Owner
ISMS Maturity Score	Overall maturity assessment of ISMS implementation	(Sum of control maturity scores / Total possible score) × 100	≥ 85%	Quarterly	CISO
Security Investment ROI	Return on investment for security initiatives	(Security benefits - Security costs) / Security costs × 100	≥ 15%	Annually	CFO/ CISO
Risk Reduction Rate	Percentage reduction in overall risk exposure	(Previous risk score - Current risk score) / Previous risk score × 100	≥ 10% annually	Quarterly	Risk Manager
Security Objective Achievement	Percentage of security objectives met	(Objectives achieved / Total objectives) × 100	≥ 90%	Quarterly	CISO
Stakeholder Satisfaction	Satisfaction level of key stakeholders with security posture	Average satisfaction score from surveys	≥ 4.0/5.0	Semi-annually	CISO

2.2 Business Impact Metrics

KPI Name	*Description*	*Formula*	*Target*	*Frequency*	*Owner*
Security-Related Downtime	Total downtime caused by security incidents	Sum of incident-related downtime hours	< 8 hours /year	Monthly	IT Operations
Business Continuity Test Success Rate	Percentage of successful BCP tests	(Successful tests / Total tests) × 100	≥ 95%	Quarterly	BCP Manager
Customer Trust Index	Customer confidence in organization's security	Customer survey results on security confidence	≥ 4.2/5.0	Semi-annually	Customer Relations
Regulatory Compliance Score	Overall compliance with applicable regulations	(Compliant requirements / Total requirements) × 100	100%	Quarterly	Compliance Officer

3. Operational KPI's

3.1 Incident Management Metrics

KPI Name	*Description*	*Formula*	*Target*	*Frequency*	*Owner*
Mean Time to Detect (MTTD)	Average time to detect security incidents	Sum of detection times/ Number of incidents	< 4 hours	Monthly	SOC Manager
Mean Time to Respond (MTTR)	Average time to respond to security incidents	Sum of response times / Number of incidents	< 24 hours	Monthly	Incident Manager
Mean Time to Recover (MTTR)	Average time to recover from security incidents	Sum of recovery times / Number of incidents	< 72 hours	Monthly	Incident Manager
Incident Recurrence Rate	Percentage of incidents that recur	(Recurring incidents / Total incidents) × 100	< 5%	Monthly	Incident Manager
False Positive Rate	Percentage of false security alerts	(False positives / Total alerts) × 100	< 15%	Weekly	SOC Manager
Security Incident Trend	Month-over-month change in incident volume	((Current month - Previous month) / Previous month) × 100	Decreasing trend	Monthly	CISO

3.2 Vulnerability Management Metrics

KPI Name	*Description*	*Formula*	*Target*	*Frequency*	*Owner*
Critical Vulnerability Remediation Time	Average time to remediate critical vulnerabilities	Sum of remediation times / Number of critical vulnerabilities	< 72 hours	Weekly	IT Security
High Vulnerability Remediation Time	Average time to remediate high vulnerabilities	Sum of remediation times / Number of high vulnerabilities	< 7 days	Weekly	IT Security
Vulnerability Scan Coverage	Percentage of assets scanned for vulnerabilities	(Scanned assets / Total assets) × 100	≥ 95%	Weekly	IT Security
Patch Management Compliance	Percentage of systems with current patches	(Patched systems / Total systems) × 100	≥ 95%	Weekly	IT Operations
Zero-Day Response Time	Time to implement protection against zero-day threats	Time from threat disclosure to protection implementation	< 24 hours	Per-incident	IT Security

3.3 Access Control Metrics

KPI Name	*Description*	*Formula*	*Target*	*Frequency*	*Owner*
Privileged Account Review Compliance	Percentage of privileged accounts reviewed on schedule	(Reviewed accounts / Total privileged accounts) × 100	100 %	Monthly	Identity Manager
Access Request Processing Time	Average time to process access requests	Sum of processing times / Number of requests	< 4 hours	Weekly	Identity Manager
Orphaned Account Detection Rate	Percentage of orphaned accounts identified and removed	(Removed orphaned accounts / Total orphaned accounts) × 100	≥ 95%	Monthly	Identity Manager
Multi-Factor Authentication Adoption	Percentage of users using MFA	(MFA users / Total users) × 100	≥ 98%	Monthly	IT Security
Password Policy Compliance	Percentage of passwords meeting policy requirements	(Compliant passwords / Total passwords) × 100	≥ 95%	Monthly	IT Security

4. Tactical KPI's

4.1 Security Control Effectiveness

KPI Name	*Description*	*Formula*	*Target*	*Frequency*	*Owner*
Firewall Rule Effectiveness	Percentage of firewall rules actively used	(Active rules / Total rules) × 100	≥ 80%	Monthly	Network Security
Antimalware Detection Rate	Percentage of malware detected and blocked	(Detected malware / Total malware attempts) × 100	≥ 99%	Weekly	Endpoint Security
Email Security Effectiveness	Percentage of malicious emails blocked	(Blocked malicious emails / Total	≥ 99.5%	Weekly	Email Security
Data Loss Prevention Effectiveness	Percentage of data exfiltration attempts blocked	(Blocked attempts / Total attempts) × 100	≥ 95%	Weekly	DLP Manager
Backup Success Rate	Percentage of successful backup operations	(Successful backups / Total backup attempts) × 100	≥ 99%	Daily	Backup Administrator

4.2 Security Monitoring Metrics

KPI Name	Description	Formula	Target	Frequency	Owner
Log Collection Rate	Percentage of systems sending logs to SIEM	(Systems sending logs / Total systems) × 100	≥ 98%	Daily	SOC Manager
Security Event Correlation Rate	Percentage of events successfully correlated	(Correlated events / Total events) × 100	≥ 85%	Weekly	SOC Manager
Threat Intelligence Integration	Percentage of threat feeds integrated and active	(Active feeds / Total feeds) × 100	≥ 90%	Weekly	Threat Intelligence
Security Dashboard Availability	Uptime of security monitoring dashboards	(Dashboard uptime / Total time) × 100	≥ 99.5%	Daily	SOC Manager

5. Compliance KPI's

5.1 Audit and Assessment Metrics

KPI Name	Description	Formula	Target	Frequency	Owner
Internal Audit Findings	Number of findings per internal audit	Total findings / Number of audits	< 10 per audit	Per audit	Internal Auditor
Audit Finding Closure Rate	Percentage of audit findings closed on time	(Closed on time / Total findings) × 100	≥ 95%	Monthly	Compliance Officer

External Audit Success Rate	Percentage of external audits passed without major findings	(Passed audits / Total audits) × 100	100%	Per audit	CISO
Control Testing Results	Percentage of controls passing testing	(Passed controls / Total controls tested) × 100	≥ 95%	Quarterly	Internal Auditor
Compliance Gap Remediation	Average time to remediate compliance gaps	Sum of remediation times / Number of gaps	< 30 days	Monthly	Compliance Officer

5.2 Training and Awareness Metrics

KPI Name	*Description*	*Formula*	*Target*	*Frequency*	*Owner*
Security Training Completion Rate	Percentage of employees completing mandatory training	(Completed training / Total employees) × 100	≥ 98%	Quarterly	HR/Training
Security Awareness Test Scores	Average score on security awareness assessments	Sum of scores / Number of participants	≥ 85%	Quarterly	Training Manager
Phishing Simulation Click Rate	Percentage of employees clicking phishing simulation emails	(Clicks / Total emails sent) × 100	< 5%	Monthly	IT Security
Security Incident Reporting	Number of security incidents reported by	Count of employee-reported incidents	Increasing trend	Monthly	CISO

Rate	employees				
Training Effectiveness Score	Improvement in security behavior post-training	(Post-training score - Pre-training score) / Pre-training score × 100	≥ 20% improvement	Quarterly	Training Manager

6. Risk Management KPI's

6.1 Risk Assessments and Treatment

KPI Name	*Description*	*Formula*	*Target*	*Frequency*	*Owner*
Risk Assessment Coverage	Percentage of assets covered by risk assessments	(Assessed assets / Total assets) × 100	100%	Quarterly	Risk Manager
High Risk Remediation Rate	Percentage of high risks remediated within SLA	(Remediated high risks / Total high risks) × 100	≥ 95%	Monthly	Risk Manager
Risk Treatment Plan Completion	Percentage of risk treatment actions completed on time	(Completed actions / Total actions) × 100	≥ 90%	Monthly	Risk Manager
Residual Risk Acceptance Rate	Percentage of residual risks formally accepted	(Accepted risks / Total residual risks) × 100	< 10%	Quarterly	Risk Manager
Risk Register Currency	Percentage of risk register entries updated within timeframe	Updated entries / Total entries) × 100	≥ 95%	Monthly	Risk Manager

7. Third-Party and Supplier KPI's

7.1 Supplier Security Management

KPI Name	*Description*	*Formula*	*Target*	*Frequency*	*Owner*
Supplier Security Assessment Rate	Percentage of suppliers assessed for security	(Assessed suppliers / Total suppliers) × 100	100%	Annually	Procurement
Supplier Compliance Rate	Percentage of suppliers meeting security requirements	(Compliant suppliers / Total suppliers) × 100	≥ 95%	Quarterly	Procurement
Third-Party Incident Rate	Number of security incidents involving third parties	Count of third- party incidents	< 2 per quarter	Quarterly	Risk Manager
Vendor Risk Score	Average risk score of all vendors	Sum of vendor risk scores / Number of vendors	< 3.0 (1-5 scale)	Quarterly	Risk Manager

8. Business Continuity KPI's

8.1 Continuity and Recovery Metrics

KPI Name	*Description*	*Formula*	*Target*	*Frequency*	*Owner*
Recovery Time Objective (RTO) Achievement	Percentage of systems meeting RTO requirement	(Systems meeting RTO / Total critical systems) x 100	100%	Per-test	BCP Manager
Recovery Point Objective (RPO) Achievement	Percentage of systems meeting RPO requirements	(Systems meeting RPO / Total critical systems) × 100	100%	Per-test	BCP Manager
Business Continuity Test Success Rate	Percentage of BCP tests meeting success criteria	(Successful tests / Total tests) × 100	≥ 95%	Per-test	BCP Manager
Disaster Recovery Drill Frequency	Number of DR drills conducted per year	Count of DR drills	≥ 4 per year	Quarterly	BCP Manager

9. KPI Implementation Guidelines

9.1 KPI Selection Criteria

When selecting KPIs for your organization, consider:

- **Relevance**: Aligns with business objectives and security goals
- **Measurability**: Can be quantified and tracked consistently
- **Actionability**: Provides insights that lead to actionable improvements
- **Timeliness**: Available when needed for decision-making
- **Cost-effectiveness**: Benefits of measurement outweigh costs

9.2 KPI Measurement Process

1. **Define baseline**: Establish current performance levels
2. **Set targets**: Define realistic but challenging targets
3. **Collect data**: Implement automated collection where possible
4. **Analyze trends**: Look for patterns and anomalies
5. **Report results**: Communicate findings to stakeholders
6. **Take action**: Implement improvements based on insights

9.3 KPI Dashboard Design

Effective KPI dashboards should include:

- **Executive summary**: High-level metrics for leadership
- **Operational details**: Detailed metrics for operational teams
- **Trend analysis**: Historical data and trend indicators
- **Alert mechanisms**: Notifications for threshold breaches
- **Drill-down capability**: Ability to investigate underlying data

10. KPI Reporting Framework

10.1 Reporting Frequency and Audience

Report Type	*Frequency*	*Audience*	*Key Metrics*
Executive Dashboard	Weekly	C-Suite, Board	Strategic KPIs, Major incidents, Compliance status
Management Report	Monthly	Department heads	Operational KPIs, Trend analysis, Action items
Operational Report	Daily/Weekly	Security teams	Tactical KPIs, Alerts, Performance metrics
Compliance Report	Quarterly	Auditors, Regulators	Compliance KPIs, Audit results, Remediation status
		All stakeholders	Year-over-year

Annual Review	Annually		trends, Achievements, Strategic planning

10.2 KPI Review and Improvement

- **Monthly reviews**: Assess KPI performance and identify issues
- **Quarterly assessments**: Evaluate KPI relevance and effectiveness
- **Annual reviews**: Update to KPI framework based on business changes
- **Continuous improvement**: Refine metrics based on lessons learned

11. Technology and Tools

11.1 KPI Measurement Tools

- **SIEM platforms**: For security event and incident metrics
- **GRC tools**: For compliance and risk management KPIs
- **Business intelligence tools**: For dashboard creation and reporting
- **Automated monitoring**: For real-time metric collection
- **Survey platforms**: For stakeholder satisfaction metrics

11.2 Data Sources

- **Security tools**: Firewalls, IDS/IPS, antimalware, DLP
- **IT systems**: Asset management, patch management, backup systems
- **HR systems**: Training records, employee data
- **Business systems**: Incident management, change management
- **External sources**: Threat intelligence, compliance databases