



Monitoring and Measurement Standard



Table of contents

Change History	2
1. Purpose, scope and Users	5
2. Compliance and exceptions	5
3. Objectives	5
4. Monitoring and logging	6
4.1. Clock synchronization	7
4.2. Usage and capacity of critical assets	7
4.3. Security monitoring and threat intelligence programs	7
4.4. Controls monitoring	8
4.5. Risk monitoring	8
4.6. Compliance monitoring	9
4.7. Threat and file integrity monitoring	10
4.8. Organizational structure	11
5. Corrective action	11
5.1. Root Cause Analysis	11
5.2. Corrective Action Plan	11
5.3. Implementation and monitoring	12
5.4. Verification of effectiveness	12
5.5. Record keeping	12
5.6. Continuous improvement	12
6. Reporting	12
7. Measurement and metrics	13
7.1. Measurement metrics	14
8. Roles and responsibilities pertaining to this Standard	15
9. Definitions	17
10. Related documents	18
11. Validity and standard management	19
Appendix A: Example measurement metrics	20
A. Occupational health and safety	20
B. Policy, standards, and controls	20
C. Security roles and responsibilities	20
D. Role-based information access	21
E. Information risk threshold	21
F. Supply chain information assurance	21



G. Identification and classification of information assets	21
H. Information systems architecture	22
I. Physical environment	22
J. Privacy	22
K. Environmental management	22
L. Artificial intelligence	23
M. Key stakeholders	23
N. Business Continuity	23
O. Risk management	24
P. Information Security	24
Q. Technical measurement	24
User identification and authentication	24
User account management	24
User and administrator privilege management	25
Configuration management	25
Security Information and Event Management	25
Communications, e-mail, and remote access security management	25
Malicious code protection management	25
Software change management	26
Network management and firewall management	26
Data encryption management	26
Backup management and recovery management	26
Incident management and vulnerability management	26
R. Service management	27