



Operational Management Standard

Table of contents

Change History	2
1. Purpose, scope and Users	6
2. Compliance and exceptions	6
3. Objectives	6
4. Leadership and commitment	7
5. Operating procedures	8
6. Asset management	8
6.1. Asset types	9
6.2. Asset inventory	10
6.3. Software management	10
7. Change management	11
7.1. Emergency changes	12
7.2. Normal changes	13
7.3. Standard changes	13
8. Capacity management	14
8.1. Capacity management plan	14
8.1.1. Capacity planning baseline	14
8.1.2. Future system capacity forecasting	14
8.1.3. IT resource availability alignment	15
8.1.4. Denial of Service (DoS) mitigation	15
8.1.5. Network redundancy implementation	15
8.1.6. System workload forecasting	15
8.1.7. Workload forecasting tools	15
8.1.8. Resource capacity management controls	15
8.1.9. System capacity testing	15
8.1.10. System performance reviews	16
8.1.11. Resource Workload Scheduling	16
9. Cloud service management	16
9.1. Cloud network management	16
9.2. Client protection	16
9.3. Geographic location and legal jurisdiction	17
9.4. Cloud service agreements	17
9.5. Cloud management procedures	17
9.6. Cloud service usage standard	18

9.7. Migration strategy	18
9.8. Monitoring and communication	18
9.9. Exiting cloud services	18
10. Governance, Risk, and Compliance	19
10.1. Governance framework	19
10.2. Risk Management framework	19
10.3. Compliance framework	20
10.4. Communication and dissemination	20
10.5. Technology integration and evaluation	20
10.6. Internal control framework	20
10.7. Compliance and Cybersecurity	21
10.8. Accountability and ownership	21
10.9. Continuous improvement and monitoring	22
10.10. Non-compliance and consequences	22
11. Service management	22
11.1. Service requirements and change management	23
11.2. Risk and continuity management	23
11.3. Service delivery and improvement	23
12. Network management	23
13. AI management	25
13.1. AI policy and communication	25
13.2. AI objectives	25
13.3. AI Risk Management	26
13.4. AI system development and deployment	26
13.5. Compliance and ethical considerations	26
13.6. Human oversight and control	26
13.7. AI compliance and termination	26
13.8. AI documentation and transparency	27
13.9. Continuous improvement	27
14. Incident management	27
14.1. Responsibilities and procedures	27
14.2. Reporting incidents	28
14.3. Reporting weaknesses	28
14.4. Assessment of and decision on events	28
14.5. Response to incidents	29

14.6. Learning from incidents	29
14.7. Collection of evidence	29
14.7.1. Threat intelligence	30
15. Accessibility management	30
15.1. Content accessibility	31
15.2. Telecommunications and technology accessibility	31
15.3. User interface and navigation	31
15.4. Accessibility in media content	32
15.5. Input and control mechanisms	32
15.6. Time-based and interactive content	32
16. Environmental management	32
16.1. Requirements	33
16.2. Environmental aspects and impacts	33
16.3. Environmental objectives	33
16.4. Environmental performance monitoring	34
16.5. Communication and dissemination	34
16.6. Compliance and Continuous Improvement	34
17. Roles and responsibilities pertaining to this Standard	34
18. Related documents	38
19. Validity and standard management	38