Appendix C: Best Practices Mapped to Standards

Table 1: Best Practices Mapped to Standards

Practice Number	Best Practice	NIST Controls	CERT-RMM	ISO 27002
1	Consider threats from insiders and business partners in enterprise-wide risk assessments.	RA-1, RA-3, PM-9	· External Dependencies Management · Human Resources Management · Access Control and Management	· Identification of risks related to external parties · Addressing security when dealing with customers · 6.2.3 Addressing security in third party agreements
2	Clearly document and consistently enforce policies and controls.	PL-1, PL-4, PS-8	· Compliance	· 15.2.1 Compliance with security policies and standards
3	Incorporate insider threat awareness into periodic security training for all employees.	AT-1, AT-2, AT-3	· Organizational Training and Awareness	· 8.2.2 Information security awareness, education, and training
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	PS-1, PS-2, PS-3, PS-8	· Monitoring · Human Resources	· 8.1.2 Screening
5	Anticipate and manage negative issues in the work environment.	PL-4, PS-1, PS-6, PS-8	· Human Resources · HRM:SG3.SP4 Establish Disciplinary Process	· 8.2.1 Management responsibilities · 8.2.3 Disciplinary process · 8.3.1 Termination responsibilities
6	Know your assets.	CM-2, CM-8, PM-5, RA-2	· Asset Definition and Management · Enterprise Focus	· 7.1.1 Inventory of assets
7	Implement strict password and account management policies and practices.	AC-2, IA-2	· Identity/Access Management	· 11.2.3 User password management · 11.2.4 Review of user access rights
8	Enforce separation of duties and least privilege.	AC-5, AC-6	· Access Management	· 10.1.3 Segregation of duties · 11.2.2 Privilege management
9	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.	AC-ALL, AU-ALL, RA-ALL, SC-ALL, SA-ALL	· External Dependencies Management	· Identification of risks related to external parties · Addressing security in third party agreements · 10.2.1 Service delivery · 10.2.2 Monitoring and review of third party services · 10.2.3 Managing changes to third party services

Practice Number	Best Practice	NIST Controls	CERT-RMM	ISO 27002
10	Institute stringent access controls and monitoring policies on privileged users.	AC-2, AC-6, AC-17, AU-2, AU-3, AU-6, AU-9, CM-5, IA-2, MA-5, PL-4, SA-5	· Identity/Access Management · Monitoring	· 10.10.4 Administrator and operator logs · 10.10.2 Monitoring system use
11	Institutionalize system change controls.	CM-1, CM-3, CM-4, CM-5, CM-6	· Technology Management · TM:SG4.SP3 Perform Change Control and Management	· 10.1.2 Change management
12	Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.	AU-1, AU-2, AU-6, AU-7, AU-12	· Monitoring	· 10.10.1 Audit logging · 10.10.2 Monitoring system use
13	Monitor and control remote access from all end points, including mobile devices.	AC-2, AC-17	· Technology Management · TM:SG2.SP2 Establish and Implement Controls	· 11.4.2 User authentication for external connections · 11.7.1 Mobile computing and communications
14	Develop a comprehensive employee termination procedure.	PS-4, PS-5	· Human Resources	· 8.3.1 Termination responsibilities · 8.3.2 Return of assets · 8.3.3 Removal of access rights
15	Implement secure backup and recovery processes.	CP-6, CP-9, CP-10	· Knowledge and Information Management · KIM:SG6.SP1 Perform Information Duplication and Retention	· 10.5.1 Information back-up
16	Develop a formalized insider threat program.	AU-6, IR-4, SI-4	· Incident Management and Control · Vulnerability Analysis and Resolution	· 6.1.2 Information security coordination · 15.1.5 Prevention of misuse of information processing facilities
17	Establish a baseline of normal network device behavior.	AC-17, CM-7, SC-7	· Monitoring	
18	Be especially vigilant regarding social media.	AT-2, AT-3	· Monitoring	
19	Close the doors to unauthorized data exfiltration.	AC-20, CA-3, CM-7, MP-2, MP-3, MP-5, PE-5, SC-7	· Technology Management · TM:SG2 Protect Technology Assets	· 12.5.4 Information leakage