

Controls Review

Uma M

Media	Label	Asset Name(s)	Threat Source/Threat Event	Vulnerability	Control	NIST Family	NIST Family ID	Global	Media
Pager		Pager Media	System Cracker/Theft of Sensitive Data	System Configuration Deficiencies	Change Control Processes			Yes	Yes
Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	User Authentication Deficiencies	Accounts Lock After Too Many Failed Logins			TBD	In progress
Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	System Configuration Deficiencies	Change Control Processes			Yes	Yes
Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	Physical Security Deficiencies	Physical Access Authorization			Yes	Yes
Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	Insecure Network Configuration	Auto Logoff or Auto Screen Locking			No	No
Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	Insecure Network Configuration	Authentication of Network Sessions (as Distinct From Users)			In progress	In progress
Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	Custom Application Weaknesses	Application Penetration and Vulnerability Testing			Yes	Yes
Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	Custom Application Weaknesses	Application Code Review			In progress	In progress
Laptop		TestingAsset	System Cracker/Insecure User Management	Dormant Accounts	Access Logging			Yes	Yes
Laptop		TestingAsset	System Cracker/Denial of Service	Insufficient Application/Network Capacity	Capacity Planning			In progress	In progress
Laptop		TestingAsset	Power Surge/Electrical Damage to Equipment	Insufficient Power Shielding	Data Backup			No	No
Laptop		TestingAsset	Malware/Theft of Sensitive Data	Anti-malware Deficiencies	Central Monitoring of Endpoint Protection Software			No	No
Laptop		TestingAsset	Malware/Theft of Sensitive Data	Anti-malware Deficiencies	Anti-virus Policy and Procedures			N/A	N/A
Laptop		TestingAsset	Malware/Theft of Sensitive Data	Anti-malware Deficiencies	Anti-Malware Software			No	No
Laptop		TestingAsset	Malicious User/Malicious Use of Sensitive Data	Endpoint Leakage	Acceptable Use Policy			Yes	Yes
Laptop		TestingAsset	Careless User/Installation of Malicious Software	Untrained/Untested Staff	Controls Around User-installed Software			No	No
Laptop		TestingAsset	Careless Software Developer/Insecure Development of Software	Custom Application Weaknesses	Application or Data Partitioning			No	No
Laptop		TestingAsset	Burglar/Thief/Theft of Equipment	Physical Security Deficiencies	Controlled Access to Areas with Mobile Devices			No	No
Disk Array		TestingAsset	System Cracker/Theft of Sensitive Data	User Authentication Deficiencies	Accounts Lock After Too Many Failed Logins			TBD	In progress
Disk Array		TestingAsset	System Cracker/Theft of Sensitive Data	System Configuration Deficiencies	Change Control Processes			Yes	Yes
Disk Array		TestingAsset	System Cracker/Theft of Sensitive Data	Physical Security Deficiencies	Physical Access Authorization			Yes	Yes
Disk Array		TestingAsset	System Cracker/Theft of Sensitive Data	Insecure Network Configuration	Auto Logoff or Auto Screen Locking			No	No
Disk Array		TestingAsset	System Cracker/Theft of Sensitive Data	Insecure Network Configuration	Authentication of Network Sessions (as Distinct From Users)			In progress	In progress
Disk Array		TestingAsset	System Cracker/Theft of Sensitive Data	Custom Application Weaknesses	Application Penetration and Vulnerability Testing			Yes	Yes
Disk Array		TestingAsset	System Cracker/Theft of Sensitive Data	Custom Application Weaknesses	Application Code Review			In progress	In progress
Disk Array		TestingAsset	System Cracker/Insecure User Management	Dormant Accounts	Access Logging			Yes	Yes
Disk Array		TestingAsset	System Cracker/Denial of Service	Insufficient Application/Network Capacity	Capacity Planning			In progress	In progress
Disk Array		TestingAsset	Power Surge/Electrical Damage to Equipment	Insufficient Power Shielding	Data Backup			No	No
Disk Array		TestingAsset	Malware/Theft of Sensitive Data	Anti-malware Deficiencies	Central Monitoring of Endpoint Protection Software			No	No
Disk Array		TestingAsset	Malware/Theft of Sensitive Data	Anti-malware Deficiencies	Anti-virus Policy and Procedures			N/A	N/A

Media	Label	Asset Name(s)	Threat Source/Threat Event	Vulnerability	Control	NIST Family	NIST Family ID	Global	Media
Disk Array		TestingAsset	Malware/Theft of Sensitive Data	Anti-malware Deficiencies	Anti-Malware Software			No	No
Disk Array		TestingAsset	Malicious User/Malicious Use of Sensitive Data	Endpoint Leakage	Acceptable Use Policy			Yes	Yes
Disk Array		TestingAsset	Careless Software Developer/Insecure Development of Software	Custom Application Weaknesses	Application or Data Partitioning			No	No
Desktop or Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	User Authentication Deficiencies	Accounts Lock After Too Many Failed Logins			TBD	Yes
Desktop or Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	System Configuration Deficiencies	Change Control Processes			Yes	Yes
Desktop or Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	Physical Security Deficiencies	Physical Access Authorization			Yes	Yes
Desktop or Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	Insecure Network Configuration	Auto Logoff or Auto Screen Locking			No	No
Desktop or Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	Insecure Network Configuration	Authentication of Network Sessions (as Distinct From Users)			In progress	In progress
Desktop or Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	Custom Application Weaknesses	Application Penetration and Vulnerability Testing			Yes	Yes
Desktop or Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	Custom Application Weaknesses	Application Code Review			In progress	In progress
Desktop or Laptop		TestingAsset	System Cracker/Theft of Sensitive Data	Anti-malware Deficiencies	Anti-Malware Software			No	No
Desktop or Laptop		TestingAsset	System Cracker/Insecure User Management	Dormant Accounts	Access Logging			Yes	Yes
Desktop or Laptop		TestingAsset	System Cracker/Denial of Service	Insufficient Application/Network Capacity	Capacity Planning			In progress	In progress
Desktop or Laptop		TestingAsset	Power Surge/Electrical Damage to Equipment	Insufficient Power Shielding	Data Backup			No	No
Desktop or Laptop		TestingAsset	Malware/Theft of Sensitive Data	Anti-malware Deficiencies	Central Monitoring of Endpoint Protection Software			No	No
Desktop or Laptop		TestingAsset	Malware/Theft of Sensitive Data	Anti-malware Deficiencies	Anti-virus Policy and Procedures			N/A	N/A
Desktop or Laptop		TestingAsset	Malicious User/Malicious Use of Sensitive Data	Endpoint Leakage	Acceptable Use Policy			Yes	Yes
Desktop or Laptop		TestingAsset	Careless User/Installation of Malicious Software	Untrained/Untested Staff	Controls Around User-installed Software			No	No
Desktop or Laptop		TestingAsset	Careless Software Developer/Insecure Development of Software	Custom Application Weaknesses	Application or Data Partitioning			No	No
Desktop or Laptop		TestingAsset	Burglar/Thief/Theft of Equipment	Physical Security Deficiencies	Controlled Access to Areas with Mobile Devices			No	No
Contractors / Consultants		TestingAsset	Service Providers / Vendors/Lack of Due Diligence	Contractual Agreement Deficiencies	Contractual Agreements			No	No
Backup Media	sample Backup label	TestingAsset	Careless User/Physical Damage to Equipment	Accidents	Backup Media Handling Policy and Procedures			Yes	Yes
Backup Media	sample Backup label	TestingAsset	Careless IT Personnel/Loss of Storage Media	Improper Media/Device Handling	Tracking of Backup Media			TBD	Yes
Backup Media	sample Backup label	TestingAsset	Careless IT Personnel/Loss of Storage Media	Improper Media/Device Handling	Encryption of Backup Media			TBD	No
Backup Media	sample Backup label	TestingAsset	Careless IT Personnel/Loss of Storage Media	Improper Media/Device Handling	Acceptable Use Policy			Yes	Yes
Backup Media	sample Backup label	TestingAsset	Careless IT Personnel/Improper Destruction, Disposal or Reuse of Storage Media	Destruction/Disposal Deficiencies	Media/Device Reuse and Disposal Policy and Procedures			TBD	In progress
Backup Media	sample Backup label	TestingAsset	Careless IT Personnel/Improper Destruction, Disposal or Reuse of Storage Media	Destruction/Disposal Deficiencies	Device Re-use and Disposal Policy and Procedures			TBD	Yes
Backup Media	sample Backup label	TestingAsset	Careless IT Personnel/Corruption or Destruction of Important Data	Lack of Data Validation	Tamper-proof Mechanisms			TBD	Yes
Backup Media	sample Backup label	TestingAsset	Burglar/Thief/Theft of Storage Media	Physical Security Deficiencies	Visitor Access Control			TBD	In progress
Backup Media	sample Backup label	TestingAsset	Burglar/Thief/Theft of Storage Media	Physical Security Deficiencies	Secure Storage of Backup Media When Not in Use			TBD	No
Backup Media	sample Backup label	TestingAsset	Burglar/Thief/Theft of Storage Media	Physical Security Deficiencies	Physical Access Monitoring			TBD	Yes

Media	Label	Asset Name(s)	Threat Source/Threat Event	Vulnerability	Control	NIST Family	NIST Family ID	Global	Media
Backup Media	sample Backup label	TestingAsset	Burglar/Thief/Theft of Storage Media	Physical Security Deficiencies	Physical Access Control			TBD	No
Backup Media	sample Backup label	TestingAsset	Burglar/Thief/Theft of Storage Media	Physical Security Deficiencies	Physical Access Authorization			Yes	Yes
Backup Media	sample Backup label	TestingAsset	Burglar/Thief/Theft of Storage Media	Physical Security Deficiencies	Inventory Control Process			TBD	In progress
Backup Media	sample Backup label	TestingAsset	Burglar/Thief/Theft of Storage Media	Improper Media/Device Handling	Offsite Backup Media Storage			TBD	In progress
Backup Media	sample Backup label	TestingAsset	Burglar/Thief/Theft of Equipment	Physical Security Deficiencies	TestControls			TBD	Yes