RISK RATING DETAIL REPORT

Customer: **Kennesaw State University** **Entity:** **I7_Wynt_De**

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		Careless User/Improper Disclosure or Use of Sensitive Data	Data Leakage	4	5	20	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 4 because these access and protection measures are partially enforced, leaving endpoints and data channels exposed. I selected the Risk Impact of 5 because without these safeguards, this can directly lead to data theft and severe compliance violations. - Denver Wynter - 10/05/2025 11:34 AM

Risk scenario ID: 33927359

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Auto Logoff or Auto Screen Locking	Component Control	In progress			
Data Loss Prevention Tools	Component Control	In progress			
Information Disclosure Procedures	Component Control	In progress			
Restrictions on the Use of Non-Organizational Devices	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		IT Development or QA Staff/Application Failure	Custom Application Weaknesses	4	5	20	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 4 because key monitoring, alerting, and secure development practices are still being established, allowing potential gaps in threat detection and control. I selected the Risk Impact of 5 because exploitation of weak administrative or code controls could expose sensitive financial and identity data, severely harming the organization and its reputation. - Denver Wynter - 10/05/2025 11:36 AM

Risk scenario ID: 33927361

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Activity Logging	Component Control	In progress			
Application Code Review	Component Control	In progress			
Automatic Alerting for Adverse Events	Component Control	In progress			
Data Backup	Component Control	In progress			
Information Systems Monitoring	Component Control	In progress			
On-call Technical Resources	Component Control	In progress			
Remote Administrative Access	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
Secure Administrative Host	Component Control	In progress			
Secure Software Development Processes	Component Control	In progress			
Secure Software Development Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		System Cracker/Theft of Sensitive Data	Application Configuration Deficiencies	4	5	20	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 4 because controls such as penetration testing and privileged account management are still being developed, leaving exploitable configuration gaps. I selected the Risk Impact of 5 because exposure of accounting or directory data would cause severe financial and operational damage. - Denver Wynter - 10/05/2025 11:33 AM

Risk scenario ID: 33927357

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Application or Data Partitioning	Component Control	In progress			
Application, Network, or System Penetration Testing	Component Control	In progress			
Application, Network, or System Vulnerability Testing	Component Control	In progress			
Change Control Processes	Component Control	In progress			
Privileged Account Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		System Cracker/Theft of Sensitive Data	Excessive User Permissions	4	5	20	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 4 because access control processes are not consistently automated, allowing users to retain permissions beyond their required job scope. I selected the Risk Impact of 5 because if a user with excessive privileges is compromised or acts maliciously, they could manipulate or export sensitive patient, payroll, or financial data, causing extensive system and regulatory damage. - Denver Wynter - 10/05/2025 12:56 PM

Risk scenario ID: 33927390

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Activity Logging	Component Control	In progress			
Information Access Control Policy and Procedures	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Principle of Least Privilege	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Privileged Account Management	Component Control	In progress			
Role-based Access Control	Component Control	In progress			
User Account Management	Component Control	In progress			
User Activity Review	Component Control	In progress			
User Permissions Reviews	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		System Cracker/Corruption, Destruction, or Loss of Data	Insufficient Data Validation	4	4	16	10-05-25	10-05-25	

Risk scenario ID: 33927371

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Backup	Component Control	In progress			
Data Input Validation	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / LAN Group	Data Center	Careless User/Improper Disclosure or Use of Sensitive Data	Endpoint Data Loss	4	4	16	10-05-25	10-05-25	I choose mitigate as the recommended risk treatment strategy because measures can be taken to protect sensitive through eliminating unauthorized access and using measure/tools to protect LAN. I reduced the residual risk from 15 to 6. - Denver Wynter - 10/05/2025 08:09 PM, RD: I selected the Risk Likelihood of 4 because several endpoints and access controls remain incomplete, giving insiders multiple paths to move or copy sensitive data. I selected the Risk Impact of 4 because unauthorized actions on the directory or intranet systems could disrupt authentication, file access, and internal communications across the LAN. - Denver Wynter - 10/05/2025 12:24 PM

Risk scenario ID: 33938089

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Acceptable Use Policy	Component Control	In progress			
Auto Logoff or Auto Screen Locking	Component Control	In progress			
Data Loss Prevention Tools	Component Control	In progress			
Information Disclosure Procedures	Component Control	In progress			
Limited Access to Output Devices (Printers, etc.)	Component Control	In progress			
Limited User Accessibility (By Time of Day, By Location, etc.)	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Prevention of User Storing Data Locally (Terminals, VDI, etc.)	Component Control	No			

Restrictions on Media Use	Component Control	In progress			
Restrictions on the Use of Internet File Storage	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Internal User / No Label		Internal Parties/Improper Disclosure or Use of Sensitive Data	Insufficient Personnel Screening	4	4	16	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 4 because while background checks are conducted for certain positions, screening processes for all internal users and contractors are not consistently verified. I selected the Risk Impact of 4 because inadequate screening could allow individuals with questionable backgrounds to access or mishandle sensitive healthcare and financial data, resulting in serious compliance and reputational consequences. - Denver Wynter - 10/05/2025 12:38 PM

Risk scenario ID: 33927419

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Personnel Screening	Component Control	In progress			

Software-as-a-Service / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Excessive User Permissions	4	4	16	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 4 because user permissions across SaaS platforms are inconsistently reviewed, and privilege creep can occur when roles change or accounts are duplicated. I selected the Risk Impact of 4 because excessive access in cloud-based applications could allow insiders or compromised users to alter, delete, or exfiltrate sensitive healthcare and financial data, leading to major service disruptions and compliance violations. - Denver Wynter - 10/05/2025 12:54 PM

Risk scenario ID: 33927388

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Activity Logging	Component Control	In progress			
Information Access Control Policy and Procedures	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Principle of Least Privilege	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Role-based Access Control	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
Session Auditing	Component Control	In progress			
User Account Management	Component Control	In progress			
User Activity Review	Component Control	In progress			
User Permissions Reviews	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		Information Technology Staff/Improper Access to Sensitive Data	Account and Password Creation and Distribution Deficiencies	3	5	🟥 15	10-05-25	10-05-25	

Risk scenario ID: 33927372

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Identification and Authentication Policy and Procedures	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Two Man Rule/Dual Authorization	Component Control	No			
User Account Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	User Authentication Deficiencies	3	5	🟥 15	10-05-25	10-05-25	I choose to mitigate as the recommended risk treatment strategy because actions can be implemented to reduced the risk surrounding login and passwords. I reduced the residual risk from 15 to 6 because the company now has policies surrounding login including usernames and passwords. - Denver Wynter - 10/05/2025 08:10 PM,RD: I selected the Risk Likelihood of 3 because basic authentication controls are active, but still rely heavily on passwords without full multi-factor enforcement. I selected the Risk Impact of 5 because credential compromise could grant wide-reaching access to financial, HR, and clinical systems, resulting in severe data loss and reputational harm. - Denver Wynter - 10/05/2025 12:03 PM

Risk scenario ID: 33938036

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Accounts Lock After Too Many Failed Logins	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Domain/Device Authentication	Component Control	In progress			
Multi-factor Authentication	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Unique User ID	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Careless User/Improper Disclosure or Use of Sensitive Data	Endpoint Data Loss	3	5	15	10-05-25	10-05-25	I chose to mitigate as the recommended risk treatment strategy because the SAN network needs to be protected from unauthorized access disrupting cloud data. I reduced the residual risk from 15 to 4. - Denver Wynter - 10/05/2025 08:33 PM,RD: I selected the Risk Likelihood of 3 because while most endpoint controls exist, users can still locally store or transfer files, creating an exposure path. I selected the Risk Impact of 5 because unauthorized access or loss of cloud backup data could result in widespread data destruction and severe recovery challenges. - Denver Wynter - 10/05/2025 12:07 PM

Risk scenario ID: 33938152

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Acceptable Use Policy	Component Control	In progress			
Auto Logoff or Auto Screen Locking	Component Control	In progress			
Data Loss Prevention Tools	Component Control	In progress			
Information Disclosure Procedures	Component Control	In progress			
Limited Access to Output Devices (Printers, etc.)	Component Control	In progress			
Limited User Accessibility (By Time of Day, By Location, etc.)	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Prevention of User Storing Data Locally (Terminals, VDI, etc.)	Component Control	No			
Restrictions on Media Use	Component Control	In progress			
Restrictions on the Use of Internet File Storage	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Information Technology Staff/Improper Destruction, Disposal or Reuse of Media	Destruction/Disposal Deficiencies	3	5	15	10-05-25	10-05-25	I chose to Mitigate as the recommended risk treatment strategy because necessity to mitigate the risk associated with IT staff in regards to improper destruction, disposal or reuse of Media . I reduced the residual risk from 15 to 2. - Denver Wynter - 10/05/2025 09:07 PM,RD: I selected the Risk Likelihood of 3 because while encryption and disposal processes exist, staff adherence and routine verification are not fully reliable. I selected the Risk Impact of 5 because any mishandling of patient records or unencrypted data could lead to serious privacy breaches and regulatory penalties. - Denver Wynter - 10/05/2025 09:25 PM

Risk scenario ID: 33927254

Asset(s): Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Retention Policy and Procedures	Component Control	In progress			
Encryption of Disks (Full Disk, File Based, etc.)	Component Control	In progress			
Media/Device Reuse and Disposal Policy and Procedures	Component Control	In progress			
Prevention of User Storing Data Locally (Terminals, VDI, etc.)	Component Control	No			
Sanitize Device/Disks/Media	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			
Training for the Security Workforce	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / LAN Group	Data Center	Information Technology Staff/Improper Access to Sensitive Data	Account and Password Creation and Distribution Deficiencies	3	5	15	10-05-25	10-05-25	I chose Mitigate as the recommended risk treatment strategy because of the need to essential need to limit exposure of data through lack of dual authentication. I reduced the residual risk from 15 to 3. - Denver Wynter - 10/05/2025 08:54 PM,RD: I selected the Risk Likelihood of 3 because authentication and password management controls are mostly in place, but lack dual authorization for sensitive account actions. I selected the Risk Impact of 5 because if an attacker gains admin-level credentials, they could manipulate directory permissions or disable services, leading to critical network outages and exposure of sensitive data. - Denver Wynter - 10/05/2025 12:27 PM

Risk scenario ID: 33938098

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Identification and Authentication Policy and Procedures	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Two Man Rule/Dual Authorization	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

User Account Management	Component Control	In progress

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / LAN Group	Data Center	Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Endpoint Data Loss/Theft	3	5	15	10-05-25	10-05-25	I chose Mitigate as the recommended risk treatment strategy because risk of movement of data and device through malicious users. I reduced the residual risk from 15 to 6. - Denver Wynter - 10/05/2025 09:02 PM,RD: I selected the Risk Likelihood of 3 because controls for device and data movement are present but not fully enforced, leaving potential for insider misuse. I selected the Risk Impact of 5 because compromise or deletion of Active Directory or intranet data would critically affect authentication, communication, and system access across the organization. - Denver Wynter - 10/05/2025 12:22 PM

Risk scenario ID: 33938086

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Loss Prevention Tools	Component Control	In progress			
Limited Access to Output Devices (Printers, etc.)	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Restrictions on the Use of Internet File Storage	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Internal Network - Wired / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Dormant Accounts	3	5	15	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because while access management and logging tools are implemented, dormant accounts are not consistently identified or removed, leaving some exposure. I selected the Risk Impact of 5 because if a dormant account is exploited, it could provide unauthorized access to critical systems like Active Directory and SQL databases, resulting in widespread compromise and data manipulation. - Denver Wynter - 10/05/2025 12:30 PM

Risk scenario ID: 33927342

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database,Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Event Correlation	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Prompt Account Termination	Component Control	In progress			
Unique User ID	Component Control	In progress			
User Account Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

User Permissions Reviews	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Internal User / No Label		Internal Parties/Improper Disclosure or Use of Sensitive Data	Insufficient Personnel Training	3	5	15	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because employee training programs are active but vary by department, leaving some users less prepared to identify phishing or manipulation attempts. I selected the Risk Impact of 5 because a successful social engineering attack or untrained employee error could expose large volumes of patient or financial information, triggering regulatory penalties and significant data loss. - Denver Wynter - 10/05/2025 12:39 PM

Risk scenario ID: 33927420

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Security/Privacy Awareness and Training	Component Control	In progress			
Social Engineering Testing	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	User Authentication Deficiencies	3	5	15	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because while password controls and account lockout mechanisms are enabled, MFA implementation across all servers remains incomplete. I selected the Risk Impact of 5 because a compromised server account could provide direct access to sensitive SQL databases and system configurations, resulting in severe data exfiltration or full domain compromise. - Denver Wynter - 10/05/2025 12:51 PM

Risk scenario ID: 33927292

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Accounts Lock After Too Many Failed Logins	Component Control	In progress			
Multi-factor Authentication	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Unique User ID	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		System Cracker/Theft of Sensitive Data	Insecure Device Configuration	3	5	15	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because while patching and vulnerability testing are ongoing, incomplete hardening and inconsistent configuration reviews still allow potential attack vectors. I selected the Risk Impact of 5 because compromise of poorly secured servers, especially those hosting SQL databases or Active Directory, could lead to massive data theft, system disruption, and loss of operational control across the network. - Denver Wynter - 10/05/2025 12:49 PM

Risk scenario ID: 33927289

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Application, Network, or System Penetration Testing	Component Control	In progress			
Application, Network, or System Vulnerability Testing	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Device Hardening	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Standardized System Configurations	Component Control	In progress			
System Configuration Management	Component Control	In progress			
System Isolation	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		System Cracker/Theft of Sensitive Data	User Authentication Deficiencies	3	5	15	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because most authentication measures are active, but incomplete MFA rollout and limited event correlation leave room for unauthorized access. I selected the Risk Impact of 5 because misuse or compromise of privileged SaaS credentials could expose integrated systems like EHR or payroll data, leading to critical data breaches and major HIPAA compliance violations. - Denver Wynter - 10/05/2025 12:57 PM

Risk scenario ID: 33927391

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Accounts Lock After Too Many Failed Logins	Component Control	In progress			
Event Correlation	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Multi-factor Authentication	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Prevention of Simultaneous User Logins	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Unique User ID	Component Control	In progress			
User Activity Review	Component Control	In progress			

Application / No Label		Careless User/Corruption, Destruction, or Loss of Data	Insufficient Data Validation	3	4	12	10-05-25	10-05-25	

Risk scenario ID: 33927374

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Backup	Component Control	In progress			
Data Input Validation	Component Control	No			

Application / No Label		Information Technology Staff/Application Failure	Insufficient Application Capacity	3	4	12	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because performance and capacity controls are not yet fully implemented across systems. I selected the Risk Impact of 4 because poor load handling or processing gaps could cause major disruptions and loss of sensitive data. - Denver Wynter - 10/05/2025 11:33 AM

Risk scenario ID: 33927358

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Application Load Testing	Component Control	In progress			
Capacity Planning	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
Distributed Processing or Storage	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		Information Technology Staff/Corruption, Destruction, or Loss of Data	Insufficient Data Backup	3	4	**12**	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because backups exist without routine integrity validation, and tamper-evident controls are only partially enforced. I selected the Risk Impact of 4 because loss or exposure of accounting and identity data would disrupt core operations and trigger major compliance actions. - Denver Wynter - 10/05/2025 11:31 AM

Risk scenario ID: 33927360

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Backup Media Testing and Validation Policy and Procedures	Component Control	In progress			
Data Backup	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		Malicious User/Corruption, Destruction, or Loss of Data	Insufficient Data Validation	3	4	**12**	10-05-25	10-05-25	

Risk scenario ID: 33927375

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Backup	Component Control	In progress			
Data Input Validation	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Custom Application Weaknesses	3	4	**12**	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because most controls are under development, but existing testing and review processes provide partial defense. I selected the Risk Impact of 4 because weak change management and improper data handling can lead to major unauthorized access or data exposure incidents. - Denver Wynter - 10/05/2025 11:40 AM

Risk scenario ID: 33927362

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Application Code Review	Component Control	In progress			
Application, Network, or System Penetration Testing	Component Control	In progress			
Application, Network, or System Vulnerability Testing	Component Control	In progress			
Change Control Processes	Component Control	In progress			
Limitations on the Use of Live Data	Component Control	No			
Secure Password Storage	Component Control	In progress			
Secure Software Development Processes	Component Control	In progress			
Segregation of Duties	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Dormant Accounts	3	4	**12**	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because account lifecycle management and log monitoring controls are still developing, leaving exposure to unauthorized access. I selected the Risk Impact of 4 because weak auditing or delayed account termination could result in severe data theft and compliance violations. - Denver Wynter - 10/05/2025 11:45 AM

Risk scenario ID: 33927363

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database,Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Event Correlation	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Prompt Account Termination	Component Control	In progress			
Session Auditing	Component Control	In progress			
Single Sign-on	Component Control	In progress			
User Account Management	Component Control	In progress			
User Activity Review	Component Control	In progress			
User Permissions Reviews	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	User Authentication Deficiencies	3	4	**12**	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because password and authentication controls are improving, but still not fully enforced, leaving systems partly exposed. I selected the Risk Impact of 4 because compromised login mechanisms could result in major unauthorized access to sensitive data and financial systems. - Denver Wynter - 10/05/2025 11:49 AM

Risk scenario ID: 33927365

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Accounts Lock After Too Many Failed Logins	Component Control	In progress			
Event Correlation	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Multi-factor Authentication	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Prevention of Simultaneous User Logins	Component Control	No			
Session Auditing	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Unique User ID	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		Service Providers or Vendors/Application Failure	Commercial Application Weaknesses	4	3	12	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 4 because continuous monitoring and response mechanisms are still being developed, leaving gaps in detecting and reacting to attacks. I selected the Risk Impact of 3 because missed alerts or slow response could interrupt service availability and compromise moderate amounts of sensitive data. - Denver Wynter - 10/05/2025 11:51 AM

Risk scenario ID: 33927366

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Activity Logging	Component Control	In progress			
Automatic Alerting for Adverse Events	Component Control	In progress			
Information Systems Monitoring	Component Control	In progress			
On-call Technical Resources	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
Remote Administrative Access	Component Control	In progress			
Secure Administrative Host	Component Control	In progress			
Service-level Agreements	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		System Cracker/Theft of Sensitive Data	Dormant Accounts	3	4	12	10-05-25	10-05-25	

Risk scenario ID: 33927369

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Accounts Lock After Too Many Failed Logins	Component Control	In progress			
Event Correlation	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Prompt Account Termination	Component Control	In progress			
Single Sign-on	Component Control	In progress			
User Account Management	Component Control	In progress			
User Activity Review	Component Control	In progress			
User Permissions Reviews	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	Careless User/Improper Disclosure or Use of Sensitive Data	Endpoint Data Loss	3	4	12	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because access and endpoint protection controls are still being rolled out, creating opportunities for data to be copied or stored insecurely. I selected the Risk Impact of 4 because if sensitive accounting or patient data were leaked or destroyed, it would cause major operational and regulatory consequences. - Denver Wynter - 10/05/2025 11:58 AM

Risk scenario ID: 33938026

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Acceptable Use Policy	Component Control	In progress			
Auto Logoff or Auto Screen Locking	Component Control	In progress			
Data Loss Prevention Tools	Component Control	In progress			
Information Disclosure Procedures	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
Limited Access to Output Devices (Printers, etc.)	Component Control	In progress			
Limited User Accessibility (By Time of Day, By Location, etc.)	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Prevention of User Storing Data Locally (Terminals, VDI, etc.)	Component Control	No			
Restrictions on Media Use	Component Control	In progress			
Restrictions on the Use of Internet File Storage	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	Careless User/Improper Disclosure or Use of Sensitive Data	Installation of Malware-External Threats	3	4	12	10-05-25	10-05-25	

Risk scenario ID: 33938070

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Acceptable Use Policy	Component Control	In progress			
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			
Block List	Component Control	In progress			
Central Monitoring of Anti-Malware Software	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Content (URL) Filtering	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			
Limitations on Administrative Rights	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	Careless User/Social Engineering	Untrained/Untested Staff	3	4	12	10-05-25	10-05-25	

Risk scenario ID: 33938038

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
Block List	Component Control	In progress			
Central Monitoring of Anti-Malware Software	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Content (URL) Filtering	Component Control	In progress			
Email Spam Filtering	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			
Limitations on Administrative Rights	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Prevention of User Storing Data Locally (Terminals, VDI, etc.)	Component Control	No			
Security/Privacy Awareness and Training	Component Control	In progress			
Social Engineering Testing	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	Information Technology Staff/Improper Destruction, Disposal or Reuse of Media	Destruction/Disposal Deficiencies	3	4	12	10-05-25	10-05-25	

Risk scenario ID: 33938061

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Retention Policy and Procedures	Component Control	In progress			
Encryption of Disks (Full Disk, File Based, etc.)	Component Control	In progress			
Media/Device Reuse and Disposal Policy and Procedures	Component Control	In progress			
Prevention of User Storing Data Locally (Terminals, VDI, etc.)	Component Control	No			
Sanitize Device/Disks/Media	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			
Training for the Security Workforce	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Endpoint Data Loss/Theft	4	3	12	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 4 because removable media and internet storage restrictions are only partially implemented, allowing users potential channels for data exfiltration. I selected the Risk Impact of 3 because loss of sensitive endpoint data could disrupt financial, HR, and clinical operations, but can be recovered within existing backup and training protocols. - Denver Wynter - 10/05/2025 11:56 AM

Risk scenario ID: 33938023

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Loss Prevention Tools	Component Control	In progress			
Limited Access to Output Devices (Printers, etc.)	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Restrictions on the Use of Internet File Storage	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Disaster/Equipment Damage	Insufficient Equipment Redundancy	4	3	12	10-05-25	10-05-25	

Risk scenario ID: 33938199

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plan Testing	Component Control	In progress			
Contingency Plans	Component Control	In progress			
Redundant or Spare Equipment	Component Control	No			
Threat/Vulnerability Intelligence Services	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Information Technology Staff/Improper Destruction, Disposal or Reuse of Media	Destruction/Disposal Deficiencies	3	4	12	10-05-25	10-05-25	

Risk scenario ID: 33938187

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Retention Policy and Procedures	Component Control	In progress			
Encryption of Disks (Full Disk, File Based, etc.)	Component Control	In progress			
Media/Device Reuse and Disposal Policy and Procedures	Component Control	In progress			
Prevention of User Storing Data Locally (Terminals, VDI, etc.)	Component Control	No			
Sanitize Device/Disks/Media	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			
Training for the Security Workforce	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	User Authentication Deficiencies	3	4	12	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because while authentication and password measures are improving, the absence of full MFA deployment keeps accounts vulnerable to brute-force or credential theft. I selected the Risk Impact of 4 because unauthorized access to cloud or SAN backups could allow data tampering or deletion, significantly affecting integrity and system recovery. - Denver Wynter - 10/05/2025 12:10 PM

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Risk scenario ID: 33938162

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Accounts Lock After Too Many Failed Logins	Component Control	In progress			
Domain/Device Authentication	Component Control	In progress			
Multi-factor Authentication	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Unique User ID	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	System Cracker/Theft of Sensitive Data	Insecure Device Configuration	4	3	12	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 4 because incomplete patching and inconsistent configurations create frequent opportunities for exploitation of known weaknesses. I selected the Risk Impact of 3 because while data loss could cause service interruption, redundant backups and restore procedures reduce long-term damage. - Denver Wynter - 10/05/2025 12:08 PM

Risk scenario ID: 33938159

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Centralized Patch Management	Component Control	In progress			
Device Hardening	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Standardized System Configurations	Component Control	In progress			
System Configuration Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Careless User/Social Engineering	Untrained/Untested Staff	4	3	12	10-05-25	10-05-25	

Risk scenario ID: 33927231

Asset(s): Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Block List	Component Control	In progress			
Central Monitoring of Anti-Malware Software	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Content (URL) Filtering	Component Control	In progress			
Email Spam Filtering	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			
Limitations on Administrative Rights	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Prevention of User Storing Data Locally (Terminals, VDI, etc.)	Component Control	No			
Security/Privacy Awareness and Training	Component Control	In progress			
Social Engineering Testing	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Inclement Weather/Unavailability of Key Personnel	Lack of Key Person Redundancy / Cross-training	3	4	12	10-05-25	10-05-25	

Risk scenario ID: 33927236
Asset(s): Support IT and IT Database
Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plans	Component Control	In progress			
Cross-functional Training	Component Control	No			
On-call Technical Resources	Component Control	In progress			
Process Documentation	Component Control	In progress			
Remote Administrative Access	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Information Technology Staff/Data Loss	Insufficient Data Backup	3	4	12	10-05-25	10-05-25	

Risk scenario ID: 33927246
Asset(s): Support IT and IT Database
Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Backup Media Testing and Validation Policy and Procedures	Component Control	In progress			
Data Backup	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Dormant Accounts	3	4	12	10-05-25	10-05-25	

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Risk scenario ID: 33927259

Asset(s): Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Event Correlation	Component Control	In progress			
Information Access Control Policy and Procedures	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Prompt Account Termination	Component Control	No			
Session Auditing	Component Control	In progress			
Single Sign-on	Component Control	In progress			
User Account Management	Component Control	In progress			
User Activity Review	Component Control	In progress			
User Permissions Reviews	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Internal Network - Wired / No Label		Information Technology Staff/Improper Access to Sensitive Data	Account and Password Creation and Distribution Deficiencies	3	4	12	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because while authentication controls are established, inconsistent enforcement of password resets and lack of dual authorization leave room for misuse of inactive accounts. I selected the Risk Impact of 4 because exploitation of a dormant privileged account could lead to unauthorized changes in system access or data integrity across critical internal applications. - Denver Wynter - 10/05/2025 12:32 PM

Risk scenario ID: 33927344

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Identification and Authentication Policy and Procedures	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Two Man Rule/Dual Authorization	Component Control	No			
Unique User ID	Component Control	In progress			
User Account Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Internal Network - Wired / No Label		Natural Disaster/Network Unavailable	Network Outage	3	4	12	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because alerting and redundancy controls are active but rely on manual verification and scheduled reviews, which leaves potential detection gaps. I selected the Risk Impact of 4 because if a compromised account is used to disable key systems or compromise backups, it could disrupt network continuity and delay critical recovery efforts across departments. - Denver Wynter - 10/05/2025 12:35 PM

Risk scenario ID: 33927346

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Automatic Alerting for Adverse Events	Component Control	In progress			
Contingency Plan Testing	Component Control	In progress			
Contingency Plans	Component Control	In progress			
Information Systems Monitoring	Component Control	In progress			
Redundant Network Communications Providers	Component Control	In progress			
Resilient Network Topography	Component Control	In progress			

Internal User / No Label		Internal Parties/Improper Disclosure or Use of Sensitive Data	Lack of Policies and Procedures Enforcement	3	4	12	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because disciplinary actions are documented but not always applied consistently across all departments, which can weaken deterrence. I selected the Risk Impact of 4 because failure to enforce sanctions for policy violations could lead to repeated misuse or disclosure of sensitive data, damaging trust and compliance posture across the organization, as well as open possible lawsuits for inconsistent disciplinary actions. - Denver Wynter - 10/05/2025 12:41 PM

Risk scenario ID: 33927422

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Personnel Sanctions	Component Control	In progress			

Server / No Label		Information Technology Staff/Data Loss	Insufficient Data Backup	3	4	12	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because backup testing and distributed storage are conducted, but not consistently validated across all systems, which leaves some exposure. I selected the Risk Impact of 4 because a misconfigured or tampered backup environment could result in loss or corruption of critical healthcare and financial data, severely impacting recovery operations and compliance efforts. - Denver Wynter - 10/05/2025 12:53 PM

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Risk scenario ID: 33927300

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Backup Media Testing and Validation Policy and Procedures	Component Control	In progress			
Data Backup	Component Control	In progress			
Distributed Processing or Storage	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	In progress			

Server / No Label		Information Technology Staff/Improper Access to Sensitive Data	Account and Password Creation and Distribution Deficiencies	3	4	12	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because servers often host multiple privileged accounts, and the absence of dual authorization increases the chance of misuse or compromise. I selected the Risk Impact of 4 because unauthorized access to high-level system credentials could lead to significant data theft, privilege escalation, or manipulation of system configurations across multiple critical environments. - Denver Wynter - 10/05/2025 12:50 PM

Risk scenario ID: 33927291

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Identification and Authentication Policy and Procedures	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Two Man Rule/Dual Authorization	Component Control	No			
User Account Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		Careless User/Improper Disclosure or Use of Sensitive Data	Data Leakage	3	4	12	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because access restrictions and user training are in place, but SaaS session controls and device limitations are not uniformly enforced across all platforms. I selected the Risk Impact of 4 because improper session authentication or unmonitored device use could expose sensitive patient or financial data stored in cloud systems, resulting in compliance and reputational consequences. - Denver Wynter - 10/05/2025 12:55 PM

Risk scenario ID: 33927389

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Acceptable Use Policy	Component Control	In progress			
Authentication of Network Sessions (as Distinct From Users)	Component Control	In progress			
Auto Logoff or Auto Screen Locking	Component Control	In progress			
Information Disclosure Procedures	Component Control	In progress			
Limited User Accessibility (By Time of Day, By Location, etc.)	Component Control	In progress			
Restrictions on the Use of Non-Organizational Devices	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Excessive User Permissions	2	5	10	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because user access and logging controls are still being developed, causing a reduction of consistent oversight. I selected the Risk Impact of 5 because weak access governance could expose critical financial and identity data, leading to severe operational and compliance consequences. - Denver Wynter - 10/05/2025 11:48 AM

Risk scenario ID: 33927364

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Activity Logging	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Principle of Least Privilege	Component Control	In progress			
Privileged Account Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
Role-based Access Control	Component Control	In progress			
Session Auditing	Component Control	In progress			
User Account Management	Component Control	In progress			
User Activity Review	Component Control	In progress			
User Permissions Reviews	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		System Cracker/Theft of Sensitive Data	Custom Application Weaknesses	2	5	10	10-05-25	10-05-25	

Risk scenario ID: 33927368

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Application Code Review	Component Control	In progress			
Application or Data Partitioning	Component Control	In progress			
Application, Network, or System Penetration Testing	Component Control	In progress			
Application, Network, or System Vulnerability Testing	Component Control	In progress			
Error Message Sanitization	Component Control	No			
Secure Password Storage	Component Control	In progress			
Secure Software Development Processes	Component Control	In progress			
Secure Software Development Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	System Cracker/Theft of Sensitive Data	Insecure Device Configuration	2	5	10	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because system patching and configuration controls are organized but not fully automated, lowering but not removing the chance of exploitation. I selected the Risk Impact of 5 because if an unpatched or misconfigured endpoint is compromised, it could expose or destroy high-value clinical and financial data across multiple systems. - Denver Wynter - 10/05/2025 12:00 PM

Risk scenario ID: 33938033

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Centralized Patch Management	Component Control	In progress			
Device Hardening	Component Control	In progress			
Operating System Patching	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Privileged Account Management	Component Control	In progress			
Standardized System Configurations	Component Control	In progress			
System Configuration Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Information Technology Staff/Improper Access to Sensitive Data	Account and Password Creation and Distribution Deficiencies	2	5	10	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because user authentication policies are partially enforced, and access to backup systems is generally restricted to administrators. I selected the Risk Impact of 5 because if those privileged credentials are compromised, an attacker could permanently delete or alter critical backups, leading to significant data loss. - Denver Wynter - 10/05/2025 12:09 PM

Risk scenario ID: 33938161

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Identification and Authentication Policy and Procedures	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Two Man Rule/Dual Authorization	Component Control	No			
User Account Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / LAN Group	Data Center	Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	User Authentication Deficiencies	2	5	10	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because Active Directory provides centralized account management with authentication and lockout controls that reduce brute-force or unauthorized access attempts. I selected the Risk Impact of 5 because if authentication controls fail, an attacker could compromise system-wide credentials, granting full access to network resources and critical internal systems. - Denver Wynter - 10/05/2025 12:28 PM

Risk scenario ID: 33938099

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Accounts Lock After Too Many Failed Logins	Component Control	In progress			
Domain/Device Authentication	Component Control	In progress			
Multi-factor Authentication	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Single Sign-on	Component Control	In progress			

Unique User ID	Component Control	In progress

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / LAN Group	Data Center	System Cracker/Theft of Sensitive Data	Insecure Device Configuration	2	5	10	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because system patching and configuration standards are largely implemented, reducing the probability of unauthorized exploitation. I selected the Risk Impact of 5 because a successful attack on Active Directory or DNS could severely impact network authentication, access control, and internal communication, leading to widespread operational downtime. - Denver Wynter - 10/05/2025 12:25 PM

Risk scenario ID: 33938096

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Centralized Patch Management	Component Control	In progress			
Device Hardening	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Standardized System Configurations	Component Control	In progress			
System Configuration Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Internal Network - Wired / No Label		Information Technology Staff/Slow or Unresponsive Applications	Lack of Capacity Planning	2	5	10	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because monitoring and alerting mechanisms are functioning, which helps detect irregular account activity before damage occurs. I selected the Risk Impact of 5 because if dormant accounts are exploited within a poorly segmented network, an attacker could move laterally across critical systems, potentially compromising the organization's entire internal infrastructure. - Denver Wynter - 10/05/2025 12:33 PM

Risk scenario ID: 33927345

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Automatic Alerting for Adverse Events	Component Control	In progress			
Capacity Planning	Component Control	In progress			
Information Systems Monitoring	Component Control	In progress			
Network Segmentation	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Internal Network - Wired / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	User Authentication Deficiencies	2	5	10	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because authentication and account lockout mechanisms are largely implemented, making brute-force or repeated access attempts less likely. I selected the Risk Impact of 5 because if a dormant account with elevated privileges is reactivated or exploited, it could enable access to multiple interconnected systems and expose large volumes of sensitive financial and clinical data. - Denver Wynter - 10/05/2025 12:31 PM

Risk scenario ID: 33927343

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Accounts Lock After Too Many Failed Logins	Component Control	In progress			
Domain/Device Authentication	Component Control	In progress			
Limited User Accessibility (By Time of Day, By Location, etc.)	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Unique User ID	Component Control	In progress			

Internal User / No Label		Internal Parties/Improper Disclosure or Use of Sensitive Data	Lack of Non-Disclosure Agreements	2	5	10	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because most employees and vendors are required to sign NDAs during onboarding, though enforcement for temporary staff may not be as consistent. I selected the Risk Impact of 5 because if an NDA breach occurs, it could result in severe legal, financial, and reputational damage due to the exposure of protected health or financial information. - Denver Wynter - 10/05/2025 12:42 PM

Risk scenario ID: 33927423

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Non-Disclosure Agreements	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Internal User / No Label		Internal Parties/Improper Disclosure or Use of Sensitive Data	Policy and Procedure Communication Deficiencies	2	5	10	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because internal policies are established and accessible, but enforcement depends on management oversight and employee acknowledgment tracking. I selected the Risk Impact of 5 because if staff fail to follow or understand these policies, sensitive health or financial data could be exposed or mishandled, leading to severe regulatory and reputational consequences. - Denver Wynter - 10/05/2025 12:39 PM

Risk scenario ID: 33927421

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Acceptable Use Policy	Component Control	In progress			
Information Disclosure Procedures	Component Control	In progress			
Information Systems Security Policies and Procedures	Component Control	In progress			
Policy and Procedure Communication	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Inclement Weather/Unavailability of Key Personnel	Lack of Key Person Redundancy / Cross-training	2	5	10	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because contingency planning and technical documentation are in place, reducing the probability of prolonged exposure from misconfigurations. I selected the Risk Impact of 5 because if remote administrative access or response plans fail during a breach, attackers could exploit misconfigured servers undetected, leading to widespread data theft and potential service outages. - Denver Wynter - 10/05/2025 12:52 PM

Risk scenario ID: 33927299

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plan Testing	Component Control	In progress			
Contingency Plans	Component Control	In progress			
Cross-functional Training	Component Control	In progress			
Lights-out/Hands-off Management	Component Control	In progress			
On-call Technical Resources	Component Control	In progress			
Process Documentation	Component Control	In progress			
Remote Administrative Access	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Information Technology Staff/System Failure or Performance Issues	Inadequate System Capacity	2	5	10	10-05-25	10-05-25	

Risk scenario ID: 33927333

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Automatic Alerting for Adverse Events	Component Control	In progress			
Capacity Planning	Component Control	In progress			
Distributed Processing or Storage	Component Control	In progress			
Information Systems Monitoring	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		System Cracker/Theft of Sensitive Data	Unsupported Operating System	2	5	10	10-05-25	10-05-25	

Risk scenario ID: 33927335

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Centralized Patch Management	Component Control	In progress			
Operating System Patching	Component Control	In progress			
System and Lifecycle Maintenance	Component Control	In progress			
System Isolation	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		Information Technology Staff/Improper Access to Sensitive Data	Account and Password Creation and Distribution Deficiencies	2	5	10	10-05-25	10-05-25	

Risk scenario ID: 33927403

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Identification and Authentication Policy and Procedures	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			

Password Strength Requirements	Component Control	In progress
Password/Token Management Policy and Procedures	Component Control	In progress
Privileged Account Management	Component Control	In progress
Single Sign-on	Component Control	In progress
Two Man Rule/Dual Authorization	Component Control	No
User Account Management	Component Control	In progress

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		Service Providers or Vendors/Improper Disposal or Destruction of Data	Contractual Agreement Deficiencies	2	5	10	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because vendor reviews and contractual agreements are in place, but they may not always include granular access control or auditing requirements. I selected the Risk Impact of 5 because weak or unclear SaaS provider agreements could lead to data loss, unapproved access, or delays in breach response, putting critical patient and financial records at severe risk. - Denver Wynter - 10/05/2025 12:58 PM

Risk scenario ID: 33927394

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contractual Agreements	Component Control	In progress			
Locally-stored Backups of Third-party Hosted Data	Component Control	In progress			
Review of Service Providers	Component Control	In progress			
Security During Systems Acquisition	Component Control	In progress			
Service-level Agreements	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		IT Development or QA Staff/Improper Disclosure or Use of Sensitive Data	Data Leakage	3	3	9	10-05-25	10-05-25	

Risk scenario ID: 33927373

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Auto Logoff or Auto Screen Locking	Component Control	In progress			
Data Loss Prevention Tools	Component Control	In progress			
Limitations on the Use of Live Data	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Restrictions on the Use of Non-Organizational Devices	Component Control	In progress

Desktop / Applications Group	Data Center	Careless User/Improper Disclosure or Use of Sensitive Data	Installation of Malware-Internal Threats	3	3	9	10-05-25	10-05-25	

Risk scenario ID: 33938071

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			
Block List	Component Control	In progress			
Central Monitoring of Anti-Malware Software	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			
Limitations on Administrative Rights	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			
Social Engineering Testing	Component Control	No			

Desktop / Applications Group	Data Center	Information Technology Staff/Data Loss	Insufficient Data Backup	3	3	9	10-05-25	10-05-25	

Risk scenario ID: 33938053

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Backup Media Testing and Validation Policy and Procedures	Component Control	In progress			
Data Backup	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	In progress			

Desktop / Applications Group	Data Center	Information Technology Staff/Improper Access to Sensitive Data	Account and Password Creation and Distribution Deficiencies	3	3	9	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because authentication and access controls are partially in place, but the lack of dual authorization increases the chance of unauthorized account use. I selected the Risk Impact of 3 because compromised credentials could lead to limited but meaningful exposure of sensitive endpoint data before being detected. - Denver Wynter - 10/05/2025 12:02 PM

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Risk scenario ID: 33938035

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Identification and Authentication Policy and Procedures	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Two Man Rule/Dual Authorization	Component Control	No			
User Account Management	Component Control	In progress			

Desktop / Applications Group	Data Center	Malicious User/Social Engineering	Untrained/Untested Staff	3	3	9	10-05-25	10-05-25	

Risk scenario ID: 33938062

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Limited User Accessibility (By Time of Day, By Location, etc.)	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			
Session Auditing	Component Control	In progress			
Social Engineering Testing	Component Control	No			

Desktop / Cloud Backup Group	Cloud	Careless User/Improper Disclosure or Use of Sensitive Data	Installation of Malware-External Threats	3	3	9	10-05-25	10-05-25	

Risk scenario ID: 33938196

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Acceptable Use Policy	Component Control	In progress			
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			
Block List	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
Central Monitoring of Anti-Malware Software	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Content (URL) Filtering	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			
Limitations on Administrative Rights	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Careless User/Improper Disclosure or Use of Sensitive Data	Installation of Malware-Internal Threats	3	3	9	10-05-25	10-05-25	

Risk scenario ID: 33938197

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			
Block List	Component Control	In progress			
Central Monitoring of Anti-Malware Software	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			
Limitations on Administrative Rights	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			
Social Engineering Testing	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Careless User/Social Engineering	Untrained/Untested Staff	3	3	9	10-05-25	10-05-25	

Risk scenario ID: 33938164

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			
Block List	Component Control	In progress			
Central Monitoring of Anti-Malware Software	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
Centralized Patch Management	Component Control	In progress			
Content (URL) Filtering	Component Control	In progress			
Email Spam Filtering	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			
Limitations on Administrative Rights	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Prevention of User Storing Data Locally (Terminals, VDI, etc.)	Component Control	No			
Security/Privacy Awareness and Training	Component Control	In progress			
Social Engineering Testing	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Information Technology Staff/Data Loss	Insufficient Data Backup	3	3	9	10-05-25	10-05-25	

Risk scenario ID: 33938179

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Backup Media Testing and Validation Policy and Procedures	Component Control	In progress			
Data Backup	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Malicious User/Social Engineering	Untrained/Untested Staff	3	3	9	10-05-25	10-05-25	

Risk scenario ID: 33938188

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Limited User Accessibility (By Time of Day, By Location, etc.)	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			
Session Auditing	Component Control	In progress			
Social Engineering Testing	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Information Technology Staff/Improper Access to Sensitive Data	Account and Password Creation and Distribution Deficiencies	3	3	9	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because authentication rules and password standards are active but not fully enforced, leaving possible gaps in user access security. I selected the Risk Impact of 3 because unauthorized access to IT databases could delay system support operations, but would not critically impact patient or financial systems. - Denver Wynter - 10/05/2025 12:18 PM

Risk scenario ID: 33927228

Asset(s): Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Identification and Authentication Policy and Procedures	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Two Man Rule/Dual Authorization	Component Control	No			
User Account Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Endpoint Data Loss/Theft	3	3	9	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 3 because basic restrictions are in place, but users still have partial device and storage access that could be misused. I selected the Risk Impact of 3 because data loss from this system would disrupt IT operations temporarily, but is recoverable within the defined recovery timeframe. - Denver Wynter - 10/05/2025 12:13 PM

Risk scenario ID: 33927216

Asset(s): Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Loss Prevention Tools	Component Control	In progress			
Limited Access to Output Devices (Printers, etc.)	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Restrictions on the Use of Internet File Storage	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / LAN Group	Data Center	Entropy/Hardware Failure	Old or Outdated Equipment	3	3	9	10-05-25	10-05-25	

Risk scenario ID: 33938112

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date

Contingency Plans	Component Control	In progress
Data Backup	Component Control	In progress
Redundant or Spare Equipment	Component Control	In progress
System and Lifecycle Maintenance	Component Control	No

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		System Cracker/Theft of Sensitive Data	Commercial Application Weaknesses	4	2	8	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 4 because patching and testing activities are still maturing, leaving opportunities for misconfigurations and outdated applications to be exploited. I selected the Risk Impact of 2 because while incidents may disrupt operations, most affected systems have recovery procedures and backups that limit long-term damage. - Denver Wynter - 10/05/2025 11:53 AM

Risk scenario ID: 33927367

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Application or Data Partitioning	Component Control	In progress			
Application Patching	Component Control	In progress			
Application, Network, or System Penetration Testing	Component Control	In progress			
Application, Network, or System Vulnerability Testing	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Security During Systems Acquisition	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Application / No Label		System Cracker/Theft of Sensitive Data	Excessive User Permissions	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33927370

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Activity Logging	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Principle of Least Privilege	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Role-based Access Control	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
User Account Management	Component Control	In progress			
User Activity Review	Component Control	In progress			
User Permissions Reviews	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Dormant Accounts	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33938066

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Event Correlation	Component Control	In progress			
Information Access Control Policy and Procedures	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Prompt Account Termination	Component Control	In progress			
Session Auditing	Component Control	In progress			
Single Sign-on	Component Control	In progress			
User Account Management	Component Control	In progress			
User Activity Review	Component Control	In progress			
User Permissions Reviews	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Dormant Accounts	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33938192

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Event Correlation	Component Control	In progress			
Information Access Control Policy and Procedures	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Prompt Account Termination	Component Control	In progress			
Session Auditing	Component Control	In progress			
Single Sign-on	Component Control	In progress			
User Account Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
User Activity Review	Component Control	In progress			
User Permissions Reviews	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Endpoint Data Loss/Theft	2	4	8	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because cloud backup access is limited to authorized admins and monitored for changes, lowering the chances of misuse. I selected the Risk Impact of 4 because if backups are altered or deleted, it could cause major delays in data recovery and disrupt continuity of clinical and business operations. - Denver Wynter - 10/05/2025 12:06 PM

Risk scenario ID: 33938149

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Loss Prevention Tools	Component Control	In progress			
Limited Access to Output Devices (Printers, etc.)	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Restrictions on the Use of Internet File Storage	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Careless User/Improper Disclosure or Use of Sensitive Data	Endpoint Data Loss	4	2	8	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 4 because physical and logical access restrictions are still being refined, making it easier for users to copy or move data outside approved systems. I selected the Risk Impact of 2 because loss of support IT data would mainly affect internal processes, causing inconvenience but limited long-term harm. - Denver Wynter - 10/05/2025 12:14 PM

Risk scenario ID: 33927219

Asset(s): Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Acceptable Use Policy	Component Control	In progress			
Auto Logoff or Auto Screen Locking	Component Control	In progress			
Data Loss Prevention Tools	Component Control	In progress			
Information Disclosure Procedures	Component Control	In progress			
Limited Access to Output Devices (Printers, etc.)	Component Control	In progress			
Limited User Accessibility (By Time of Day, By Location, etc.)	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Prevention of User Storing Data Locally (Terminals, VDI, etc.)	Component Control	No			
Restrictions on Media Use	Component Control	In progress			
Restrictions on the Use of Internet File Storage	Component Control	In progress			

Control	Type	Response	Control Notes	Author	Created Date
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Careless User/Improper Disclosure or Use of Sensitive Data	Installation of Malware-External Threats	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33927263
Asset(s): Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Acceptable Use Policy	Component Control	In progress			
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			
Block List	Component Control	In progress			
Central Monitoring of Anti-Malware Software	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Content (URL) Filtering	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			
Limitations on Administrative Rights	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Careless User/Improper Disclosure or Use of Sensitive Data	Installation of Malware-Internal Threats	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33927264
Asset(s): Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			
Block List	Component Control	In progress			
Central Monitoring of Anti-Malware Software	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			
Limitations on Administrative Rights	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Social Engineering Testing	Component Control	No

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Careless User/Physical Damage to Equipment	Accidents	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33927241
Asset(s): Support IT and IT Database
Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plans	Component Control	In progress			
Data Backup	Component Control	In progress			
Redundant or Spare Equipment	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	User Authentication Deficiencies	4	2	8	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 4 because while basic authentication and lockout features exist, the lack of universal MFA coverage increases exposure to account misuse. I selected the Risk Impact of 2 because compromise of the Support IT database would cause limited operational inconvenience without major data or patient impact. - Denver Wynter - 10/05/2025 12:20 PM

Risk scenario ID: 33927229
Asset(s): Support IT and IT Database
Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Accounts Lock After Too Many Failed Logins	Component Control	In progress			
Domain/Device Authentication	Component Control	In progress			
Multi-factor Authentication	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Unique User ID	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	System Cracker/Theft of Sensitive Data	Insecure Device Configuration	2	4	8	10-05-25	10-05-25	RD: I selected the Risk Likelihood of 2 because endpoints are periodically updated and managed, reducing the chance of successful exploitation. I selected the Risk Impact of 4 because a compromised IT system could interrupt maintenance tasks and user support services, impacting daily operations across departments. - Denver Wynter - 10/05/2025 12:16 PM

Risk scenario ID: 33927226
Asset(s): Support IT and IT Database
Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Centralized Patch Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Device Hardening	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Standardized System Configurations	Component Control	In progress			
System Configuration Management	Component Control	In progress			

Desktop / LAN Group	Data Center	Inclement Weather/Unavailability of Key Personnel	Lack of Key Person Redundancy / Cross-training	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33938106

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plans	Component Control	In progress			
Cross-functional Training	Component Control	No			
On-call Technical Resources	Component Control	In progress			
Process Documentation	Component Control	In progress			
Remote Administrative Access	Component Control	In progress			

Internal Network - Wired / No Label		System Cracker/Improper Access to Sensitive Data	Network Configuration Deficiencies	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33927348

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Application, Network, or System Vulnerability Testing	Component Control	In progress			
Network Access Control	Component Control	In progress			
Network Segmentation	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Secure Name/Address Resolution Service	Component Control	In progress			
Split Tunneling Prevention	Component Control	In progress			

Server / No Label		Careless User/Physical Damage to Equipment	Accidents	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33927305

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plans	Component Control	In progress			
Data Backup	Component Control	In progress			
Distributed Processing or Storage	Component Control	In progress			
Redundant or Spare Equipment	Component Control	In progress			
Service-level Agreements	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Information Technology Staff/Improper Disclosure or Use of Sensitive Data	Data Leakage	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33927330

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Loss Prevention Tools	Component Control	In progress			
Information Disclosure Procedures	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Remote Access Controls	Component Control	In progress			
Restrictions on Media Use	Component Control	In progress			
Secure Administrative Host	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Malicious User/Improper Disclosure or Use of Sensitive Data	Data Leakage	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33927331

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Session Auditing	Component Control	In progress			
User Activity Review	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Malicious User/Social Engineering	Untrained/Untested Staff	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33927319

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			
Session Auditing	Component Control	In progress			
Social Engineering Testing	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Dormant Accounts	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33927401

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Accounts Lock After Too Many Failed Logins	Component Control	In progress			
Event Correlation	Component Control	In progress			
Information Access Control Policy and Procedures	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Log Aggregation and Analysis	Component Control	In progress
Prompt Account Termination	Component Control	In progress
Single Sign-on	Component Control	In progress
User Account Management	Component Control	In progress
User Activity Review	Component Control	In progress
User Permissions Reviews	Component Control	In progress

Software-as-a-Service / No Label		System Cracker/Theft of Sensitive Data	Dormant Accounts	2	4	8	10-05-25	10-05-25	

Risk scenario ID: 33927402

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Accounts Lock After Too Many Failed Logins	Component Control	In progress			
Event Correlation	Component Control	In progress			
Information Access Control Policy and Procedures	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Prompt Account Termination	Component Control	In progress			
Single Sign-on	Component Control	In progress			
User Account Management	Component Control	In progress			
User Activity Review	Component Control	In progress			
User Permissions Reviews	Component Control	In progress			

Application / No Label		Malicious User/Audit Log Tampering	Inadequate Audit Log Safeguards	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33927377

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Audit Log Protection	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Authoritative Time Source	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	In progress			

Application / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Excessive Admin Rights	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33927376

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Principle of Least Privilege	Component Control	In progress			
Privileged Account Management	Component Control	In progress			

Desktop / Applications Group	Data Center	Careless User/Physical Damage to Equipment	Accidents	3	2	6	10-05-25	10-05-25	

Risk scenario ID: 33938048

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plans	Component Control	In progress			
Data Backup	Component Control	In progress			
Redundant or Spare Equipment	Component Control	No			

Desktop / Applications Group	Data Center	Disaster/Equipment Damage	Insufficient Equipment Redundancy	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938073

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plan Testing	Component Control	In progress			
Contingency Plans	Component Control	In progress			
Redundant or Spare Equipment	Component Control	No			
Threat/Vulnerability Intelligence Services	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	Entropy/Hardware Failure	Old or Outdated Equipment	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938049

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plans	Component Control	In progress			
Data Backup	Component Control	In progress			
Redundant or Spare Equipment	Component Control	No			
System and Lifecycle Maintenance	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	Inclement Weather/Unavailability of Key Personnel	Lack of Key Person Redundancy / Cross-training	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938043

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plans	Component Control	In progress			
Cross-functional Training	Component Control	No			
On-call Technical Resources	Component Control	In progress			
Process Documentation	Component Control	In progress			
Remote Administrative Access	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	System Cracker/Corruption, Destruction or Disclosure of Sensitive Data	Hardware Deficiencies	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938069

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Application, Network, or System Vulnerability Testing	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Firmware Patching	Component Control	In progress			
Operating System Patching	Component Control	In progress			
System and Lifecycle Maintenance	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Entropy/Hardware Failure	Old or Outdated Equipment	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938175

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plans	Component Control	In progress			
Data Backup	Component Control	In progress			
Redundant or Spare Equipment	Component Control	No			
System and Lifecycle Maintenance	Component Control	In progress			

Desktop / Cloud Backup Group	Cloud	Inclement Weather/Unavailability of Key Personnel	Lack of Key Person Redundancy / Cross-training	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938169

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plans	Component Control	In progress			
Cross-functional Training	Component Control	No			
On-call Technical Resources	Component Control	In progress			
Process Documentation	Component Control	In progress			
Remote Administrative Access	Component Control	In progress			

Desktop / Cloud Backup Group	Cloud	Malicious User/Audit Log Tampering	Inadequate Audit Log Safeguards	3	2	6	10-05-25	10-05-25	

Risk scenario ID: 33938200

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Audit Log Protection	Component Control	In progress			
Authoritative Time Source	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	In progress			

Desktop / Cloud Backup Group	Cloud	System Cracker/Corruption, Destruction or Disclosure of Sensitive Data	Hardware Deficiencies	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938195

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Application, Network, or System Vulnerability Testing	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Firmware Patching	Component Control	In progress			
Operating System Patching	Component Control	In progress			
System and Lifecycle Maintenance	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	System Cracker/Theft of Sensitive Data	Unsupported Operating System	3	2	6	10-05-25	10-05-25	

Risk scenario ID: 33938198

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Centralized Patch Management	Component Control	In progress			
Operating System Patching	Component Control	In progress			
System and Lifecycle Maintenance	Component Control	In progress			
System Isolation	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Entropy/Hardware Failure	Old or Outdated Equipment	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33927242

Asset(s): Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plans	Component Control	In progress			
Data Backup	Component Control	In progress			
Redundant or Spare Equipment	Component Control	In progress			
System and Lifecycle Maintenance	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Malicious User/Audit Log Tampering	Inadequate Audit Log Safeguards	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33927267

Asset(s): Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Audit Log Protection	Component Control	In progress			
Authoritative Time Source	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Malicious User/Social Engineering	Untrained/Untested Staff	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33927255
Asset(s): Support IT and IT Database
Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Limited User Accessibility (By Time of Day, By Location, etc.)	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			
Session Auditing	Component Control	In progress			
Social Engineering Testing	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Power Surge/Electrical Damage to Equipment	Insufficient Power Shielding	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33927252
Asset(s): Support IT and IT Database
Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Backup	Component Control	In progress			
Redundant or Spare Equipment	Component Control	In progress			
Surge Protectors	Component Control	In progress			
Uninterruptible Power Supply (UPS)	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / LAN Group	Data Center	Careless User/Improper Disclosure or Use of Sensitive Data	Installation of Malware-External Threats	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938133
Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2
Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Acceptable Use Policy	Component Control	In progress			
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			
Block List	Component Control	In progress			
Central Monitoring of Anti-Malware Software	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Content (URL) Filtering	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
Limitations on Administrative Rights	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / LAN Group	Data Center	Careless User/Improper Disclosure or Use of Sensitive Data	Installation of Malware-Internal Threats	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938134

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			
Block List	Component Control	In progress			
Central Monitoring of Anti-Malware Software	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			
Limitations on Administrative Rights	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			
Social Engineering Testing	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / LAN Group	Data Center	Careless User/Social Engineering	Untrained/Untested Staff	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938101

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			
Block List	Component Control	In progress			
Central Monitoring of Anti-Malware Software	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Content (URL) Filtering	Component Control	In progress			
Email Spam Filtering	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Limitations on Administrative Rights	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Operating System Patching	Component Control	In progress			
Prevention of User Storing Data Locally (Terminals, VDI, etc.)	Component Control	No			
Security/Privacy Awareness and Training	Component Control	In progress			
Social Engineering Testing	Component Control	No			

Desktop / LAN Group	Data Center	Disaster/Equipment Damage	Insufficient Equipment Redundancy	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938136

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plan Testing	Component Control	In progress			
Contingency Plans	Component Control	In progress			
Redundant or Spare Equipment	Component Control	In progress			
Threat/Vulnerability Intelligence Services	Component Control	No			

Desktop / LAN Group	Data Center	Information Technology Staff/Data Loss	Insufficient Data Backup	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938116

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Backup Media Testing and Validation Policy and Procedures	Component Control	In progress			
Data Backup	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	No			

Desktop / LAN Group	Data Center	Information Technology Staff/Improper Destruction, Disposal or Reuse of Media	Destruction/Disposal Deficiencies	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938124

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Retention Policy and Procedures	Component Control	In progress			
Encryption of Disks (Full Disk, File Based, etc.)	Component Control	In progress			
Media/Device Reuse and Disposal Policy and Procedures	Component Control	In progress			
Prevention of User Storing Data Locally (Terminals, VDI, etc.)	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Sanitize Device/Disks/Media	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			
Training for the Security Workforce	Component Control	In progress			

Desktop / LAN Group	Data Center	Malicious User/Social Engineering	Untrained/Untested Staff	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33938125

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Limited User Accessibility (By Time of Day, By Location, etc.)	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			
Session Auditing	Component Control	In progress			
Social Engineering Testing	Component Control	No			

Server / No Label		Malicious User/Audit Log Tampering	Inadequate Audit Log Safeguards	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33927338

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Audit Log Protection	Component Control	In progress			
Authoritative Time Source	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	In progress			

Software-as-a-Service / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	User Authentication Deficiencies	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33927404

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Accounts Lock After Too Many Failed Logins	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Multi-factor Authentication	Component Control	In progress			
Password Change Required on 1st Login	Component Control	In progress			
Password Strength Requirements	Component Control	In progress			
Password/Token Management Policy and Procedures	Component Control	In progress			
Prevention of Simultaneous User Logins	Component Control	In progress			
Single Sign-on	Component Control	In progress			
Unique User ID	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		Service Providers or Vendors/Loss of Contracted Services	Service Interruption	2	3	6	10-05-25	10-05-25	

Risk scenario ID: 33927411

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plan Testing	Component Control	In progress			
Contingency Plans	Component Control	In progress			
Locally-stored Backups of Third-party Hosted Data	Component Control	In progress			
Redundant Service Providers	Component Control	In progress			
Service-level Agreements	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	System Cracker/Corruption, Destruction or Disclosure of Sensitive Data	Hardware Deficiencies	1	5	5	10-05-25	10-05-25	

Risk scenario ID: 33927262

Asset(s): Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Application, Network, or System Vulnerability Testing	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Firmware Patching	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Operating System Patching	Component Control	In progress			
System and Lifecycle Maintenance	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Dormant Accounts	1	5	5	10-05-25	10-05-25	

Risk scenario ID: 33927326

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Event Correlation	Component Control	In progress			
Information Access Control Policy and Procedures	Component Control	In progress			
Internal IT Audit Program	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Prompt Account Termination	Component Control	In progress			
Session Auditing	Component Control	In progress			
Single Sign-on	Component Control	In progress			
User Account Management	Component Control	In progress			
User Activity Review	Component Control	In progress			
User Permissions Reviews	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		System Cracker/Corruption, Destruction or Disclosure of Sensitive Data	Hardware Deficiencies	1	5	5	10-05-25	10-05-25	

Risk scenario ID: 33927329

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Application, Network, or System Vulnerability Testing	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Firmware Patching	Component Control	In progress			
Operating System Patching	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
System and Lifecycle Maintenance	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		System Cracker/Malicious Data Encryption	Ransomware	1	5	5	10-05-25	10-05-25	

Risk scenario ID: 33927337

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Application, Network, or System Penetration Testing	Component Control	In progress			
Backup Media Testing and Validation Policy and Procedures	Component Control	In progress			
Device Hardening	Component Control	In progress			
Incident Response Planning	Component Control	In progress			
Incident Response Testing	Component Control	In progress			
Multi-factor Authentication	Component Control	In progress			
On-call Technical Resources	Component Control	In progress			
Privileged Account Management	Component Control	In progress			
Recovery Backup	Component Control	In progress			
Redundant or Spare Equipment	Component Control	In progress			
Secure Administrative Host	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		Careless User/Corruption, Destruction, or Loss of Data	Insufficient Data Validation	1	5	5	10-05-25	10-05-25	

Risk scenario ID: 33927397

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Backup	Component Control	In progress			
Data Input Validation	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Excessive Admin Rights	1	5	5	10-05-25	10-05-25	

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Risk scenario ID: 33927408

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Principle of Least Privilege	Component Control	In progress			
Privileged Account Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	Malicious User/Audit Log Tampering	Inadequate Audit Log Safeguards	2	2	4	10-05-25	10-05-25	

Risk scenario ID: 33938074

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Audit Log Protection	Component Control	In progress			
Authoritative Time Source	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Applications Group	Data Center	Power Surge/Electrical Damage to Equipment	Insufficient Power Shielding	2	2	4	10-05-25	10-05-25	

Risk scenario ID: 33938059

Asset(s): Accounting Software and Accounting SQL Database,Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Marketing Software and Marketing Database,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SQL Server

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Backup	Component Control	In progress			
Redundant or Spare Equipment	Component Control	No			
Surge Protectors	Component Control	In progress			
Uninterruptible Power Supply (UPS)	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Careless User/Physical Damage to Equipment	Accidents	2	2	4	10-05-25	10-05-25	

Risk scenario ID: 33938174

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plans	Component Control	In progress			
Data Backup	Component Control	In progress			
Redundant or Spare Equipment	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Cloud Backup Group	Cloud	Power Surge/Electrical Damage to Equipment	Insufficient Power Shielding	2	2	4	10-05-25	10-05-25	

Risk scenario ID: 33938185

Asset(s): Cloud-based Backup Service (iDrive),SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases)

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Backup	Component Control	In progress			
Redundant or Spare Equipment	Component Control	No			
Surge Protectors	Component Control	In progress			
Uninterruptible Power Supply (UPS)	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / Desktop Group	Office	Disaster/Equipment Damage	Insufficient Equipment Redundancy	1	4	4	10-05-25	10-05-25	

Risk scenario ID: 33927266

Asset(s): Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plan Testing	Component Control	In progress			
Contingency Plans	Component Control	In progress			
Redundant or Spare Equipment	Component Control	In progress			
Threat/Vulnerability Intelligence Services	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / LAN Group	Data Center	Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Dormant Accounts	1	4	4	10-05-25	10-05-25	

Risk scenario ID: 33938129

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Event Correlation	Component Control	In progress			
Information Access Control Policy and Procedures	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Prompt Account Termination	Component Control	No			

Control	Type	Response	Control Notes	Author	Created Date
Session Auditing	Component Control	In progress			
Single Sign-on	Component Control	In progress			
User Account Management	Component Control	In progress			
User Activity Review	Component Control	In progress			
User Permissions Reviews	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Disaster/Equipment Damage	Insufficient Equipment Redundancy	1	4	4	10-05-25	10-05-25	

Risk scenario ID: 33927336

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plan Testing	Component Control	In progress			
Contingency Plans	Component Control	In progress			
Redundant or Spare Equipment	Component Control	In progress			
Threat/Vulnerability Intelligence Services	Component Control	No			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Entropy/Hardware Failure	Old or Outdated Equipment	1	4	4	10-05-25	10-05-25	

Risk scenario ID: 33927306

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Automatic Alerting for Adverse Events	Component Control	In progress			
Contingency Plan Testing	Component Control	In progress			
Contingency Plans	Component Control	In progress			
Data Backup	Component Control	In progress			
Distributed Processing or Storage	Component Control	In progress			
Information Systems Monitoring	Component Control	In progress			
Redundant or Spare Equipment	Component Control	In progress			
Service-level Agreements	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Control	Type	Response	Control Notes	Author	Created Date
System and Lifecycle Maintenance	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Information Technology Staff/Improper Destruction, Disposal or Reuse of Media	Destruction/Disposal Deficiencies	1	4	4	10-05-25	10-05-25	

Risk scenario ID: 33927318

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Retention Policy and Procedures	Component Control	In progress			
Encryption of Disks (Full Disk, File Based, etc.)	Component Control	In progress			
Media/Device Reuse and Disposal Policy and Procedures	Component Control	In progress			
Sanitize Device/Disks/Media	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Information Technology Staff/Improper Disclosure or Use of Sensitive Data	Installation of Malware	1	4	4	10-05-25	10-05-25	

Risk scenario ID: 33927334

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Allow List	Component Control	In progress			
Anti-Malware Software	Component Control	In progress			
Automatic Alerting for Adverse Events	Component Control	In progress			
Block List	Component Control	In progress			
Central Monitoring of Anti-Malware Software	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Host-based Firewalls Enabled	Component Control	In progress			
Locked Down External Ports (USB, CD, DVD, Firewire, etc.)	Component Control	In progress			
Operating System Patching	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Malicious User/Improper Access to, or Use or Destruction of Sensitive Data	Excessive Admin Rights	1	4	4	10-05-25	10-05-25	

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Risk scenario ID: 33927332

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Principle of Least Privilege	Component Control	In progress			
Privileged Account Management	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		Malicious User/Corruption, Destruction, or Loss of Data	Insufficient Data Validation	1	4	4	10-05-25	10-05-25	

Risk scenario ID: 33927409

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Backup	Component Control	In progress			
Data Input Validation	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		Malicious User/Social Engineering	Untrained/Untested Staff	1	4	4	10-05-25	10-05-25	

Risk scenario ID: 33927398

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / LAN Group	Data Center	Careless User/Physical Damage to Equipment	Accidents	1	3	3	10-05-25	10-05-25	

Risk scenario ID: 33938111

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contingency Plans	Component Control	In progress			
Data Backup	Component Control	In progress			
Redundant or Spare Equipment	Component Control	In progress			

Desktop / LAN Group	Data Center	Malicious User/Audit Log Tampering	Inadequate Audit Log Safeguards	1	3	3	10-05-25	10-05-25	

Risk scenario ID: 33938137

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Audit Log Protection	Component Control	In progress			
Authoritative Time Source	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	No			

Desktop / LAN Group	Data Center	System Cracker/Corruption, Destruction or Disclosure of Sensitive Data	Hardware Deficiencies	1	3	3	10-05-25	10-05-25	

Risk scenario ID: 33938132

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Application, Network, or System Vulnerability Testing	Component Control	In progress			
Centralized Patch Management	Component Control	In progress			
Firmware Patching	Component Control	In progress			
Operating System Patching	Component Control	In progress			
System and Lifecycle Maintenance	Component Control	No			

Internal Network - Wired / No Label		Malicious User/Audit Log Tampering	Inadequate Audit Log Safeguards	1	3	3	10-05-25	10-05-25	

Risk scenario ID: 33927352

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Audit Log Protection	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Authoritative Time Source	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Tamper-proof Mechanisms	Component Control	In progress			

Internal Network - Wired / No Label		Malicious User/Vandalism	Physical Security Deficiencies	1	3	3	10-05-25	10-05-25	

Risk scenario ID: 33927347

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Limited Access to Network Cabling and Devices	Component Control	In progress			
Physical Access Control	Component Control	In progress			
Physical Access Monitoring	Component Control	In progress			
Physically Secured Demarcation Points	Component Control	In progress			

Internal Network - Wired / No Label		Man Made Disaster/Network Unavailable	Network Outage	1	3	3	10-05-25	10-05-25	

Risk scenario ID: 33927350

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Automatic Alerting for Adverse Events	Component Control	In progress			
Contingency Plan Testing	Component Control	In progress			
Contingency Plans	Component Control	In progress			
Information Systems Monitoring	Component Control	In progress			
Redundant Network Communications Providers	Component Control	In progress			
Resilient Network Topography	Component Control	In progress			

Internal Network - Wired / No Label		System Cracker/Improper Access to Sensitive Data	Network Sniffing	1	3	3	10-05-25	10-05-25	

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Risk scenario ID: 33927349

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Domain/Device Authentication	Component Control	In progress			
Limited Access to Network Cabling and Devices	Component Control	In progress			
Network Access Control	Component Control	In progress			
Network Segmentation	Component Control	In progress			
Physically Secured Demarcation Points	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Server / No Label		Power Surge/Electrical Damage to Equipment	Insufficient Power Shielding	1	3	3	10-05-25	10-05-25	

Risk scenario ID: 33927315

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Automatic Alerting for Adverse Events	Component Control	In progress			
Contingency Plans	Component Control	In progress			
Data Backup	Component Control	In progress			
Distributed Processing or Storage	Component Control	In progress			
Information Systems Monitoring	Component Control	In progress			
Redundant or Spare Equipment	Component Control	In progress			
Service-level Agreements	Component Control	In progress			
Surge Protectors	Component Control	In progress			
Uninterruptible Power Supply (UPS)	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		Service Providers or Vendors/Possible Sanctions by Regulators	Contractual Agreement Deficiencies	1	3	3	10-05-25	10-05-25	

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Risk scenario ID: 33927400

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Contractual Agreements	Component Control	In progress			
Review of Service Providers	Component Control	In progress			
Security During Systems Acquisition	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		System Cracker/Corruption, Destruction, or Loss of Data	Insufficient Data Validation	1	3	3	10-05-25	10-05-25	

Risk scenario ID: 33927410

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Backup	Component Control	In progress			
Data Input Validation	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Software-as-a-Service / No Label		System Cracker/Social Engineering	Untrained/Untested Staff	1	3	3	10-05-25	10-05-25	

Risk scenario ID: 33927405

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Access Logging	Component Control	In progress			
Log Aggregation and Analysis	Component Control	In progress			
Security/Privacy Awareness and Training	Component Control	In progress			

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes
Desktop / LAN Group	Data Center	Power Surge/Electrical Damage to Equipment	Insufficient Power Shielding	1	2	2	10-05-25	10-05-25	

Risk scenario ID: 33938122

Asset(s): Active Directory/Primary DNS,Internet Information Server #1 (Intranet),Internet Information Server #2,Network Attached Storage #1,Network Attached Storage #2

Component Group Name	Physical Location	Threat	Vulnerability	Likelihood	Impact	Rating	Created Date	Updated Date	Risk Notes

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Data Backup	Component Control	In progress			
Redundant or Spare Equipment	Component Control	In progress			
Surge Protectors	Component Control	In progress			
Uninterruptible Power Supply (UPS)	Component Control	In progress			

Internal User / No Label		Former Employee/Improper Access to or Disclosure of Sensitive Data	Inadequate Termination Procedures	1	2	2	10-05-25	10-05-25	

Risk scenario ID: 33927424

Asset(s): Accounting Software and Accounting SQL Database,Active Directory/Primary DNS,Cloud-based Backup Service (iDrive),Electronic Health Record System,ERP Software and ERP SQL Databases,Exchange Email Server and Database,Financial Software and Financial Database,Human Resources Information Systems Database,Internet Information Server #1 (Intranet),Internet Information Server #2,Marketing Software and Marketing Database, Network Attached Storage #1,Network Attached Storage #2,Office 365 Server and Office Database,Operation Management Software and Operation Management SQL Database,Payroll,SAN #1 (Weekly backup for client PCs and Office Files,SAN #2 (Daily backup for all data and databases),SQL Server,Support IT and IT Database

Asset Tag(s): No Asset Tag

Control	Type	Response	Control Notes	Author	Created Date
Non-Disclosure Agreements	Component Control	In progress			
Personnel Separation Procedures	Component Control	In progress			
Prompt Account Termination	Component Control	In progress			