| **Ref** | **Control Category** | **Question(s)** | **Answer** |
| --- | --- | --- | --- |
| GV1.0 | Organizational Structure | Is there an organizational chart?  How many lines of authority?  Where/Who do each of the following IT functions report to:  -Information Security  -Infrastructure Support  -Network Support  -Development  -Application Support |  |
| GV2.0 | Goals and Objectives | Does the organization have an IT steering committee?   How are IT budgets determined?  How often does IT meet with management to discuss IT plans and review IT policies and procedures? |  |
| GV3.0 | Internal Risk Assessment | Are any internal/external risk assessments performed? Penetration testing?  Are written risk assessments performed?  How are threats identified? Have any new threats been evaluated this year.  Who is responsible for assessing risks and preparing the assessment?  Who reviews the risk assessment?  Who determines mitigation strategies?  Who reviews the status of mitigation performed? |  |
| GV4.0 | Regulatory Compliance | Who is responsible for monitoring the regulatory environment?  What regulations is the entity subject to?  Are reviews of IT policies and procedures periodically conducted to ensure compliance requirements are documented within procedures? How often? By whom?  Is the entity subject to any type of regulatory audits? What and how often? |  |
| GV5.0 | Policies and Procedures | Compare the policies and procedures to written goals and strategic objectives….verify there is a policy covering each objective.  Compare the policies and procedures to the risk assessment results. Determine if policies are in place to address risks.  Request and review all IT policies. Determine if the minimum policy requirements are addressed:   * Acceptable Use Policy- * Data Classification Policy- * Data Security/Encryption Policy*-* * Social Media Policy * Password Policy- * Remote Access Policy*-* * Personal Device/BYOD Policy- * Email Policy – * Configuration Standards Policy *–* * Privileged Identify Management Policy- * Security Monitoring Policy- * Vendor Management Policy- * Data Backup Policy * Patch Management Policy * Vulnerability Management Policy * Incident Management Policy * Change Management Policy * Access Management Policy * Data Retention and Minimization Policy |  |
| GV6.0 | Metrics and Measurements | 1. What metrics are in place in the strategic plan to measure success of strategic objections? 2. What metrics are in place to measure success of IT department(s)? 3. How often are measurements taken? By whom? 4. How are measurements reported? 5. Who reviews measurement data? Does the subject see and have opportunity to challenge data? |  |
| HR1.0 | Background Checks-Professional | Are the formal job requirements for each IT job description?  What processes are in place to ensure candidates meet job requirements (e.g. background/ reference checks, educational verifications, skill tests)? |  |
| HR2.0 | Background Checks- Criminal | What types of background checks are performed (e.g. criminal, credit checks, social media investigations)? |  |
| HR3.0 | Background Checks-Contractors | What is the process for vetting contractors? (e.g. interviews, resume, background checks, references)  If the outsourcing firm is required to perform background checks, what processes are in place to ensure they are meeting contractual obligations (e.g. contractor, confirmation, background checks received/reviewed? |  |
| HR4.0 | Communication of Policies | Walk through the onboarding process..what policies and procedures are reviewed upon hire?  Are employees required to sign acknowledgment of policies or other contractual documents like non-disclosure agreements? |  |
| HR5.0 | Internal Policy Awareness | Is a security awareness training program in place?  Who is subject to training?  Are employees required to retake the training annually?  Are training logs maintained? |  |
| HR6.0 | Employee Evaluations | How are job requirements and department objectives communicated to employees? Is there a set of standard objectives given to each employee? Do these objectives align with the strategic goals and objectives of the organization?  How often are employees evaluated?  Are evaluations in writing?  Are objectives included in the evaluation?  Are employees required to acknowledge evaluations? |  |
| NT1.0 | Security Design | Is there a network diagram?  Is there a DMZ?  Firewall placement- how are they placed in the DMZ and at network boundary?  Are host-based firewalls used?  Is the network segmented? Not just subnets…but network segments that restrict access…either requires separate authentication or limits access via firewall/ACL to only specific users.  Is there a wireless network? Do you have a separate guest network? How are they segregated (at the router level or separate firewall)? |  |
| NT2.0 | Device Deployment/ Configuration | Does the organization have checklists specific to various network components?  Who is responsible for installing and configuring network devices: -Switches  -Routers  -Firewalls  What minimum hardening is required for each?  Regarding any special configurations (ACL’s for routers)…how are those communicated?  Are configuration settings subject to periodic audit or peer review? |  |
| NT3.0 | Firewall | Is the firewall(s) configured to a "least privilege" model, or an implicit "deny all" rule is present?  How often are firewall rules reviewed/ modified? Are they subject to a periodic review?  Are firewall logs archived and retained for at least 12 months (PCI requirement)?  Are firewall logs monitored? Describe?  Are alerts triggered when the firewall rules are changed?  What other alerts/monitoring?   * Aggregated rule hits? * AlgoSec configuration reviews/optimization. |  |
| NT3.1 | Web Application Firewall  For IT risk assessment | Does the organization have any internally-developed/maintained web applications?  Is a Web Application Firewall in place to detect common web code vulnerabilities, such as cross-site scripting and SQL injection?  Does the WAF scan test systems prior to production updates?  Who monitors WAF alerts?  What is the SLA for resolving WAF alerts? |  |
| NT4.0 | Antivirus | What virus protection is in place at the organization?  How are scans performed? (i.e. manually, scheduled, detection)  Where is antivirus installed- severs, workstations, other network connected devices (e.g. mobile phones, tablets, IoT)? |  |
| NT5.0 | Email Filters | What tool is used to scan email?  Who monitors for suspicious content?  Do incident management procedures require investigation and root cause analysis of suspicious email reports?  How often are filter rules updated?  Do end users have access to modify or delete rules for their inbox? |  |
| NT5.5 | Internet Content Filters | Are filters used to prevent misuse of internet access:  -Block access based on key word  -Block specific sites |  |
| NT6.0 | IPS/IDS | Is a dedicated IDS/IPS appliance used or is IDS/IPS implemented through the router?  How are often are signatures updated?  How long are IDPS logs retained (12 months for PCI)?  Are IDPS logs monitored?  Who monitors the logs (internal or vendor?)  Who configures IDPS alerts? What is SLA for alert investigation/resolution? |  |
| NT7.0 | SIEM | Is there a SIEM tool in place?  What logs is it collecting/not collecting?  Are the logs stored in a secure location?  Are any alerts configured in the SIEM tool? What specific alerts are configured (e.g. failed logons, administrative logons, export of information)?  Who monitors alerts? What is the SLA for investigation/resolution? |  |
| NT8.0 | DLP | Who is responsible for configuring the tool?  What fields and values are configured?  Can the tool read encrypted communications (e.g. encrypted email, fie sharing tools)?  Is data quarantined to a specific area? Who has access to release quarantined data? |  |
| NT9.0 | Authentication- network components | How do you authenticate to network equipment:  Firewalls  Routers/switches  Wireless controllers  Is authentication local or via a directory service (TACACS) or LDAP?  Are generic administrator accounts used to access network devices? If yes, where are passwords stored- who has access- and how often are they changed? |  |
| NT10.0 | Port Scans | Are port scans performed?  What tool?  How often?  Who reviews?  Who tracks remediation? |  |
| NT11.0 | Capacity Planning | Are capacity planning exercises performed?  If yes, how often?  Describe the process:  -paper reviews  -stress testing  -log reviews  What is included in the scope- servers, critical applications, etc.? |  |
| NT12.0 | Performance Monitoring | What tool is used (e.g. Solarwinds, SCOM)?  Who configures the tool?  Who monitors alerts?  What basic alerts are configured (e.g. memory, latency, heart beat monitor)?  What is SLA for resolving alerts? Incident Management Segway- how are they classified/prioritized? |  |
| LS1.0 | Network Authentication | What directory service is used to authenticate users (e.g. Active Directory, Apache Directory, Open LDAP)  What is the user ID naming convention?  Are any shared ID’s in use (end user access only…note that Admin and Firecall ID’s will be covered later)?  What are the password rules with respect to:   * Password length * Complexity (alpha, numeric, special) * Expiration (30 days, 90 days) * Initial (first password) should be set to 0 days to require immediate reset. * History/reuse (5 passwords, 10 passwords, etc.) * Lockout (5 invalid attempts) * Lockout time (locked to 30 minutes after 5 invalid attempts)   Are any passwords set to never expire? Explain (should be limited to service and admin accounts only) |  |
| LS2.0 | Network Authentication- Remote | What methods of remote authentication?   * VPN * Virtual Desktop/Citrix Client * Direct connection via firewall   Is split tunneling disabled on the VPN configuration?  For each method of remote authentication- identify who uses- general users, administrators/privileged users, vendors/service providers.  Remote access mechanisms widely used in the organization or restricted?  If restricted, who has access and who is required to approve?  Is multi factor authentication used for remote access? If yes, what tool? |  |
| LS3.0 | Server Authentication-Local | What server OS are used (e.g. Windows, Unix, Linux)? Obtain the versions in use.  Are servers authenticated locally or LDAP via central directory service? If yes to 2nd, what directory service is used?  If local authentication is used, do all administrators authenticate through unique ID’s?  If local authentication is used, what are the password rules with respect to:   * Password length * Complexity (alpha, numeric, special) * Expiration (30 days, 90 days) * Initial (first password) should be set to 0 days to require immediate reset. * History/reuse (5 passwords, 10 passwords, etc.) * Lockout (5 invalid attempts) * Lockout time (locked to 30 minutes after 5 invalid attempts)   Same questions above for directory service if not covered in network authentication.  Are administrators (whether local or LDAP) authenticating using separate “Administrator” accounts?  If “Admin” accounts are used, do these accounts have any of the following access levels:   * Interactive network logon rights. * Internet access * Email access |  |
| LS4.0 | Server Authentication - Remote | Are users required to authenticate through the VPN for remote access to servers?  Are any remote access tools, like Team Viewer, used to access and troubleshoot servers remotely?  For servers located in the DMZ or outside of the firewall- how are those authenticated?  Is multi-factor authentication required for remote access to servers? |  |
|  | Database Authentication- Local | What databases are used (e.g. SQL, Oracle)? Obtain the versions in use.  Are servers authenticated locally or LDAP via central directory service? If yes to 2nd, what directory service is used?  If local authentication is used, do all administrators authenticate through unique ID’s?  If local authentication is used, what are the password rules with respect to:   * Password length * Complexity (alpha, numeric, special) * Expiration (30 days, 90 days) * Initial (first password) should be set to 0 days to require immediate reset. * History/reuse (5 passwords, 10 passwords, etc.) * Lockout (5 invalid attempts) * Lockout time (locked to 30 minutes after 5 invalid attempts)   Same questions above for directory service if not covered in network authentication.  Are administrators (whether local or LDAP) authenticating using separate “Administrator” accounts? |  |
| LS5.0 | Authentication- Web Application | Is a unique ID and password required to access the application?  Does the website utilize multi-factor authentication or user verification?  What is the user ID naming convention?  Are any shared ID’s in use?  What are the password rules with respect to:   * Password length * Complexity (alpha, numeric, special) * Expiration (30 days, 90 days) * Initial (first password) should be set to 0 days to require immediate reset. * History/reuse (5 passwords, 10 passwords, etc.) * Lockout (5 invalid attempts) * Lockout time (locked to 30 minutes after 5 invalid attempts)   Are any passwords set to never expire? Explain (should be limited to service and admin accounts only) |  |
| LS6.0 | Authentication- Application | Are users required to authenticate to the network in order to access the application? Are there any backdoors?  Does the application use local authentication or are users authenticated via LDAP from directory service?  For local authentication- Is a unique ID and password required to access the application?  What is the user ID naming convention? Does the user ID match the network logon?  Are any shared ID’s in use?  What are the password rules with respect to:   * Password length * Complexity (alpha, numeric, special) * Expiration (30 days, 90 days) * Initial (first password) should be set to 0 days to require immediate reset. * History/reuse (5 passwords, 10 passwords, etc.) * Lockout (5 invalid attempts) * Lockout time (locked to 30 minutes after 5 invalid attempts)   Are any passwords set to never expire? Explain (should be limited to service and admin accounts only) |  |
| LS7.0 | Administrative Access Control | Is there a specific policy for management of “Privileged” identities or administrative accounts with respect to provisioning, tracking and password changes?  Who has admin privileges for the network and servers?  Who has admin privileges to the network devices (firewall, routers)?  Who has admin privileges to applications?  Are “Admin” accounts segregation from general access accounts? If “Admin” accounts are used, do these accounts have any of the following access levels:   * Interactive network logon rights. * Internet access * Email access   Are any generic or service accounts used?  Do generic accounts have interactive logon permissions to the network or application? If yes, where are passwords stored? Is there are mechanism to track generic accounts with respect to purpose, ownership, application, authorized users and last password change?  Is there any special monitoring for administrative accounts- like monitoring of logons or new administrative rights assignments? |  |
| LS8.0 | Security Administration | Who has rights to provision users/ modify security role structure for  -Directory Service (AD)  -Databases  -Critical Applications  Who must approve provisioning of security administration rights?  Are personnel with security administration rights subject to regular (i.e. quarterly) user access reviews?  Is there any special monitoring for security administrators, such as:   * Audits of accounts created/provisioned for approval. * Alerts of modifications to own accounts. * Alerts of modifications to batch or generic ID’s. |  |
| LS9.0 | Batch Administration | Is there a policy or procedure for restricting access to create/modify batch schedules?  Who has access to create or modify batch processes at the following levels:  -Server/OS scripts  -Database  -Application  -Scheduling tool (e.g. TWS, Maestro).  Who must approve provisioning of scheduling access?  Is there any special monitoring for batch administrators, such as:  -Alerts of new jobs added to schedule.  -Periodic audit of new jobs and structural changes (i.e. changes to steps and processes) for approval.  What logons are used to run scheduled processes:   * Generic Batch or Service account? * Running under administrator’s ID.   Do generic batch ID’s have interactive logon rights to the network or applications? |  |
| LS10.0 | Backup Administration | Is a backup utility used? Which one?  Does the backup utility control backups for all system components: servers, databases, application front end?  Who has access to backup scheduling software?  Where are backups stored: NAS, SAN, mirrored server, cloud, tape or mix?  Are backups offline or segmented from the main network?  Who has access to the backup repository:   * NAS/SAN * Cloud * Mirrored Server   Who has access to tape off-site storage facility?  Is access to backup repositories subject to period review and validation? How often reviewed? |  |
| LS11.0 | End User/Application level security design | How is security structured at the network level:  -Organizational Units  - Security Groups  - Folder -Structure/Owners  What are the critical applications? For a sample of critical applications, ask the following:  - Are security roles/groups in use?  -Are roles job based on task based?  -If job based…How do you handle instances of 2 people with same job title requiring different access levels?  -How many total roles are there?  - How many different roles in the average user assigned? |  |
| LS12.0 | User Access Policies/ Provisioning and De-provisioning | Are user access policies in place?  Do policies require, at a minimum:  -Formal access request  - Approval of account creation  -Guidance for access assignments (e.g. matrix by job title or approval requirements).  -Termination SLA (notification and removal of access within X days of termination date).  -Policy scope- applications, network, server. |  |
| LS13.0 | Network Provisioning | What is the process for creating network accounts and assigning access?  Are access request forms completed?  Who must approve the network account?  Who must approve network access?  Are there standard access assignments for certain job functions?  What access levels provide secondary approval?  Are network access levels (e.g. file share folders, SharePoint) managed by end users versus IT? |  |
| LS14.0 | Application Provisioning | What is the process for requesting application access?  Are access request forms completed?  Are forms manual or automated?  Do forms include a list of authorizations to select from?  Do forms allow- “mirror access” as?  Who must approve new application accounts?  Who must approve role assignments?  Who provisions accounts?  Is a general display role assigned? If yes, are authorizations to sensitive views removed from this role? |  |
| LS15.0 | Database Provisioning | What is the process for creating database accounts and assigning access?  Who, besides database administrators, have access to the database?  Are access request forms completed?  Who must approve the database account?  Who must approve the database access level?  -DBA  -Data Views  Are there standard access assignments for certain job functions/applications?  What access levels provide secondary approval? |  |
| LS16.0 | User De-provisioning | What is the process for notifying IT of transfers and terminations:  -Does HR or hiring manager send an access termination form?  -Does HR provide a report of transfers/terminations?  -Is it an email notification?  What checks are in place to ensure IT is being notified of all transfers and terminations:  -Weekly/monthly report from HR?  What is the SLA for removing access from terminated or transferred users:  -Same day, next day  -Date of termination/transfer  Who is responsible for collecting computer equipment:  -Badges  -RSA Tokens  -laptops or mobile devices  Are alternate procedures in place for handling involuntary terminations? |  |
| LS17.0 | Administrator Access Reviews- application level | Are administrator access reviews conducted for critical applications, specifically financial applications?  Who is deemed an “administrator” at the application level?  How are access listings queried:  -on role assignment  -on department  -on transaction  Who performs reviews?  How often are they performed? |  |
| LS18.0 | User Access Reviews | Are user access reviews conducted for critical applications, specifically financial applications?  What is the scope of reviews:   * Just checking for invalid users (terminations/transfers) * Invalid users+ review of key access functions (transactions/roles) * Complete access review- review of all users and role assignments for validity.   How often are reviews performed?  Who performs reviews?  -System Owner  -Process Owner  -Department Managers  -All of the above  What applications are reviewed?  How often are reviews conducted? |  |
| DS1.0 | Data Classification | What types of sensitive data does the organization receive, process, store, or transmit:  -passwords  -intellectual property  -PHI (medical diagnosis)  -PII (SSN, name, address)  -Bank accounts  -Payment Card Account Numbers (PAN)  -Credit scores  -Background check information  -Confidential personal information  -Confidential business information  Is a data classification policy in place?  What classification categories are used? |  |
| DS1.5 | Confidential Data Access Restrictions | Where is confidential information stored:  -Network folders  -Applications  -Databases  -Backup media  Has a data inventory been performed to identify stores of confidential or sensitive data?  Has a strategy been developed to restrict access to confidential data stores?   * Data tokenized and moved to central database. * Data masked or views restricted at application level. * Direct database or query access restricted to authorized users.   How is security designed to restrict information:  -At network level (network segmentation/ACL’s/host-based firewalls, organizational units, folder structure)  - At application level (general display roles, sensitive data display, data masked on screen)  -At database level (data views, data queries) |  |
| DS2.0 | Confidential Data- Access Restrictions | How is access to confidential data restricted?  Provide some examples?  Ballpark figure- how many users have access to view confidential data:  -Via network shares?  -Via application screens?  -Via application queries?  -Via database views?  -Via FTP sites?  -Via data transmissions/packets? |  |
| DS3.0 | Confidential Data- Monitoring | Are user accounts with access to sensitive data stores tracked and subject to periodic user access reviews?  Are logs to highly sensitive areas (e.g. token database, encryption keys) logged and actively monitored (alerts configured)?  Are any other types of reviews performed- periodic audits of logs, analysis of user activity performed? |  |
| DS4.0 | Release/ Transmission of Confidential Data | Do data classification and security policies/procedures cover release and transmission of confidential data?  How often are users briefed on procedures?  What authorization is required to release or transmit confidential data? Is it written or verbal?  What mechanisms are used to transmit confidential information:  -encrypted email  -secure FTP  -scan or fax |  |
| DS4.1 | Cloud drives | Is use and/or installation of cloud drives (e.g. Dropbox, Drive, OneDrive, Box) permitted?  If no to above, how are cloud drive installations monitored and prevented?  Can the DLP tool detect or block uploads or transfers of sensitive data to cloud drives (either via internet of desktop installation)? |  |
| DS4.2 | Flash Drives | Is use of flash/USB drives permitted?  If no, how are they prevented:  -via group policy  -via desktop/laptop/server/device configuration  If flash drives are permitted, is there a policy governing use of flash drives? What policy?  Are the following provisions in policy:  -No transfer of confidential information to flash drives  -Mandated use of encrypted flash drives |  |
| DS5.0 | Data Encryption- at rest | Is a data security/encryption policy in place?  What data requires encryption/tokenization?  Has a data inventory been performed to identify data stores and workflows of sensitive data?  What encryption method(s) are used for data storage? Have approved methods been explicitly defined in policy?  Is an Encryption Key Management policy in place?  How is access to encryption keys restricted?  -Network segmentation used to isolate and restrict access to EK. Do users need to re-authenticate or enter a code/RSA token for access to the location?  - Access to EK storage locations monitored? Are alerts fired when users authenticate or access locations.  -Are encryption keys stored on the same server/database as the encrypted data- or are they isolated to a separate network location? |  |
| DS6.0 | Data encryption- in transit | Are policie(s) in place regarding transmission of confidential data?  -Email Policy  -Data Security Policy  -Non-disclosure Policy  What protocols are used for internal data transmission?  Is encrypted email in use? Are staff aware of what to send encrypted/unencrypted?  What protocols are uses for external transmissions?  What protocols are used for authentication:   * Network (if Windows, probably Kerberos). * Web applications |  |
| DS7.0 | Data Retention/ Minimization | Is a data retention policy in place?  When was the last data purge? |  |
| DS8.0 | Asset Disposal | Is there a data disposal procedure? Does it apply to anything with a hard-drive, including fax machines, copiers, phones?  What is the disposal process?  -DBAN or other tool  -Hard drives physically destroyed  -Transferred to a 3rd party vendor for sanitization  What is the tape and electronic media disposal procedure? |  |
| PE1.0 | Facility Security- Data Center | Obtain the following through inquiry or observation:   1. Facility location- urban, suburban, or remote setting. 2. Is facility marked or unmarked (entity logo on data center facility)? 3. Are concrete barriers placed near outside doors? 4. Does the facility have an alarm system? Is it monitored 24X7? 5. Does the facility have a security guard on site 24X7? 6. If no security guard, are surveillance cameras monitored 24X7? 7. What systems are in place to access facility:    1. Badge readers    2. Biometric scanners 8. Is the data center divided into separate zones requiring badge access? 9. Are deadman doors in place to prevent piggy backing? 10. Are employees/visitors required to display a badge at all times?   11) Are there any alternate ways to enter data center or server room:  - Emergency doors  - Windows  - Drop Ceiling  - Air Shaft  12.) If yes to above, are motion detectors or alarms installed to detect access through these channels? |  |
| PE2.0 | Facility Security- Office | Obtain the following through inquiry or observation:   1. Does the facility have an alarm system? Is it monitored 24X7? 2. What systems are in place to access facility:    1. Badge readers    2. Biometric scanners 3. Are deadman doors in place to prevent piggy backing? 4. Are employees/visitors required to display a badge at all times? |  |
| PE3.0 | Facility Access System | 1. Who administers the badge system? 2. Approximately how many users can assign access to the facility? 3. What is the name of the system used? 4. Is there a maintenance agreement? 5. How often are maintenance/ checks performed by the vendor? 6. What happens during power outage or other event when the badge access system goes down? (doors should lock from outside only as default with key override. Personnel on inside should be able to exit). |  |
| PE4.0 | Facility Access Provisioning | Do new facility users or changes require the following:  -Formal access request  - Approval of access (facility)  -Guidance for zone access assignments (e.g. matrix by job title or approval requirements).  -  -Policy scope- applications, network, server. |  |
| PE5.0 | Facility Access De-provisioning | What is the termination SLA (notification and removal of access within X days of termination date)?  Who is tasked with collecting facility badges and keys?  Who is tasked with removing access from the badge system? |  |
| PE6.0 | Security Monitoring | What types of monitoring controls are in place:  -Security cameras  -Alarms on doors and windows.  -Motion detectors  Who has access to security camera feed? Can it be deleted or modified?  Are security cameras actively monitored- or just in place for forensic purposes?  At what times are motion detectors and alarm systems activated? De-activated?  Are motion detectors/alarms monitored 24X7? By whom? Is there a contract with this provider?  Are facility access reports monitored for suspicious activity:  -after-hours access  - frequent entry  -failed entry |  |
| PE7.0 | Facility Access Reviews | Are facility access listings periodically reviewed for unreported terminations and/or unauthorized access?  How often?  Who performs?  What happens when an unreported termination is detected? |  |
| PE8.0 | Visitor Access | What is the process for registering visitors?  How is the visitor’s identity validated?  Are visitor’s logged with respect to name, organization, and person visiting?  Are visitors required to be escorted by company employees?  Are visitor badges noticeably different than employee badges?  Are visitor badges restricted to public areas only (or no access extended)?  Do visitor badges expired at pre-defined closing time? |  |
| PE9.0 | Video Surveillance Maintenance | What video surveillance system is in place?  Are cameras placed at all entrances and exits?  Is an agreement in place to maintain the surveillance system?  When was the surveillance system last serviced? |  |
| PE10.0 | Alarm System | What alarm system is in place?  Are alarms/motion detectors placed on all entrances/exits and windows?  Is an agreement in place to maintain the alarm system?  When was the alarm system last serviced?  Is an agreement in place to monitor the alarm system? What provider is used? |  |
| PE11.0 | Redundancy | For critical systems with high-availability requirements, are systems placed in data centers with the following levels of redundancy:  Telecommunications- 2 or more ISP’s or communication providers  Power- dual power lines on separate circuits, UPS  Internal network- failover built into network design + onsite spares of network equipment (firewalls, routers, switches)  Server- mirrored servers (offsite or onsite) |  |
| PE12.0 | Fire Suppression System | What fire suppression system(s) are in place?  -dry pipe sprinklers  -sprinklers  -fire extinguisher (how many and where)  -Halon  Are fire suppression devices placed throughout the facility?  Is an agreement in place to maintain the fire suppression system?  When was fire suppression system last serviced/inspected?  Is an agreement in place to monitor the fire suppression system? What provider is used? |  |
| PE13.0 | Water Threats | Are any wet pipes running above the data center/server room?  Is the data center located in the ground floor or basement?  What water sensor system is in place?  Are water sensors placed throughout the data center?  When were water sensors last serviced/inspected?  Are alerts fired when sensors are triggered? Who receives alerts? Are alerts sent to contacts after hours? |  |
| PE14.0 | HVAC System | Are redundant HVAC systems in place? Describe:  -Full dual HVAC with fail over  -portable HVAC units  -portable fans  Is an agreement in place to maintain the HVAC system(s)?  When was the HVAC last serviced/inspected?  Are temperature sensors in place?  Are temperature sensors placed throughout the data center?  When were temperature sensors last serviced/inspected?  Are alerts fired when sensors are triggered? Who receives alerts? Are alerts sent to contacts after hours? |  |
| PE15.0 | UPS | What make/model of UPS units are in use?  How old are the units?  When was the last time the batteries were replaced?  Is the UPS covered under a maintenance agreement? When were the units last inspected/serviced?  How often is the UPS tested? What where the results of the last test? |  |
| PE16.0 | Generators | What is the make/model and capacity of the generator?  How long can it power the data center?  What is the time lag to fail over to the generator? Is this in line with the UPS power life (example- generator takes 2 hours to power up and UPS only last 30 minutes)?  Is the generator regularly tested? How often? What were the results of the last test?  Is the generator subject to regular inspections an maintenance? Who performs? Is there a contract? When and what regarding last maintenance appointment? |  |
| CM1.0 | Change Management | Is a change management or SDLC policy in place?  Does the policy cover the following changes? If no, are they covered in other policies:   * Security role or group changes (new authorizations , new role)- application and directory service * Code changes * Configuration changes (OS, DB, and application level) * Infrastructure changes (new server, memory card) * Patches and upgrades |  |
| CM2.0 | Change Request | Are change requests required for the following types of changes:   * Security role or group changes (new authorizations , new role)- application and directory service * Code changes * Configuration changes (OS, DB, and application level) * Infrastructure changes (new server, memory card) * Patches and upgrades   Explain any exceptions.  What is documented on the change request:  -Change purpose  -Impacted system(s)  -Risk assessment  -Test plan  -Back out plan  -Post implementation validation  Who typically approves change requests?  When are change requests approved? After initiation or before? |  |
| CM3.0 | Emergency Change Request | Are emergency change request procedures documented?  Is any initial review or approval required for these requests? |  |
| CM4.0 | Test Plans | Are test plans required for all changes? What are the exceptions? Are these exceptions documented in policy?  Are test results documented and attached to change tickets?  Are test results reviewed and independently approved prior to migration of change? |  |
| CM5.0 | Separate Test and Development Instances | What applications/systems have separate test and development instances:  -Active Directory  -Financial Applications  -Other Critical Applications  - Test Windows environment  -Test Unix environment  Which applications/systems do not have separate test and/or development environments?  How are changes validated if no separate test instance in place:   * Back out plans * Phased in roll out (OS patches) * Production validation |  |
| CM6.0 | Version Control | Are source code comparisons between DEV and PRD systems performed as part of the change testing/peer review/validation process? |  |
| CM7.0 | Change Migration | What is the process for migrating changes to production (for sample of systems):  -Who approves migration  -What do they review/validate  -Who migrates |  |
| CM8.0 | Post Implementation Review | For sample of system:   1. What is the process for validating changes and system functionality post migration? 2. Are tasks outlined in written deployment plans or procedures? |  |
| CM9.0 | Segregation of Duties | For select applications:  Do developers have access to production?  If yes…Can they run programs or transactions in production?  Do end users have access to development instances?  Who is responsible for migrating changes to the test and production environments? Do developers have access?  Do developers test or validate their own changes?  Do developers approve their own changes?  Do developers move their own changes to production? |  |
| CM10.0 | Change Monitoring | For a sample of critical systems:   1. Are migrated changes periodically audited to ensure proper authorization and approval. |  |
| CM11.0 | Change Control –Infrastructure | Are formal change requests required for the following infrastructure changes:  -Firewall rule modifications  -Router ACL changes  -Equipment swap out  -Equipment firmware updates/patches  -Virtual server farm changes (new blades, servers, hypervisor changes)  -VPN modifications  -Exchange/email modifications  -Server hardware (memory, NIC card)  -Server migration  -New server deployment  Are changes requests independently approved? (not approved by technician performing change)  Are changes subject to peer review, testing, or other validation? |  |
| CM12.0 | Change Control- Batch/Interface | Are formal change request required for new batch processes or modification of process steps?  What requires a formal change request?  What does not require a formal change request? (job restart, schedule change)  Are batch process changes subject to testing/validation? |  |
| CM13.0 | Change Control- Databases | Are formal change requests required for the following database changes:  -Dictionary change  -Direct data change  -Index change  -Field change  -Table change  -Database change  -Security change (add new role)  Are changes subject to testing/validation?  Is testing performed in a separate test instance?  Do DBA’s test own changes? Is there a 2nd level of approval/validation? |  |
| PM1.0 | Project Request | What is the process for requesting and approving new projects:   * Request * Business Case Document (Reason for request, projected cost and ROI) * Steering Committee review/ approval * Funding request/approval |  |
| PM2.0 | Project Planning | Are detailed project plans prepared for major projects?  What constitutes a “major” project?  Do project plans include the following basic information:   * Project timeline * Project Phases * Phase tasks * Milestones * Cost budget * Resource assignments |  |
| PM3.0 | Project Tasks | Are change tickets linked to a project code?  For changes associated with a project, are work hours tracked and billed to the project? How?  How are change interdependencies tracked (i.e. change z needs to move before change m)?  If several changes are linked to a single test or test plan, does the change ticket link or reference that documentation?  If several changes are linked to a single project test plan…are individual changes approved for migration…or is it the project as a whole?  If several changes are linked to a single project- is a migration plan developed to show the order tasks must move. |  |
| DR1.0 | Business Impact Analysis | Are the DRP and BCP based upon Business Impact Analysis (BIA) completed by the business unit mangers?  How often are BIA’s updated?  Have RTO’s and RPO’s been defined for each system application? |  |
| DR2.0 | Backup Policy | Is a formal backup policy in place?  What, if any, classifications are assigned to applications?  Does the policy provide the following minimum guidelines for each classification:  -Backup frequency for full and incremental backups.  -Backup media (e.g. tape, disk, mirrored server, SAN, cloud)  -Redundancy (e.g. mirrored server, online backup + tape backup, offsite versus onsite) |  |
| DR3.0 | Backup Schedule Monitoring | Is a backup utility used? Which one?  What does it cover?  Who is responsible for maintaining the backup schedule (e.g. DBA, application support, data center)?  Does the backup schedule align with the Backup Policy and RTO/RPO objectives?  Who is responsible for monitoring backups?  How are backups monitored (e.g. daily log review, alerts of failure)?  What is the general SLA for responding to backup errors and failures?   * Restart backup * Wait until next backup   Does the SLA align with the backup policy and is it appropriate for the system criticality RTO/RPO?  Does the organization conduct regular backups of system-level information? |  |
| DR4.0 | Offsite Backup Storage | Are backups transferred off-site?  Are they at least 10 miles away from the client site?  What form are these offsite backups (i.e. cloud, tapes, HDD)? |  |
| DR5.0 | Recovery Processes- periodic tests | Are recovery tests done regularly to ensure information integrity?  How often are the tests conducted? Are logs retained?  Who is responsible for the recovery test performance (e.g. application admin or data center)? |  |
| DR6.0 | Oversight and Management- DRP/BCP | How often is the DRP/BCP updated?  Is there a designated DR Coordinator? Does this person have another job, or is he/she completely dedicated to DR/BCP.  What type of Senior Management oversight is in place over DR/BCP:  -Annual review/sign off on plan  -Review of test results |  |
| DR7.0 | Disaster Recovery Planning | Does the organization have a formal Disaster Recovery plan that addresses the following items:  • Business Impact Analysis  • Hardware priority list (which servers are required and in what order they should be restored  • Software inventory and priority list  • Employee and critical vendor contact list  • Detailed instructions for system recovery (i.e. How is email restored?)  • Plan testing and annual review requirements |  |
| DR8.0 | Business Continuity Planning | Is a BCP in place?  What disaster site(s) have been named? Are there contracts in place?  Has a disaster site been designated for the data center?  -Cold Site- just equipment  -Warm Site- configured equipment, just need data restore  -Hot Site- fully functional equipment, ready to go.  If remote access/VPN has been designated part of the BCP- have stress tests been performed to ensure these systems can handle the projected load resulting from site loss? |  |
| DR9.0 | Disaster Recovery/ Business Continuity Training | Does each site/department have a copy of the BCP? Have they been trained on what to do?  Have emergency contracts/first responders been designated for DR? Do they have a copy of the DRP? Have they been trained on what to do? |  |
| DR10.0 | Disaster Recovery/ Business Continuity Testing | Is a formal test plan in place for DR/BCP?  Are all applications and sites included in the scope of annual testing, or has a cycle test plan been developed? What is the methodology for the cycle plan?  Is BCP included in DRP testing- or is scope just limited to system recovery?  Who is responsible for scheduling and coordinating testing?  What type of testing is performed:  -Tabletop  -Drill  -Full-scale  Are business unit managers involved in testing?  What processes are in place to review results and tweak the DRP/BCP?  Are test results summarized, documented, and provided to Management? |  |
| IF0.5 | Device Procurement | Are computer devices and IoT devices (e.g. firewalls, routers, switches, servers, workstations, laptops, tablets, phones, copiers/scanners) connected to the network subject to formal purchasing procedures?  Are there formal contract with hardware and maintenance providers?  Are device purchases required to go through central purchasing, or may individual departments and teams purchase their own equipment? |  |
| IF0.8 | Equipment Receipt and Inspection | What is the process for receiving and inspecting computer devices and IoT devices connected to the network:  -Is there a central receiving point or does the requesting department/ person receive?  -Is there a formal inspection checklist (e.g. box not open, no tampering evidence)? |  |
| IF1.0 | Device Inventory | Is a device inventory master list in place?  Is it sufficiently detailed:  Device purpose  Location  Asset Tag  Owner  Firmware version  Installed applications  IP address  How was the list compiled:  -manually from fixed asset register  -automated via discovery tool  -combination of both |  |
| IF2.0 | Device Inventory Reconciliations | Are Dynamic Host Configuration Protocol (DHCP) servers in place to assign network devices IP addresses?  Is a discovery tool in place? Provide make, model, and version.  What level of detail is the reporting:  -Device IP  -Device type  -Installed software  Are discovery tool reports reconciled to the IT asset list and Fixed Asset Register? How often? By whom?  What are considered reconciliation discrepancies:  -Device not accounted for.  - Unauthorized device  - Unauthorized software  How are discrepancies reported, investigated, and remediated? |  |
| IF3.0 | Asset Inventories | When was the last physical inventory of devices conducted?  What was the scope:  -Servers  -Network Devices  -Workstations  -laptops  -mobile devices  -fax, copiers, printers  What was excluded from scope?  Were there any discrepancies (missing items)? How were these handled? Did of these constitute a data breach under HIPAA or PCI? |  |
| IF4.0 | Software Inventory | Does the organization maintain an approved software list?  Where is it posted?  What controls are in place to ensure unauthorized software is not installed on devices:  -IT policies and procedures require approval before installing software  -Removal of local administrator rights from servers and workstations  -Whitelisting  -Periodic network scans to identified unlicensed or unapproved software |  |
| IF5.0 | Periodic Software Audits | Are periodic review of the asset discover tool reporting performed to identify unsupported, unlicensed, and out-of-date firmware, OS and software installations?  If yes, how often and by whom? |  |
| IF6.0 | Deployment/ Configuration | Are configuration hardening checklists in place for the following devices:  -Firewall appliances  -Routers and Switches  -Modems  -Servers (Windows, Linux, etc.)  -Databases (Oracle, SQL)  -Workstations/laptops  -mobile devices  If images are used to configure devices- which devices- and who has access to modify the images?  At a minimum, what configurations are changed?  Is any documentation retained related to device deployment?  Is device deployment subject to any periodic audits, vulnerability scans, or peer reviews?  What happens when a configuration error is identified in a vulnerability scan? |  |
| IF7.0 | Antivirus | What antivirus product is used?  Where is it installed?  -Servers  -Workstations  -Point of Sale Devices  -Payment/information kiosks  -Laptops  -Mobile devices  What is it not installed on?  Are antivirus installations included in device configuration checklists? |  |
| MT1.0 | Maintenance schedule | Are maintenance schedules in place for all system components, including:   1. Network devices 2. Servers 3. Workstations   Does the maintenance schedule include an end of life replacement date for each device in inventory? |  |
| MT2.0 | On site spares | 1. Is an on-site spare inventory maintained? 2. If no, are procurement plans in place to replace equipment when necessary? |  |
| MT2.5 | Vendor Repairs and Maintenance | 1. What is the process for sending devices to vendor for repairs or maintenance? 2. Is there a central site that processes repairs and returns? 3. What measures are taken to ensure devices are secure and not tampered with during transport? 4. Who receives devices returned from the vendor? 5. What is the inspection procedure:    1. Virus Scan    2. Physical Inspection    3. Device log review |  |
| MT3.0 | Network firmware Maintenance | 1. What is the process for identifying patches and updating network device firmware? 2. Have responsibilities been assigned for this? Who is responsible? 3. Is there a process (vulnerability scans/ audits) for identifying unpatched firmware and operating systems? Are discrepancies investigated? |  |
| MT4.0 | Operating System Maintenance- Servers and Workstations | 1. What is the process for identifying patches and updating operating system (e.g. Windows, Linux, Unix) installations on servers and workstations (including desktops, laptops)? 2. Have responsibilities been assigned for this? Who is responsible? 3. Is there a process (vulnerability scans/ audits) for identifying unpatched firmware and operating systems? Are discrepancies investigated? |  |
| MT5.0 | Application Maintenance | 1. What is the process for identifying patches and updating applications, including critical applications and ancillary desktop applications, like Adobe, Firefox, and Java? 2. Have responsibilities been assigned for this? Who is responsible? 3. Is there a process (vulnerability scans/ audits) for identifying unpatched applications? Are discrepancies investigated? |  |
| MT6.0 | Database Maintenance | 1. What is the process for identifying patches and updating databases, including both Oracle and SQL instances? 2. Have responsibilities been assigned for this? Who is responsible? 3. Is there a process (vulnerability scans/ audits) for identifying unpatched databases? Are discrepancies investigated? |  |
| MT7.0 | Vulnerability Scanning | 1. Are systems periodically scanned for vulnerabilities? 2. How often? 3. What scanner is used? 4. What is the scope:    1. Operating System    2. Database    3. Network Devices |  |
| MT8.0 | Vulnerability Resolution | 1. Is there a formal vulnerability management policy? 2. What is the SLA for reviewing scanner reports? 3. Does the scanner assign a risk classification to vulnerabilities? 4. What is the SLA for investigating High, Medium, and Low risk vulnerabilities? 5. How are deficiencies in operating procedures and personnel training addressed? 6. What is the SLA for resolving High, Medium, and Low risk vulnerabilities? |  |
| OP1.0 | Batch Administration | 1. At formal procedures in place concerning batch job administration and m monitoring? 2. Who is responsible for creating new batch processes:    1. Application Admin    2. Separate Batch Admin Team or Network Operations Center    3. Combination of both 3. Who is responsible for monitoring batch processing:    1. Application Admin    2. Separate Batch Admin Team or Network Operations Center    3. Combination of both |  |
| OP2.0 | Batch Classification | 1. Are all new batch processes assigned a priority/criticality? 2. What are the priorities and what are the associated service level expectations?    1. For monitoring- alerts set, email/text alerts, log review    2. For response- contact support after hours, wait till next business day    3. For resolution- immediately, within 24 hours, n/a- wait for next process. |  |
| OP3.0 | Central Scheduling | 1. Is a central scheduling tool used for batch processing? 2. What tool? 3. What processes must be scheduled via the tool? What processes can be scheduled within the application? 4. Does the tool generate and maintain a batch inventory report? 5. What does the batch scheduling team use for monitoring and error resolution guidance? Does the tool or list provide instructions for notifying support personnel and resolving batch processing issues? |  |
| OP4.0 | Batch Process Monitoring | Who is responsible for monitoring batch processes?  -Application admin  -NOC or batch team  What type of monitors?  -Alerts  -manual log review  Does the team have explicit instructions for responding to alerts?  -What to do  -Who to call  -How to escalate |  |
| IM1.0 | Central Helpdesk Function | Is there a central helpdesk function?  Are there formal procedures for fielding and moving problem calls?  What are the help desk hours?  Is there any after-hours call desk? |  |
| IM2.0 | Central Incident Tracking Application | What ticketing application is used?  Does the ticketing application have workflow capability to assign tickets, request approval, and track progress?  Is a separate system used for change requests? |  |
| IM3.0 | Incident Prioritization and Service Level Metrics | What categories of incidents are available?  Are these categories communicated in written helpdesk procedures?  Are SLA’s for each category documented?  Are alerts fired if an incident extends past its SLA? |  |
| IM4.0 | Incident Resolution Monitoring | Are reports of open incidents regularly reviewed for status updates and delays in resolution?  How often?  By whom? |  |
| IM5.0 | Incident Trend Analysis | Is any trend analysis performed of the ticketing application- examples include:  -Incidents by team  -Incidents by application  -Change requests by team  -Problem reports by team  What reports are reviewed?  How often?  By whom?  What is the general process for investigating trends, identifying and addressing root cause? Ask for some examples. |  |
| IM6.0 | Security Incident Reporting and Categorization | Does the helpdesk have formal procedures to distinguish between a routine incident or problem and a security incident?  What are the criteria given to the team?  Has the team been trained on these procedures?  Is a special category reserved for security incidents? |  |
| IR1.0 | Incident Response Plan | Are there formal procedures relating to incident response including, what constitutes an incident, how to report an incident, and available training for employees?  Does the incident response plan address the following:  -Identification of risk  -Protection of data  -Detection mechanisms  -Response plan  -Recovery plan  Does the incident response plan have formal metrics/SLA’s for detection and reporting of incidents:  -Monitoring alerts  -Virus detection  -Phishing emails |  |
| IR2.0 | End User Communications and Training | Is a security awareness training program in place?  Are responsibilities for detecting and reporting security incidents communicated? How?  -Training  -Procedures  -Emails  -Key Focal Points/metrics for Managers  Are any other type of exercises used to reinforce procedures:  -Email updates or alerts  -Training Exercises (mock phishing exploits) |  |
| IR3.0 | Incident Response Handling | Are incident reports subsequently reviewed for the following:  -Timeliness of identification  -Timeliness of reporting  -Timeliness and effectiveness of containment efforts  -Investigation and root cause analysis  -Forensic reviews  -Lessons learned  Are summaries of incident reviews prepared and reviewed by Senior Management to determine the following:  -If updates to policies and procedures are required.  -If updates to the security awareness training program are required.  -If additional resources are required. |  |
| IR4.0 | Incident Response Plan/ BCP and DR Transitions | Are criteria in place in the Incident Response Plan for declaring a DR event?  What are those criteria?  Are security incident scenarios included in BCP/DRP training exercises? Describe? |  |
| VM1.0 | Vendor Contracts | Are contracts/ SLA’s in place for all vendors?  Are mandated information system and security control included in the terms of the contract or SLA?  Does the contract have a right to audit clause?  What is required to evidence controls are operational:  -SOC Report  -Security Assessment Questionnaire (SAQ)  -Onsite inspection/audit |  |
| VM2.0 | Service Level Expectations | When are service level agreements required?  -Significant Service Providers  -all service providers  Who determines SLA objectives?  Are specific metrics/benchmarks in place for each objective?  What is the process for reporting and monitoring service level performance?  -Who is responsible?  -How often performed? |  |
| VM3.0 | Transfer of Risk | Have remedies for breach of contract or failure to implement controls been identified?  Are significant service providers required to carry a minimum level of insurance? |  |
| VM4.0 | Third Party Monitoring- SLA | Is a formal vendor evaluation process in place?  How often is it performed?  Who performs?  Are vendor evaluations documented and independently reviewed? Documented by whom? Reviewed by whom? |  |
| VM5.0 | Third Party Monitoring- Audits | Who is required to have a SOC or equivalent examination performed?  Who is responsible for reviewing the SOC?  Are the Complementary User Entity controls reviewed to ensure the organization has implemented those controls?  Are the controls in the examination scope reviewed for adequacy and compliance to the organization’s IT policies with respect to:  -Data disclosure  -Data encryption  -Access restrictions  -Security monitoring  -Network controls  -Uptime/performance monitoring |  |