Information Security Statement

08/10/2020

Overview

Deloitte[1] has developed and implemented an Information Technology (IT) infrastructure that is designed to generally align with industry standards. The security boundary of the IT infrastructure includes Deloitte-issued laptops, as well as infrastructure and applications, such as databases, and backup systems. The IT infrastructure security controls and associated information security processes were developed to protect confidential information while making it available in appropriate circumstances. A summary of such policies, controls, and associated processes is set forth below.

Purpose

The purpose of this Information Security Statement is to provide an overview of Deloitte's IT security practices that are in effect as of the recent published date of this document.

[1] As used in this Information Security Statement, "Deloitte" refers to Deloitte USA LLP, Deloitte LLP and/or their respective subsidiaries.

Table of Contents

Cyber Security

Deloitte's Chief Information Security Officer (CISO) oversees the Cyber Security team, which provides assistance in the following areas:

- eDiscovery Forensic Investigations:
  - Manages the end-to-end process of collecting data requested by the Office of General Counsel (OGC) for legal and regulatory matters
  - Works with OGC and the Talent organization to conduct internal investigations on misuse of data resources and manages security incident responses
  - Acquires, documents, and preserves digital evidence for computer forensics
- Risk & Compliance:
  - Leads and manages the vendor security program and privacy impact assessment process
  - Collaborates with client service leaders and OGC in responding to client security inquiries and security agreements
  - Leads Deloitte's third-party audit and assessment (e.g., SOC2 and ISO)
  - Leads Deloitte's security awareness efforts and assists with global security awareness efforts
  - Responsible for exceptions to security policies and standards
- Cyber Defense:
  - Monitors, analyzes, and responds to all types of system, device, and application events, such as user activity, firewalls, IDS/IPS, antivirus, and vulnerabilities
  - Identifies, rates, and remediates potential security vulnerabilities of applications and systems
  - Understands which Deloitte systems are used, how, and by whom and uses this information to protect the organization from potential threats
- Data Protection:
  - Reviews emerging technologies, security architecture, and proposals for improvements
  - Leads the identity management program
  - Leads Federal support and maintains FedRAMP certifications

Members of the Cyber Security team hold various industry security and audit-based certifications (e.g., CISSP, CISM, CISA, ISSM, CRISC, CEH, ISO 27001 Lead Auditor, and OSCP).

Information Security Program

Deloitte maintains a comprehensive information security program, which includes policies, standards, procedures and guidelines. The information security program is informed by several industry-standard guidelines and best practices including ISO27001, COBIT, ITIL, and the American Institute of Certified Public Accountants (AICPA) Service Organization Controls (SOC2).

Deloitte's IT leadership meets on a regular basis to consider strategic and tactical direction for the information security program, and its policies, standards, procedures and guidelines.

Information security policies are drafted with input from internal information security stakeholders and are based upon industry standard practices. The drafts are reviewed and approved by Deloitte's Cyber Security leadership, OGC, Confidentiality & Privacy, the CISO and Deloitte's Chief Information Officer. Once approved, the policies are published on Deloitte's intranet and communicated to personnel.

Certification

Deloitte has established and operates an Information Security Management System (ISMS) that manages its client confidential information. The ISMS has been certified by an independent third party that it complies with the requirements of the International Information Security Management System Standard ISO/IEC 27001. In addition, Deloitte's Business Continuity Management (BCM) program has been certified by an independent third party that it complies with the requirements of ISO 22301:2012 (Societal security — business continuity management systems).

On-Site Security Assessments

In an effort to protect and minimize risk to Deloitte's client data, in lieu of permitting individual clients to perform independent security assessments of Deloitte's information security program, each year Deloitte engages an independent third-party auditor (Third Party) to (i) conduct an examination in accordance with AT Section 101 of the Statement on Standards for Attestation Engagements to report on controls at a Service Organization relevant to security and availability established by the AICPA (AICPA Standards) and, subject to AICPA Standards, prepare a Type 2 service organization controls report with respect thereto (the SOC2 Report).

SOC2 Report

The SOC2 Report includes the Third Party's opinion on the fairness of the presentation of the description of Deloitte's systems in management's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on the Third Party's examination. The SOC2 Report also includes a description of Deloitte's systems and controls, and a description of the Third Party's criteria, test procedures, and the results of such tests. The SOC2 Report may be made available to a current or prospective client that is bound by appropriate non-disclosure or confidentiality terms with Deloitte applicable to the disclosure of the SOC2 Report.

Awareness and Training

Deloitte has implemented training and awareness programs for its personnel related to information-security, confidentiality and privacy policies and practices. Deloitte personnel are required to complete a confidentiality, privacy, and information security awareness training during the new-hire onboarding process, as well as an annual update course thereafter. Deloitte personnel are presented with an information security policy awareness statement via Deloitte's intranet two times each year, which they are required to acknowledge within two weeks of the statement's release.

Deloitte has a dedicated security awareness committee. The committee is responsible for developing ideas to enhance Deloitte's awareness of security risks and issues through policy development and training. The committee is comprised of delegates from Deloitte's Cyber Security leadership, National Office of Security, Confidentiality & Privacy, CISO, National Quality Risk Management, Talent, and OGC, and from Deloitte Touche Tohmatsu Limited's Global Information Security Office, who regularly meet to discuss new or recurring security, confidentiality, and privacy issues, devise strategies and implementation plans, and provide progress reports on existing projects.

Management and Protection of Confidential Information

Deloitte is committed to protecting the confidential information and Personally Identifiable Information (PII), of our clients, our organization and the third parties with whom we work. "Confidential Information" refers to any information not generally available to the public, in any form, that Deloitte receives or creates in the course of business. To support this commitment, Deloitte's Confidentiality & Privacy is responsible for setting guidelines, developing procedures, and providing consultation and training on the management of confidential information.

Confidentiality & Privacy has also developed the "Confidential Information Program" for the proactive management protection of confidential information and is responsible for implementing the Confidential Information Program across Deloitte. The Confidential Information Program consists of processes, technology controls, training, and communications that help our professionals to improve their awareness of risks associated with confidential information and their ability to properly manage and safeguard confidential information.

The Confidential Information Program

The Confidential Information Program consists of processes and activities that are performed throughout the engagement lifecycle to manage and protect confidential information.

Client account and engagement teams in the Confidential Information Program generally do the following:

- Appoint a Confidentiality & Privacy Manager responsible for overseeing program activities;
- Develop and maintain a Confidential Information Management Plan (CIMP) to document the confidential information management strategy and safeguards employed;
- Develop and deliver confidentiality and privacy information onboarding training that outlines the protocols that team members must follow when accessing, storing, using, transferring, and disposing of confidential information and PII;
- Implement physical, administrative, and technical safeguards identified in the Confidential Information Management Plan to proactively manage risk; and
- Complete all other required confidentiality and privacy training as applicable.

Deloitte also has an insider threat program in which Deloitte conducts active monitoring of insider threats. Insiders are defined as personnel and contractors who, based on their access to certain systems and information, could adversely affect the brand, reputation and/or business of Deloitte or its clients. Leveraging potential risk indicators, the insider threat program monitors persons of interest across a broad risk spectrum, including workplace violence, espionage, fraud, and theft of intellectual property and confidential information. Analytic and cognitive technologies are used to help identify indicators of poor risk-culture fit and determine corresponding strategic tactics and mitigation strategies to align our sub-cultures.

Data Privacy

Deloitte is committed to protecting our clients' Personally Identifiable Information (PII). Deloitte has privacy policy, applicable procedures, and personnel dedicated to privacy compliance activities related to our privacy policy and applicable data privacy laws and regulations. We regularly monitor for changes in privacy laws and regulations and adjust our policies and procedures when appropriate. Additionally, we have instituted an annual review process across all Deloitte business areas to verify compliance with our privacy policy and procedures.

Deloitte has policies and procedures that protect PII and support compliance with US and the European Union (EU) legal requirements relating to the transfer and processing of PII, including personal health information.

- Deloitte adheres to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks with respect to PII that is transferred from the European Economic Area, the United Kingdom, and Switzerland to the United States.

- Deloitte is not a "Covered Entity" as defined under the Health Insurance Portability and Accountability Act, as amended (HIPAA). Therefore, Deloitte is generally not required to, and does not, comply with the obligations of a Covered Entity. However, when Deloitte acts in the capacity of a "Business Associate" to our clients, as such role is defined under HIPAA, Deloitte is required to comply with the obligations of a Business Associate under HIPAA. Deloitte has implemented policies, procedures, and controls that facilitate compliance with those obligations.

- Deloitte performs an annual self-assessment process to validate adherence to data privacy lifecycle safeguards regarding the collection, use, transfer, storage and destruction of Personally Identifiable Information (PII) for Business Processes and Service Lines that process PII.

- Deloitte utilizes a Privacy Impact Assessment (PIA) process for new systems, changes to existing systems and high-risk business processes that access, transfer or store PII.

- In support of the Privacy by Design concept, Deloitte has incorporated privacy and confidentiality requirements into our secure systems development lifecycle (SSDLC) for internally developed systems so that these requirements are considered early and often throughout the lifecycles of technology projects using a risk-based approach.

- Members of Deloitte's Privacy team hold various security and privacy certifications (e.g., CIPP/US, CISSP).

Confidentiality & Privacy Incident Management

Deloitte has instituted an integrated incident response process designed to facilitate prompt reporting and resolution of incidents. Our confidentiality and privacy incident response process is characterized by the following:

- Centralized reporting of actual or suspected incidents to a Help Desk, which is available 24/7 with access via a toll-free number and self-reporting available on Deloitte's intranet site;

- Training and awareness programs focused on helping personnel understand immediate steps to be taken in case of actual or suspected incidents;

- Established roles and responsibilities for incident management and response including involving the appropriate consultation resources across the Deloitte organization, as applicable to the specific matter;

- Documented processes and tools to help gather incident facts, initiate response activities, engage incident response teams, escalate incidents and alert appropriate leaders, based on the nature of the specific incident;

- Consultation among the relevant parties regarding the need for a corrective action plan;

- Development, as appropriate, of action plans, including any required communications, as well as actions to mitigate the risk of a future recurrence; and

- Post-incident follow-up process to analyze root causes and integrate lessons learned.

IT Continuity Management

Deloitte maintains an active disaster recovery and business continuity program which helps to continue delivering information-technology-related services should a disruption occur. Deloitte's program includes the following basic activities:

- Business continuity planning for IT infrastructure support staff;

- Business impact assessments to help define criticality of processes and systems related to recovery time objectives;

- Disaster recovery planning of our technology through multiple failover capabilities;

- Implementation of resilient architectures where technology allows;

- Risk assessments as part of continual service improvement, with countermeasures identified and implemented for the newest scenarios; and

- Internal review process for maintaining the quality of plans and services.

The Business Continuity Program (BCP) and plans include emergency-response business procedures, which go into effect following the occurrence of a disaster or other unplanned interruption.

Disaster Recovery (DR) plans include technical and business contact call lists, as well as notification and escalation information and architecture diagrams. Where pertinent, third-party information is also included. Recovery time objectives and recovery point objectives are documented and tested for each plan.

BCP/DR plans for critical infrastructure are subject to review and testing every 12 months with industry standard testing methods.

Risk assessment test scenarios vary based on business sensing and technology security. Test results are reviewed and recorded.

In summary, Deloitte has a comprehensive disaster recovery and business continuity program that is designed to provide for the continuity of essential IT business functions and critical business processes following the occurrence of a disaster or other unplanned interruption impacting Deloitte's IT infrastructure.

Business Continuity Management (BCM) Program

Deloitte takes disaster and contingency planning very seriously, including planning for events that impact its people, its facilities and/or its technology. Deloitte's business continuity planning addresses issues such as, communications, travel, resource allocation, technology needs, and alternate work sites. Response procedures assess the well-being of personnel, provide for the continuity of essential business functions, and utilize recovery procedures for the restoration of critical business processes. These critical business processes are identified during a business impact analysis process and are documented in the business continuity plans for each business and enabling area.

Cross-functional teams are identified to manage potential disruptive events, emergency situations or disasters. Each Deloitte office has a local crisis management team to handle smaller, localized events impacting a single location. For larger events or those that are not specific to a single location or geography, an experienced National Incident Support Team is assigned. A National Crisis Council handles incidents that rise to the level of a true crisis requiring strategic involvement and decision-making.

Cross-functional teams are identified and documented in the plans to include representation of key stakeholders from the following areas:

- Client Services
- Office Services/Operations/Facilities
- Office of Security
- Human Resources and Benefits
- Information Technology Services
- Procurement and travel
- Communications
- Risk Management

Deloitte has designed an impact-driven approach, which focuses on the impacts of an event, emergency, or crisis, rather than specific scenarios. Each type of situation could have an impact on our people, our facilities, our technology, or our clients. Each type of situation could require communications, whether internal or external. The team-based, impact-driven approach utilized by Deloitte provides the best resources to assess and address the impacts of an event.

Deloitte's planning considers the potential impacts and continuity of operations in the event of a pandemic, which includes a pandemic-specific governance model and response triggers. Pandemic planning and response is aligned with the crisis management and business continuity processes, including the use of the National Incident Support Team, but is supplemented by additional members of a Pandemic Response Committee. The Pandemic Response Committee monitors potential pandemic developments and would oversee implementation of specific pandemic action steps based on the severity of the pandemic, including targeted communications that would be issued internally and externally, and identification of critical people and resources.

Limits of Business Continuity and Pandemic Planning

Due to the significant uncertainties associated with a possible flu pandemic or other disaster, Deloitte can make no representations or warranties, nor provide any assurances, that its plans will be adequate to respond to any possible consequences, or that the plans of any third parties to deal with a possible flu pandemic or other disaster are or will be sufficient to address any situations or problems that might arise during a pandemic or other disaster. Deloitte's objective is to prepare for a possible flu pandemic or other disaster based on the information and data that it has at this time, and to possibly modify those plans as it believes conditions or facts may warrant.

Every organization needs to develop its own preparedness plan based on its specific circumstances, business functions, and operational factors. Consequently, a plan developed for one function or business cannot be expected to address the potential issues that may be faced by another business enterprise. Because business continuity and disaster recovery plans and documentation contain information about Deloitte that is proprietary and confidential, Deloitte does not provide third parties with copies of such plans or documentation.

Human Resources Security

Upon hire, all personnel agree to comply with Deloitte's policies, including those relating to information security, confidentiality and privacy. In addition, all Deloitte personnel are required to complete security awareness training during the new hire onboarding process.

Background Checks for U.S. Personnel

Deloitte generally requires that background investigations be conducted for partners, principals and all employees at the time that they join Deloitte. Potential issues that are identified in the background investigation are reviewed on an individual case-by-case basis, in light of guidance from the Equal Employment Opportunity Commission and applicable federal, state and local law. This individualized assessment includes a determination of whether the issues identified are job-related or pose a risk to Deloitte or to its employees, partners, principals, or clients. The type of background investigation performed depends on whether the individual joining is a partner or principal and the level of the employee. While background investigations were not always performed on Deloitte personnel, and may not always have covered the same information, all background investigations of Deloitte personnel in the U.S. currently include the following, at a minimum:

- Social Security Number (SSN) verification: confirms a valid number and the names and addresses associated with that number
- Felony and misdemeanor conviction searches: searches of the following records for felony and misdemeanor convictions are performed for the last five years in areas of residence, work and school:
    - Federal courts
    - County courts
    - State repositories, where the state has made one available and it is reasonably accessible
- A national criminal record database search, including the state sex offender registries.
- Education confirmation: education beyond high school confirmed
- Employment confirmation: professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, such as SEC, OFAC, OIG/GSA, FDA, FBI Most Wanted, EU Terrorist Watch List, Interpol Watch List, etc.
- Professional licenses: confirm relevant professional licenses

Background checks for Personnel of Deloitte entities located in India (U.S. India)

The type of background investigation performed depends on whether the individual joining U.S. India is a partner, principal, or employee, and the level of the employee. While background investigations were not always performed on U.S. India's personnel and may not always have covered the same information, all background investigations of U.S. India personnel currently include the following, at a minimum:

- Identity Verification, where possible
- Criminal checks: check all relevant court records for a five-year period
- Education confirmation: all university level education is confirmed
- Employment confirmation: all professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, including India specific and global databases
- Professional licenses: confirm relevant professional licenses

Physical and Environmental Security

Only authorized personnel with a Deloitte-issued electronic badge are granted access to Deloitte's facilities. Procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the facilities. Deloitte data centers are further restricted to only those personnel with the need to access restricted areas. Data centers have the following physical security measures: security guards, man-trap doors at primary entrance, multi-factor authentication (Deloitte-issued electronic badge and biometric readers) at secondary entrance, video cameras, and sign-in and sign-out sheets for escorted visitors.

The electricity, water, and temperature controls are all pre-approved for use by the facilities administrators in the data centers. Each utility has a control in place to monitor its usage and to notify an administrator in case of failure. Automatic emergency lighting is installed in areas necessary to maintain personnel safety.

Emergency exits are located in appropriate places in Deloitte facilities. Automatic fire suppression systems have been installed to protect the facilities. In data centers, the primary system is HFC-125 chemical based and activated via multiple smoke detectors, and the second type is pre-action hydronic, and the detection method is temperature. Master water shut-off valves are present. Temperature and humidity controls have been implemented to protect against temperature fluctuations in all areas of the data centers containing IT equipment.

Risk Management

Deloitte has a risk management program that monitors possible threats and vulnerabilities to information technology assets. Risk assessment(s) are performed annually and when there are significant changes to infrastructure, technology or environment. There are several control domains defined for risk assessment. These control domains are derived from industry standard practices and frameworks. For each control domain, implemented controls are identified and tailored and their effectiveness assessed for risk management. Risks that are not at an acceptable level are remediated or mitigated.

Vendor Hosting and Processing

Deloitte has arrangements with vendors who provide Deloitte with certain software-as-a service and hosting services. Deloitte selects and retains these vendors based on, among other qualities, their capability to maintain safeguards for the systems, software and information at issue that are consistent with leading industry security practices. Deloitte requires these vendors to implement and maintain such safeguards.

Vendor Assessment Process

The Vendor Assessment process is designed to reduce vendor-related risk by:

- Building a repository of acceptable vendors;
- Assessing the security posture of vendors;
- Tracking remediation of identified issues; and
- Reviewing and assisting with vendor contracts with respect to obligations relating to Deloitte's information security program.

Deloitte's ITS Cyber Security Risk and Compliance (CSRC) program is responsible for reviewing our vendors' compliance with a standard set of security requirements, based upon the type and volume of data the vendor will access, as well as the risk posed to Deloitte and our clients. As part of this process, all internal projects as well as client-facing engagements which will require the services of a third-party vendor, must be added to the Third- Party Risk Management (TPRM) gateway by the Deloitte representative seeking the vendor relationship.

The ITS Cyber Risk review is focused on third parties who will access, be provided with, store or process Deloitte or client's data. Third parties rated as high or medium risk must complete an online security questionnaire within Deloitte's vendor assessment system, whereas third parties rated as critical risk undergo an onsite assessment. The third party will have a maximum of thirty days to complete the online questionnaire. The questions presented within the online questionnaire, as well as during the onsite assessment, cover the following security domains: Access Control, Asset Management, Business Continuity Management, Communications and Operations Management, Compliance, Human Resource Security, Information Security Incident Management, Information Systems Acquisition Development and Maintenance, Organizational Security, Physical and Environmental Security, Risk Management, Cloud Governance and Security Policy.

Upon the third party's completion of the online questionnaire or onsite assessment (if applicable), the ITS Cyber Risk and Compliance team reviews the responses provided to identify findings, which are gaps or weaknesses in the vendor's security controls. The findings are assigned remediation dates and tracked to completion by the CSRC team in collaboration with the Deloitte contact, as well as with the third party. Once all findings are remediated, high risk vendors are re-assessed annually, and medium risk vendors are re-assessed every two years, for the duration of their contract with Deloitte.

Asset Management

Deloitte has an asset management team that is responsible for oversight and management of Deloitte assets and inventory throughout its lifecycle. There are tools and controls in place that manage hardware and software assets. Deloitte has policies and procedures in place to manage licensed software and security controls to deter prohibited software from being installed and/or used. A software and hardware inventory system is maintained, which identifies hardware and software components used within Deloitte information systems. Multiple controls are used to manage the configuration baselines, including mobile device management. These controls are supported by automated tools that provide configuration and inventory information on a continuous basis specific to configuration compliance, known vulnerabilities, inventory by Internet Protocol address (IP address)/device name and asset operational and connection status.

Access Control

Access to Deloitte information contained on Deloitte IT systems is granted on a need-to-know basis and must be approved by the Deloitte data owner.

Vendor and contractor access is requested through procedures that involve Deloitte's Talent and Technology groups. Upon approval, the vendor user accounts are created in a controlled domain organizational unit giving the access necessary to perform their defined duties. Vendor and contractor access is granted on a temporary basis based on business need.

For certain systems, remote access is provided via Transport Layer Security (TLS) using two-factor authentication with account activity being logged to Deloitte's logging/alerting mechanism. Depending on the level and type of access required, the VPN solution provides a secure virtual session or web interface with access into the needed application(s) or platform.

For web-based applications that contain or provide access to sensitive internal or client data (including VPN), Multi-Factor Authentication (MFA) has been enabled. Verification options include phone call, text message, or mobile application.

Privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into role-based groups (e.g., key management, network, system administration, database administration, and web administration).

Identification and Authentication

All users must authenticate to the Deloitte network using a unique user identification (ID) and a strong password prior to gaining access to the information system.

Deloitte strong passwords contain the following characteristics:

- Passwords are required to be at least ten (10) characters in length and contain at least three of the following four elements: (1) westernized Arabic numbers (e.g., 2,5,9), (2) non- alphanumeric characters (e.g., #, %, !, %, @, ?, -, *), (3) English uppercase letters (e.g., A, B, C), and/or (4) English lowercase letters (e.g., a, b, c)

- Passwords are not permitted to contain:

    - parts of the users' username, first name, or last name
    - dictionary words with or without (i) numbers or special characters at the beginning or end, or (ii) letters, numbers, or character exchanges (e.g., Summer2017, ?Happyman, H3llofr!end?)
    - words or numbers connected with users such as family names, pet names, birthdays, addresses, or phone numbers
    - common terminology, acronyms, or names associated with the Deloitte or its clients
    - any variation of 'Deloitte' or 'Password' (e.g., Deloitte12, P@ssw0rd12, Pa$$w0rd!2)
    - any sequencing of letters and numbers that follow the order of a keyboard (i.e., keyboard walk patterns such as 1234qwerASDF, 1qazXSW@3edc)

Additional Password Safeguards

The following additional password related safeguards are enforced:

- Users are not permitted to reuse their previous twenty-four passwords
- Passwords expire every 90 days
- There is a password lockout threshold after 6 invalid logon attempts

System Security

System and Communications Protection

An intrusion prevention system (IPS) is employed at the point of entry to the Deloitte network environment. The logs for the IPS, firewall, and VPN are sent to a log aggregator. Access control lists are placed on firewalls controlling the inbound and outbound flow of traffic. Traffic is denied by default unless approved by the gateway protocols as configured and approved by the Deloitte security team. A demilitarized zone (DMZ) and trusted zones are used to segment traffic to areas that are protected in accordance with the accepted risk levels.

System and Information Integrity

Firewall, IPS, and VPN audit logs are sent to the log aggregator, which checks for abnormal activity and anomalous behavior that would trigger an information security review. Hardware and software checks are done by automated tools with identified alert levels that trigger a notification to the system administrators in case of a system flaw. Anti-virus and malware protection is managed by enterprise policy and distributed by a server located in the environment periodically. Anti-virus is configured to scan external devices attached to the information system as well as email traffic.

Data Back-up

Deloitte systems are scheduled for daily backup and two iterations of data through redundant data mirroring: one onsite and one offsite. If a system backup is interrupted for any reason, it will resume in the same site once the issue that caused the interruption is resolved. A reputable vendor is utilized for offsite backup storage and disposal. All backup media is encrypted prior to shipment to the vendor and a controlled process exists for turnover. The vendor is subject to obligations of confidentiality. The vendor has security practices in place and uses a tracking application for all media it handles on Deloitte's behalf. Deloitte is provided with inventory reports of the media and chain-of-custody. The vendor stores the media in a secure, environmentally controlled storage facility.

Information Systems Acquisition, Development and Maintenance

Security Planning

The Deloitte information security program, applicable policies, standards, standard operating procedures and guidelines are reviewed annually and updated as necessary.

Acquisition of System and Services

Deloitte does not acquire IT systems or services until Cyber Security has reviewed the product or service to determine whether it meets internal guidelines with respect to security and encryption. Software installation requests are submitted for risk assessment and approval. Software is not implemented unless it meets applicable Information Technology Services (ITS) standards. There is a Change Control Board (CCB) that discusses any changes that may affect the security posture of the environment and documents all proposed upgrades or modifications to the environment, assets and infrastructure.

Application Development

Deloitte follows secure coding best practices during the system development lifecycle for Deloitte applications. Deloitte's applications undergo security reviews, testing and vulnerability scans prior to being placed in production.

Change Control

Deloitte has a change management process in place for its IT systems. Proposed changes are submitted, tested, and reviewed during regularly scheduled CCB meetings. Approved changes are tested and vulnerability scans are performed prior to deployment. Deployment windows are scheduled to minimize the impact to Deloitte's operations. Back-out plans are in place should they be needed.

Patch Management

Deloitte has a patch-management program and supporting tools in place that are managed by an internal patch management team (PMT). Vendor and industry-accepted alert lists are monitored for new patches. Patches are reviewed by the PMT at regularly scheduled meetings and are rated for deployment based on assessed severity levels. Emergency patch management meetings are called when needed.

Vulnerability Management

Deloitte's network undergoes penetration testing and vulnerability scans performed by Deloitte's Cyber Defense team. Penetration tests are performed annually on the network infrastructure's external perimeter by Deloitte's Cyber Defense team. Vulnerability scanning is performed weekly on the network infrastructure's internal and external perimeter by Deloitte's Cyber Defense team.

Maintenance

Deloitte ITS performs software and hardware maintenance on Deloitte's environment servers.

Information system backups are performed daily. Performance reports are initiated through automated tools that specify certain levels of performance to trigger the generation of the report (i.e., % of CPU processor utilization, etc.).

Third-party contractor maintenance personnel must be approved prior to receiving access to the information system servers. Third party maintenance personnel are escorted into the facility and accompanied during the period of access. A log is maintained which documents the name, date, length of time, justification, and escort name for each maintenance individual who is granted access to the information system(s).

Information Security Incident Management

Deloitte has built an integrated incident response team that brings together the appropriate subject matter experts from various cross-functional disciplines to address each specific incident. The Security Incident Response Procedures (Procedures) describe how various types of incidents are handled. The Procedures identify key resources and communications that will take place based on various incident types. The Procedures identify to whom suspected incidents should be reported and describe the escalation path from the entry point in the process through fruition. Security awareness training is in place to educate Deloitte personnel of their responsibilities concerning security incidents. Each incident is logged and the relevant facts are captured for analysis and reporting. When necessary, data related to the incident is maintained in a forensically sound manner and appropriate chain-of-custody is documented.

The incident response team has a variety of tools available to assist them in the analysis of incidents. These include standard security tools from software and hardware providers as well as commercial forensic tools specifically targeted for such matters.

Information security incident procedures are executed periodically so the teams remain prepared for response should the need arise. At the completion of each significant incident, a post-incident review is conducted to identify any areas for improvement as well as lessons learned. These findings are used to adjust, enhance or improve the procedures.

Compliance

System Audit and Accountability

System audit logs and records are created to monitor the following

- anti-virus services
- intrusion prevention services
- remote access services, web proxy services
- domain authentication
- router events
- firewall events
- VPN access
- application logs
- operating system logs
- privileged access logs

System audit logs are maintained to support analyses and investigations. Logs are maintained for a period of one (1) year. Logs may also be preserved based on legal or regulatory requirements.

System audit log content includes: (i) date and time of the security event; (ii) the component of the information system (e.g., software component, hardware component) where the security event occurred; (iii) type of security event; (iv) unique user/subject identity; and (v) the outcome (success or failure) of the security event.

System Audits

Deloitte's internal audit team periodically performs internal audits on various aspects of Deloitte's systems, processes, and policies.

Application Configuration Management

Software baseline requirements are created in accordance with Deloitte policies and standards. Software is tested against the baseline requirements prior to being placed in the production environment. Continued monitoring and change management processes are conducted while in operation.

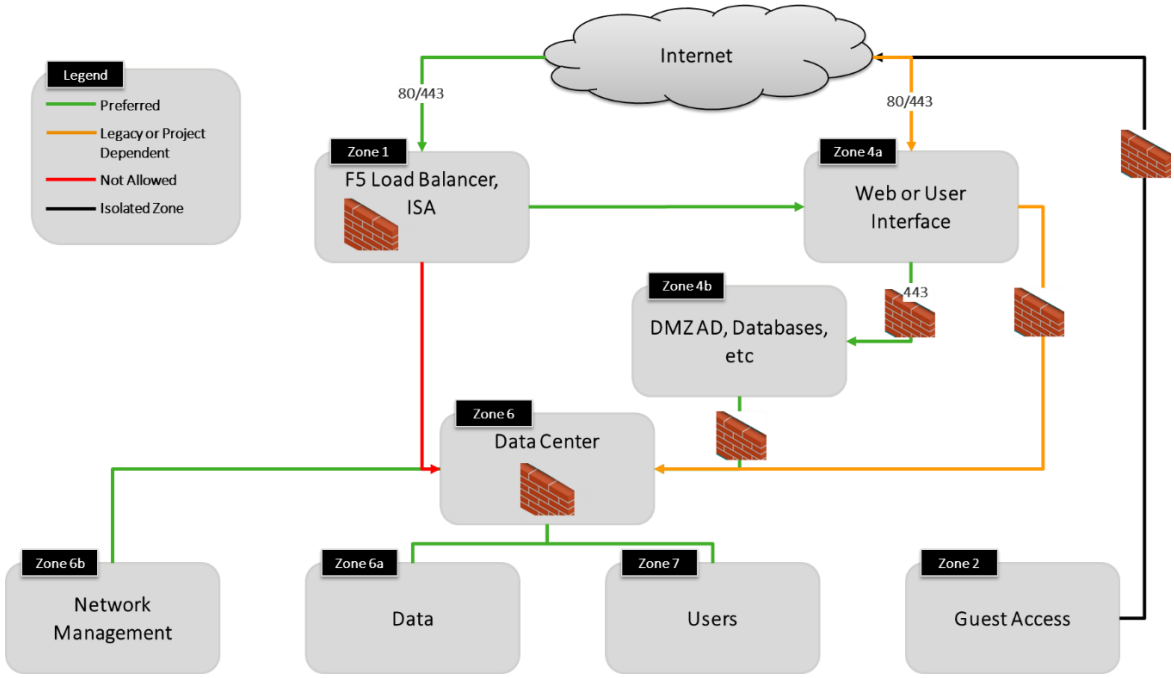
Wireless Access

Deloitte supports an internal wireless network within the organization. A wireless-security and acceptable-use policy is in place. Only Deloitte-approved access points will be connected to Deloitte's network.

- For wireless access to Deloitte's networks, personnel are required to use Wi-Fi Protected Access (WPA2 or stronger protection) where it is available.
- For the convenience of visitors, clients, or guests, a guest wireless network providing controlled access to the Internet may be made available in Deloitte's facilities.

Data Flow Diagram

Zone Flow – Basic Rules for Zone Flow



Name: Network Diagram.pptx
Revised 6/22/2020
Reviewed: 06/23/2020

Data Protection

Deloitte personnel receive training on the proper handling of PII. In instances where Deloitte may transmit client PII outside of the Deloitte environment, Deloitte requires transmission of such data in an encrypted format.

Media Protection

Secure printing is available at multiple locations within each Deloitte office that requires the usage of a Deloitte-issued electronic smartcard badge to enable the print job. Further, Deloitte issues encrypted USB drives to its personnel that meet the encryption standards outlined in Federal Information Processing Standard (FIPS) 140-2. In addition, software has been deployed to Deloitte-issued IT assets as part of the standard application toolset that allows the creation of encrypted WinZip files (FIPS 140-2 compliant).

Deloitte has implemented a technical control that encrypts data written/copied to external USB devices which can only be read by a Deloitte machine.

Laptops are encrypted and required to be physically secured at all times. Physical access to servers is restricted to authorized parties. Magnetic drives are wiped/over-written with a minimum of three passes with a media sanitization tool prior to being released for re-use and disposal.

Deloitte has employed the following methods of mobile device protection: 1) forced access PINs; 2) remote wipe in the event of 10 incorrect pin attempts; 3) remote wipe if the PDA is reported as lost or stolen; 4) encryption; and 5) an installed mobile device management tool.

Data Destruction

Policies and practices are in place with regards to the destruction of confidential information and PII that vary depending on type of media on which such information is stored. Deloitte is aligned with the National Institute for Standards and Technology's (NIST) guidelines for media sanitization. For example, hard disks, CD/DVD, USB drives are required to be wiped using a disk cleaning tool, while tapes are required to be destroyed at end-of-life. Paper containing such information is required to be shredded.

Encryption

Whole-disk encryption has been deployed on Deloitte-issued laptops. Deloitte's laptops have deployed encryption with the 256-bit Advanced Encryption Standard (AES) algorithm.

Deloitte has deployed encrypted USB drives intended for use in transporting sensitive or confidential data. This encryption method is FIPS 140-2 compliant.

WinZip is installed on all Deloitte-issued laptops. This encryption method is FIPS 140-2 compliant.

Additionally, Deloitte Internet email gateways are configured to attempt to transmit all email in an encrypted manner, using opportunistic TLS encryption, if the recipient of the transmission can support such encryption methodology. If TLS is enabled on the recipient email gateway, the email will be encrypted between the Deloitte gateway and the recipient gateway. TLS encryption can also be enforced when agreed with the recipient organization. This encryption method is FIPS 140-2 compliant.

Data in transit is protected by secure TLS using certificates with minimum 2048-bit RSA key and SHA2 signing when using Deloitte secure websites and file transfer services.

Secure File Transfer Protocol (SFTP) is an available option for the transfer of client data. SFTP securely encrypts and compresses files during transmission. This encryption method is FIPS 140-2 compliant.

Records Management

Deloitte maintains and retains records in accordance with applicable legal and regulatory requirements and professional standards. Specific areas of focus include:

- Facilitating compliance with external requirements and internal policies and practices pertaining to record retention;
- Managing recordkeeping critical to the operation of our business and service to our clients;
- Designing and implementing records management technology, tools, and standard processes;
- Coordinating the proper handling of files on legal hold due to legal, tax or regulatory preservation requirements; and
- Maintaining a strong, compliance-focused records and information management governance organization.