xDTM Standard

Version 1.0

March 2016

Table of Contents

The xDTM Standard

The Transaction Management Standard for an Open Digital World

Faced with the equally important objectives of increasing productivity and simplifying processes, global businesses are eliminating slow, paper-based workflows in favor of 100-percent digital ones. Digital Transaction Management (DTM) is a new category of cloud services designed to digitally manage transactions that include documents and data.

DTM removes the friction inherent in transactions. The benefits of paper-free, all-digital transactions include reduced transaction time, improved compliance with industry and government regulations, and streamlined business processes that enhance the customer experience.

Why a Standard?

Amidst a backdrop of record-high identity theft, frequent privacy breaches, and uneven availability of cloud services, the xDTM Standard allows DTM solution providers to establish trust and transparency when it is needed most. The xDTM Standard was developed to encourage and enhance the quality of digital transaction management solutions and to facilitate the broad adoption of DTM globally. Customers benefit from enhanced confidence in the security and availability of their digital transactions.

xDTM Standard Elements

Established by experts from diverse industries, the xDTM Standard includes a foundational set of criteria for managing digital transactions. Solutions that conform to the xDTM Standard meet high levels of quality across eight core areas:

Who Should Follow the Standard?

The xDTM Standard applies to digital transaction management providers that store, process, and transmit digital transactions. Entities that support the digital transaction management workflow and other organizations that would like to demonstrate a high level of quality in connected digital applications may also choose to follow the xDTM Standard.

How to Use This Document

This document, the xDTM Standard 1.0, was designed for use during xDTM Standard compliance self-assessments. The following sections provide in-depth guidelines and best practices to help entities to prepare for, conduct, and report the results of an xDTM Standard self-assessment.

The xDTM Standard comprises a minimum set of requirements for protecting and connecting digital transactions. The xDTM Standard does not supersede local or regional laws, government regulations, or other legal requirements.

With the xDTM Standard, organizations and consumers can leverage the speed, efficiency, and convenience of DTM to conduct critical transactions online without exposing them to the risks and consequences of using noncompliant technologies.

Security

The xDTM solution features best-in-class technical protection, highly secure access, and proactive protection policies as evidenced in the ways listed below.

1. Sensitive customer data, encrypted or tokenized at rest or in transit, adheres to a referable standard, such as NIST, ISO, or equivalent.

Companies providing xDTM services shall document their customer data policy or equivalent.

- The policy shall state the terms used by the company to classify and describe customer data that the xDTM solution captures, including how customer data is treated based on use context.
  - For example, designations of customer data (such as private, confidential, or secret) may be used, as long as they are accompanied by company-supplied definitions for those terms.
  - Use context must also be considered in classifying information. For example, certain customer data may be part of a customer agreement, while other customer data may be used to enable a customer-support purpose or serve as metadata about an agreement or transaction. The customer data policy shall reflect how data is secured based on its circumstances of use.
- Customer data shall be secured while at rest and in transit in accordance with the requirements in the company's customer data policy:
  - For Encrypted Data:
    - The policy shall state the level of encryption provided for data at rest, appropriate to the context for which it is being used.
    - For data in transit (defined as data flowing through networks), the policy shall state the strong ciphers and/or level of TLS encryption used, depending on type and use context.
    - Companies shall document that data currently encrypted by their xDTM solution is encrypted at no less than AES-128. Crypto systems established after the effective date of this Standard shall use AES-256 at minimum.
  - For Tokenized Data:
    - Companies that tokenize data shall document the types of transactions they are supporting and their compliance with regulations, such as PCI DSS, applicable to the type of data they are tokenizing.
    - Companies shall document their policy that tokenization algorithms used must not allow the unauthorized derivation of tokenized data from the tokens themselves.
  - In addition, the policy shall indicate the level of protection (encryption or tokenization) and access control in place as a part of measures to ensure that

company personnel do not have unauthorized access to transaction information included within a customer's agreement.

The company shall document the policies in place that require the use of the company's customer data policy (or equivalent).

Companies providing xDTM solutions shall follow industry-leading standards and best practices related to security:

- Companies will document their certifications, compliance, or internal policies that specify that the company meet particular standards. Policies shall also require that the company achieve certification to the latest versions of an applicable standard within 12 months of the most recent version being published.
- Examples of referable standards or certifications for companies providing xDTM solutions may include, but are not limited to:
  - ISO/IEC 27001 certification
  - ETSI EN 319 401
  - Standards or requirements from organizations such as the National Institute of Standards and Technology (NIST), the Federal Information Security Management Act of 2002 (FISMA), or others the company requires based on internal policies

2. Secure segmentation or containment of data is provided.

Companies providing xDTM solutions shall maintain a secure segmentation program and will document policies requiring, but not limited to, the following:

- Segmentation shall isolate specific systems and define authorized access through particular security zones.
- The xDTM solution and corporate business systems shall be maintained as physically and logically separate networks.
- Where applicable within a multitenant environment, xDTM solutions shall separate customer data so that each tenant views only their own information.
- Separate environments and data sets will be used for development, testing, and production to protect customer data.
- Data that is classified as requiring specific controls to meet legal, regulatory, or other compliance requirements will not be used in development or test environments.
- The secure segmentation program will include capabilities for managing inbound/outbound network traffic via firewalls in order to separate elements of the production environment from direct exposure to the Internet (e.g., a demilitarized zone or DMZ). Access to data storage should also be managed to prevent direct access, where appropriate.
- The secure segmentation program will include containment capabilities that enable xDTM solutions to ingest or render untrusted input in a safe manner, such as antivirus and virtualization.

- Companies will document a policy stating scope and frequency for reviewing corporate and production firewalls to ensure rule sets are configured to resist vulnerabilities. The policy will also identify an external validation method.
- Third-party service providers with access to production systems shall provide evidence of an independent assessment of their security controls annually.

3. Standards-based security systems at data centers (ISO or equivalent) are utilized.

Companies providing xDTM solutions shall operate their critical systems in a physically secured room or data center employing standards-based security, such as ISO/IEC 27001:2013, ISO 9001:2008, AICPA SOC 1, Type 2 or SOC 2, Type 2 attestations or other certifications. Secured systems shall include, but not be limited to, servers, firewalls, and storage.

Companies shall also document their policies that require the following:

- Only authorized personnel may access data centers.
- Access authorization is reviewed quarterly.
- CCTV monitoring is in place, with camera data retained for at least 90 days.
- Fire suppression and alarms for fire, water, and physical intrusion are in place and will automatically alert monitors responsible for responding.
- A member of the company's security organization has reviewed the physical security plan (in the case of an external data center).

4. Standards-based encryption key management is offered (ISO, NIST, or equivalent), including the ability for customers to hold encryption keys.

Companies providing xDTM solutions shall document their policies for encryption and key management.

Documented key management policies shall address:

- Protection of root keys for digital certificate hierarchies using dual control, split key components, and segregation of duties
- Physical security of keys
- Key custodianship, including internal control procedures and recovery capabilities
- Protection of encryption keys from unauthorized disclosure

In certain situations, encryption keys may be directly under the control of external customers, for example, banks managing keys on their own premises in order to maintain compliance with customer agreements, security policies, and regulations. Companies providing xDTM solutions for customers managing their own encryption keys shall document:

- Their solution can implement the key storage and release policies they run on their own platform on the external customer's private network
- They are ISO/IEC 27001 certified

5. Multi-factor authentication methods are deployed and documented.

Companies providing xDTM services shall document their policies requiring multi-factor authentication, including:

1. Authentication of internal personnel to internal company production systems
2. Authentication into administration environments

Access to the production environment shall be restricted to authorized users. Companies shall document that their policies for authenticating internal users to their production environment require:

- Users to log on over an encrypted VPN using multi-factor authentication
- Strong industry-standard encryption that meets globally recognized standards, such as the American or European standards of NIST or ETSI (e.g., ETSI EN 319 401), respectively
- Audit capabilities for privileged users

Access to internal administration systems that control, configure, or relate to an xDTM solution shall be restricted to authorized users. Companies shall document that their policies for authenticating internal users to their internal administration systems require:

- Users to log on over an encrypted VPN using two-factor authentication, or a private internal corporate network
- Strong industry-standard encryption that meets globally recognized standards, such as the American or European standards of NIST or European authorities, such as ETSI (e.g., ETSI EN 319 401), respectively
- Authentication mechanisms that provide identification of a specific user and his or her actions on the administration system

Companies shall document that their policy requires at least quarterly reviews of employee access to verify that only appropriate individuals have access to these environments and others, as appropriate.

6. The company performs periodic penetration testing by qualified third parties.

Companies providing xDTM solutions shall document their policies for conducting penetration tests as part of validating the security of their solution. Penetration testing shall include, but not be limited to, the following:

- Penetration testing shall be performed against the full external perimeter of the data environment, including testing against the network, application, and other appropriate infrastructure layers.

- Where segmentation policies prevent direct access to areas or components of the IT infrastructure, penetration testing shall test and validate the required separation.
- Penetration testing will be performed both externally from the Internet and internally as required to validate internal segmentation.
- Penetration testing will be performed no less than annually, and companies shall describe their required qualifications for testing by independent third parties.
- Companies shall document any policies requiring the company to perform more frequent penetration testing, such as an infrastructure change the company deems significant.
- Policies shall require that vulnerabilities experienced through penetration testing or other means in the last 12 months shall be regularly reviewed and assessed. Vulnerabilities that are deemed exploitable shall be corrected and re-tested.

7. The xDTM solution monitors for malicious and inappropriate activity on an ongoing basis.

Companies providing xDTM solutions shall document policies requiring precautions, such as monitoring and scanning, to protect customer data and the production environment.

Policy documentation shall include, but not be limited to, the measures below:

- **Vulnerability management**–companies shall perform vulnerability and network scans on a quarterly basis
- **Antivirus/antimalware**–companies shall deploy antivirus and antimalware capabilities on their xDTM solution and document their policies for updating to new virus/malware definitions
- **Intrusion detection**–companies shall document their policies for using intrusion detection systems and/or other real-time analysis tools
- **Endpoint security**–companies shall document their policies for providing endpoint security to workstations and laptops in their production environment
- **Email security**–companies shall document their policies for protecting email or messaging systems associated with the xDTM solution from phishing, SPAM, or other elements deemed inappropriate

8. The organization focuses on intelligence collection, leading to security breach detection and prevention.

Companies providing xDTM solutions shall document their policies for intelligence collection related to breach detection and prevention. Policies shall include, but are not limited to, the measures below:

- Policies for engaging with external organizations that provide resources on threat intelligence/monitoring, vulnerability management, or incident management
- Policies for engaging with security organizations and other groups that provide intelligence resources, such as:

- Governmental bodies
- Local or national law enforcement community meetings
- Open-source intelligence or threat feeds
- Peer organizations participating in information-sharing programs
- Cyber security research centers
- Information Sharing and Analysis Centers (ISAC)

- Policies requiring memberships, participation, or subscriptions to alerts from external security intelligence or threat monitoring organizations
- Policies that require the company to act on intelligence, including, but not limited to:
  - Creating incident reports, threat analyses, risk register entries, or reporting to the company security/risk council.
  - Log file analysis and reporting, IP blocking of bad sites, efforts to stop unauthorized online use of the company name by third parties, or other protective measures
  - Response times or other performance criteria related to intelligence collection

9. Provides the ability to anonymize data for participation in threat intelligence networks.

For companies providing xDTM solutions, sharing of anonymized transactional data could help in the containment, reduction, or elimination of a security threat.

Companies providing xDTM solutions shall document their policy for anonymizing data, indicating the form of anonymized data the company produces or languages the company may use for describing threat information in a standardized/structured manner. Examples include:

- Structured Threat Information Expression (STIX)
- Trusted Automated Exchange of Indicator Information (TAXII)
- Cyber Observable eXpression (CybOX)

In documenting this policy, companies shall indicate governmental laws, privacy requirements, or other regulatory requirements that govern their policy in this area.

10. The company employs a response model that adheres to applicable laws.

Companies providing xDTM services shall document policies to ensure their security threat response model adheres to applicable laws. Documentation shall contain, but is not limited to:

- Requirements for the company to comply with breach notifications and associated reporting requirements, including notifying individuals or customers impacted by a breach or applicable security incident
- Guidelines requiring the company to contact third-party organizations that manage data on the company's behalf or that may be impacted when the company has sustained a security incident

- The requirement for an appropriately trained forensic analyst for incidents that necessitate more rigorous analysis (in-house or provided via a qualified third-party)

Companies may choose to indicate where areas of their response model, such as notification deadlines, are incorporated into their incident response playbook.

11. The company has an incident response playbook in place.

Companies providing xDTM solutions shall document their policy requiring an enterprise-wide process or program that specifies guidance, procedures, and service-level agreements (SLAs) in response to a security incident, such as an incident response playbook.

Companies shall document:

- Participating internal organizations, role owners, and accountability
- Scope and procedures for containment, communication, and resolution
- Activities that have response times, as well as the required response times/SLAs
- How frequently the response program is reviewed and updated to reflect changing business conditions
- Scope and frequency of drills to validate program execution, such as tabletop exercises, red/blue team exercises
- Existing enterprise controls that measure the quality and response times of playbook execution and define the requirements for improving performance

12. The company maintains a mature security/risk council.

Companies shall design and document policies to ensure risks are evaluated and mitigated in accordance with management expectations.

Companies shall maintain a security/risk council or other internal governance organization and document its responsibilities for ensuring the company maintains policies and procedures for addressing risk areas, including, but not limited to, security risks, external threats, business continuity, and risks related to the company's external ecosystem.

The company shall document the following:

- A company-designated individual or role, such as the Chief Risk Officer, that is responsible for leading the security/risk council (or designated governance entity).
- The accountabilities of the Chief Risk Officer (or company designate), such as security policies, information security, or corporate security.
- The organizational structure associated with the security/risk council that provides the council with the visibility and authority to meet its accountabilities (a company org. chart, for example).

Companies shall document that the security/risk council is accountable for ensuring policies and procedures are in place to meet the company's responsibilities in areas including, but not limited to:

- **Threat mitigation**–implementing processes and procedures that:
  - Enable the company to identify potential threats
  - Assess associated risks
  - Develop mitigation strategies in response
- **Risk monitoring–**implementing processes and procedures that:
  - Monitor identified risks (for example, capturing them in a risk register)
  - Specify how to communicate risks throughout the organization
  - Assure that the security/risk council (or designated governance entity) receives regular reporting on monitored risks and mitigation strategies
- **Policies–**ratifying and disseminating new policies and policy changes for the following areas:
  - Information security
  - Security operations
  - Data breach notification
  - Business continuity
  - Physical security
  - Key management
  - Secure segmentation
  - Incident response program
  - Third-party security assessment program
  - Applicable ecosystem companies
- **Controls**–ensuring that existing company controls are effective when assessed against objectives for areas such as security and risk
- **Audits**–making sure that third-party audits are completed for areas where a need for independent verification has been identified
- **Personnel policies**–approving personnel policies related to mitigating risk and security issues, such as background checks, employee training, workplace standards, or termination procedures

Companies shall also document the policy requiring the security/risk council or internal governance team to review policies and procedures periodically and direct that they be updated, if deemed necessary.

Assurance

The xDTM Solution provides assurance that xDTM transactions are compliant with applicable laws.

1. The xDTM solution will comply with applicable laws, regulations, and industry standards.

- In accordance with leading DTM-compliance principles, companies providing xDTM solutions will enable:
  - Users to consent to do business electronically at a meaningful/appropriate time in the transaction
    - Consent for business transactions can either be expressed or implied
    - Consent for consumer transactions must be affirmative and electronic
  - Information integrity, reliability, and reporting
- Companies providing xDTM solutions shall document that their xDTM solution meets the requirements necessary to comply with applicable laws, regulations, and industry standards relevant to their digital transaction type, industry, geography, and use cases, as applicable. Examples of applicable laws, regulations, and industry standards include, but are not limited to:
  - ISO 27001
  - SSAE 16
  - HIPAA
  - PCI DSS
  - U.S. ESIGN Act
  - European Union Directive 1999/93/EC
  - European Regulation 910/2014 (also known as eIDAS)
  - TRUSTe
  - Skyhigh CloudTrust

Privacy

The xDTM solution allows a person or company to reveal information selectively, at their discretion, and meets the requirements outlined below.

1. Personal data is used for the purpose it was intended and is consistent with the organization's privacy policy.

Companies providing xDTM services shall document that personal data collected by or provided to the xDTM solution will only be used for its intended purpose, which is within the confines of digital transactions, including electronic execution of contracts and application of electronic signatures.

Companies shall also document:

- Treatment of personal data if the company is acquired or sold, including, but not limited to, changes in how personal information may be used, choices users may have regarding the use of their personal information, and notifying users via email or site notices about changes in ownership
- Policies that prohibit service providers (used to facilitate or outsource aspects of the company's service) from using data for any purposes other than the contracted services
- Policies that prohibit employees, including customer support, from viewing the content in customer documents
- Customer service policies indicating what information may be accessed by support personnel when responding to a customer's request
- System maintenance policies that specify what information the xDTM company may see in connection with maintaining the xDTM service, for example, customer metadata

Companies providing xDTM services shall document their assessment procedures for ensuring that only the personal information described in notices is collected and retained, and that the personal information collected is necessary to accomplish the authorized business purpose.

2. Treatment of notice, consent, and choice is clearly reflected in a publicly available, written privacy policy.

Companies providing xDTM services shall maintain a publicly available, written privacy policy that describes the following:

- The personal information collected by the service or solution as part of its normal operation
- How personal information may be used, shared, or maintained by the service
- The means by which users accept the policy (e.g., the act of registering) and what their acceptance signifies (e.g., they are expressly consenting to the company's privacy policy)

- Circumstances where personal information may be disclosed in the normal scope of business, as required to provide services associated with the xDTM solution

Companies shall also document in their privacy policy that in the course of transacting on an xDTM platform, users may access the personal information of other participants in the transaction. Accordingly, the policies shall communicate that such personal information may only be used in services offered by the xDTM platform and related communications that are not unsolicited commercial messages.

Companies providing xDTM services shall document their policies regarding the collection, use, and retention of personal information as it relates to compliance with international data transfer requirements. Examples include Binding Corporate Rules, the EU-US Privacy Shield, and the U.S.-Swiss Safe Harbor Framework.

Companies providing xDTM solutions should strive for third-party verification of their compliance choice, where possible.

3. Policies addressing transaction retention and purging are clearly stated.

Companies providing an xDTM solution shall:

- Document the capabilities in the xDTM solution that enable customers to configure retention and purging policies for transactions, documents, or data that align with the policies of their organization
- Warrant that their xDTM solution complies with applicable regulations requiring information to remain available, such as the US E-SIGN Act, European Regulation 910/2014, or regional equivalents
- Record the solution's policies governing the treatment of documents or transactions that are completed, declined, or voided with respect to what is:
    - Stored by the solution
    - Removed from the customer's view (deleted)
    - Removed from the system (purged)

4. Private information is only provided to government organizations when there is a good-faith belief that such disclosure is reasonably necessary to comply with any applicable subpoena or other legal process or to protect the rights, property, or safety of anyone.

Companies providing xDTM services shall document that it is their policy to not knowingly disclose an individual's private information to a government organization.

Companies shall document exceptions to this policy, such as:

- The company has the individual's permission to disclose the information.
- The information is publicly available.

Companies shall document their policy for providing information to law enforcement and other government agencies, including:

- Circumstances necessitating the sharing of information, such as receiving a subpoena or court order, a potential threat to the physical safety of a person, and preventing suspected illegal activity
- The type of information the company may provide in response to a law enforcement or government request

5. Company policies include measures to evaluate the potential to cause harm by releasing private data.

Companies providing xDTM services shall document their policies for evaluating the potential to cause harm through the release of private data due to breach, accidental disclosure, or compliance with the law.

Policies that companies may utilize include, but are not limited to those requiring the:

- Use of a formal risk assessment methodology to both evaluate the scale or impact of harm and assess the effectiveness of available mitigations
- Creation or maintenance of controls, such as policies and procedures, to implement or execute mitigation strategies for this risk
- Company to periodically reassess existing policies and procedures used to assess harm from a data release and revise them as appropriate
- Reporting and resolution (including a risk register or similar risk tracking) and a point of accountability for resolution, such as a security/risk council

☑ Validity

The xDTM solution has a reliable, transparent, and verifiable chain of custody, and a digitally signed, tamper-evident audit trail and shall provide or enable the capabilities listed below.

1. Transparency into relevant transaction attributes, such as transaction or message origin, author, content, and transmission time.

In support of transparency, providers of xDTM services shall provide capabilities for transaction documentation that include the following attributes:

- Number of pages or items for all documents or data in a transaction
- Originator detail, including identity or contact information for the person or system that sent the documents or data, as well as the IP address
- Transaction status, spanning initiation and in-process through to completion
- Storage information, indicating where the completed documents and final data are held
- Recipient contact information for each document or data component
- Information that indicates what authentication methods were used and whether they were satisfied
- Confirmation of whether the recipient agreed to any disclosures, as well as the content of the disclosures
- Event and action timestamps to support a detailed audit trail for the transaction with integrity protection

2. A verifiable chain of custody for each custodian that includes document/transaction, metadata, and history/future length of contact.

Companies providing xDTM services shall document the ability of their solution to deliver a chain of custody for transactions executed on their platform, including, but not limited to:

- Tamper-evident indicators that provide additional robustness to the chain of custody
- An activity history that includes key events and transaction details

The xDTM solution shall utilize tamper-evident capabilities to secure documents and signatures.

- Companies shall document the safeguards in place, such as digital certificate technology, to ensure signatures and documents on their platform are not modified in an unauthorized manner.
- Companies shall document the tamper-evident measures, such as hashing technology, that are used by their xDTM solution to verify that a document has not been modified after it has been downloaded from the solution.

The Chain of custody capabilities above shall be augmented with capabilities that:

- Enable an audit trail
- Provide proof of integrity

3. Appropriate credentialing, such as criteria for credentials, credential creation, and documented treatment of co-transactors.

The xDTM solution shall enable a customer to select credentialing methods for participants in the transaction, including co-transactors or signers, which the customer deems appropriate to the sensitivity of the agreement or subject matter of the transaction.

Companies providing xDTM services shall document the end-customer authentication capabilities provided by their solution. Examples include, but aren't limited to:

- Email
- Access code
- SMS authentication
- Federated identity authentication
- Knowledge-based ID check via publicly available knowledge-base information
- Social ID login
- Hardware or software token

The xDTM solution shall enable customers to use more than one authentication method simultaneously to verify a participant, such as requiring a participant to correctly provide an access code and a correct social login ID.

Companies shall document that their solution enables customers to authorize privileges for participants in a transaction, including, but not limited to, capabilities that:

- Enable a sender to edit documents or limit interactions with documents (e.g. read only)
- Allow a participant to change their signing responsibility or transfer it to another person
- Require participants to sign in a particular order
- Enable senders to manage participants outside of their own organization (such as externally managed accounts), including:
    - Granting credentials
    - Authorizing or un-authorizing the participation of external signers in company-related documents and transactions

4. Clear evidence of agreement, including manifestation of assent, intent to transact, attribution, and audit trails.

xDTM companies shall document the capabilities of their solution to provide evidence of agreement, assent, intent to transact, and attribution. Examples include, but are not limited to:

- Explicitly obtaining "consent" from all parties to transact electronically, prior to the electronic transaction process
- Allowing for consent to be withdrawn, as specified in applicable regulations
- A user experience that simulates the transaction process to make it obvious the act of transacting is taking place; for example, in the case of an electronic signature, the use of an online "button" to start the signing and/or the graphical representation of the signer's name in a handwriting font
- Allowing a participant to add his or her evidence of assent to the document
- Ensuring attribution by associating a participant to a document or transaction via multiple methods of authentication
- Obtaining a confirmation that the participant wants to complete the transaction, so that the participant cannot subsequently claim a defense that he or she transacted by mistake

The xDTM solution shall provide an audit trail capturing a history of activities associated with each transaction. Companies shall document that the xDTM solution provides a transaction log or equivalent that captures and documents the following items where applicable:

- Authorized user
- Email addresses
- Event dates and times
- IP address used to access the system
- Sending notices
- Viewing events
- Signing or declining
- Forwarding
- Voiding
- Reassignments
- Authentication failures
- Complete or in-process status

Company policies shall document how the transaction log is managed, secured, and accessed so that unauthorized changes to a transaction log cannot be made without detection.

Companies providing xDTM services shall have the capability to provide transaction audit information that can be admitted into court as proof of the transaction.

The validity capabilities above shall be augmented with capabilities that:

- Provide additional support for an audit trail
- Enable a chain of custody
- Provide proof of integrity

5. Complete records management, including long-term records management with proof of integrity, designated document retention periods, and transferability.

Companies providing xDTM services shall document the following capabilities of their platforms:

Records Management

- All retained customer data shall be stored at the level of security and encryption required by the xDTM company's customer data policy.
- Companies providing xDTM solutions with a vault, storage appliance, or other storage solution, either directly or via partnership with a third-party company, shall document the compliance of the storage solution to the areas of the xDTM Standard they believe are applicable.
- The xDTM solution shall meet additional requirements related to records management.

Document Retention

- The xDTM solution shall meet requirements related to document retention.

Proof of Integrity

- When transactions include stored documents, these documents shall be secured with tamper-evident seals to ensure they are not altered without authorization.
- Companies shall use strong industry-standard security for their anti-tamper technology and document the encryption standard utilized (e.g., X.509 Public Key Infrastructure Standard).

Transferability

- The xDTM solution shall enable portability, such that documents that have been completed and/or transaction data that is stored (as applicable) is transferable.
- When transactions include stored documents, documents transferred out of the xDTM service shall retain their tamper-evident capabilities in order to preserve document integrity.

6. An industry-standard clock time convention from a trusted third-party source of time.

The xDTM solution shall follow an industry-standard clock-time convention from a trusted third-party source of time to ensure accuracy in records and audit trails.

- Companies shall document that their xDTM solution is synchronized with and creates timestamps for actions within the solution, based on a trusted third-party source of time.
- Companies shall document the source of time used in their xDTM solution, for example, Network Time Protocol or NIST Internet Time Service.
- In regions where government regulations require an xDTM solution to use a hardware appliance for time-keeping requirements, companies shall document that they conform to this legally mandated requirement.

Availability

The xDTM solution ensures that transactions are always accessible and obtainable, high performing during periods of peak use, resilient across disaster scenarios, and free of scheduled offline maintenance.

1. The solution offers carrier-grade availability/system uptime.

The xDTM solution shall be highly available and engineered for carrier-grade performance with a demonstrated ability to deliver system uptime of 99.9% based on the following definition:

- Availability will equal the time the xDTM solution is available for customers as a percentage of all the time in that period
- The period for the availability calculation will include all of the previous 12 months (or since service inception if less than 12 months)

Note:

- *The impact of any outage downtime is reduced if only a percentage of all customers are impacted by the outage.*
- *The availability requirement applies only to the solution's boundary to the Internet.*
- *No allowance is given for maintenance.*

Calculation Method

Example of an availability calculation for the past 12 months
= (Outage minutes) * (% customers impacted) / (525,600)
= 1 - (outage calculation above)
= * 100 to create a percentage

(Note: 525,500 is the total minutes of possible availability in 12 months.)

Companies shall publish availability statistics for their xDTM solution on a public-facing website.

2. The solution is continuously available – online/offline – with no maintenance downtime.

The xDTM solution shall operate with zero downtime for offline maintenance. Companies providing xDTM solutions shall document their policy to meet this requirement.

3. Customer data is continuously accessible for customer use.

Companies providing xDTM solutions shall maintain two copies of backed-up data within the datacenter in use. This will be the Version Retention Objective (VRO) for the xDTM Standard.

4. Redundant geographically-dispersed data centers are used.

Companies providing xDTM solutions shall store replicated versions of customer data in redundant, geographically dispersed data centers. This shall serve as a supplemental means of ensuring that data remains available for customers in the event of system failure.

The Geographic Redundancy Objective (GRO) requirement for the xDTM Standard:

- Companies shall maintain two backups of the original data at a minimum of two additional data centers.
- Data centers shall be geographically separated as an additional risk-mitigation measure.
- The amount of customer data replicated to a data center shall be sufficient to restore the service to normal function.

Companies providing xDTM solutions shall document their policy to meet this requirement.

5. There is zero data loss during catastrophic events.

The xDTM solution shall preserve data in the event of a significant disruption to the service using data protection capabilities.

The solution shall be engineered to achieve a data loss of no greater than 0 minutes with a demonstrated ability to achieve a data loss of no greater than 5 minutes, its Recovery Point Objective (RPO).

- The RPO of 5 minutes shall be defined as the maximum time duration between data protection events, where exposed data is subject to unrecoverable loss.
- The scope of data protection events conducted by the xDTM solution shall capture the then-current state of data changes on the service (e.g. data creation, modification, and deletion).
- The RPO shall be scoped to apply to performance within a single data center to assure that simultaneous data replication is able to occur.

The company shall also document their policy to maintain a disaster recovery or business continuity plan, specifying additional actions they will take in the process of system recovery.

Companies shall provide information on data losses that have occurred within the past six months to qualified customers upon request.

6. There is sub-minute service restoration after a disruption.

The xDTM solution shall be engineered to achieve sub-minute restoration after a disruption (with failover capabilities to recover quickly from a service interruption).

The xDTM solution shall have a demonstrated ability to achieve a return to service in 15 minutes or less, its Recovery Time Objective (RTO).

- The RTO is defined as the targeted maximum length of time an xDTM solution is unavailable before it is returned to service at the boundary of the Internet and available for customers.
- In addition, the recovery time calculation shall include the time required to migrate information from the prior point of service to the new point of service, if necessary.

xDTM companies shall also provide information on service disruptions lasting longer than 15 minutes that have occurred within the past six months to qualified customers upon request.

Downtime from any service disruptions will be included in publicly posted availability data (as described in section 1).

7. Customer transaction support is provided.

Companies providing an xDTM solution shall provide customer support for all transaction types offered by the solution.

Companies shall document the available customer support services, including, but not limited to:

- Support case services, including:
  - Self-service documentation
  - 24x7 live or chat support
  - 24x7 emergency support, including response SLAs
  - Case submission and management services, including response SLAs
- Support for compatibility testing and integration point testing, such as:
  - Demo/sandbox access, where customers can test their internal code against new or upcoming releases of the xDTM solution
  - The ability for customers to test new code their organization is developing against the xDTM solution prior to the customer's internal release
  - Connectors/integration support between the xDTM solution and third-party solutions (note: documentation should confirm the presence of handoff procedures specifying how errors will be handled by the xDTM solution should a problem occur on the third-party application or service)
- Support resources that facilitate additional learning about the xDTM solution, such as:
  - Courses and certifications to help ensure successful solution implementations
  - Training, tools, and access to user communities to further supplement and share knowledge

8. The organization maintains a trust center for transparency into service performance, availability, certification status, and privacy.

Companies providing xDTM services shall maintain an external, customer-facing trust center (or similar self-service means) that provides information on the solution's performance, availability, certification status, and privacy.

The trust center shall provide information and guidance to customers and other external parties in the following areas:

Companies providing xDTM solutions shall provide and document status information to customers, including, but not limited to:

- Status confirmations that the xDTM solution is available and operating normally
- Alerts regarding service disruptions
- Information on planned system changes that may impact availability
- Updates and alerts on security threats the company deems relevant

Companies shall display the security and privacy-related certifications in their trust center (or equivalent) for external reference purposes.

Scalability

The xDTM solution accepts increased volume without impacting performance due to ongoing capacity modeling and proactive lifecycle management and adheres to the criteria outlined below.

1. **There is a formal process in place to anticipate future business growth/needs with the ability to provide ongoing system capacity modeling.**

   Companies providing an xDTM solution shall document policies requiring a formal planning process for increasing the capacity of their xDTM solution in anticipation of expected future business growth. Examples include, but are not limited to:

   - Event-based capacity modeling/planning, such as calendared or cyclical planning processes
   - Data-driven planning, such as performance monitoring capabilities that provide information for capacity planning actions with threshold values or triggers

2. **There is a formal lifecycle management in place with proactive implementation of architectural changes and hardware purchasing.**

   To scale their xDTM solution, companies shall proactively implement architectural changes and acquire needed hardware.

   Companies shall document that they incorporate a minimum of a primary and secondary method in combination from the options below, for planning and implementing changes required to scale their solution:

   - Monitoring and assessment of KPIs related to system performance, which may include both software and hardware measures (e.g., mean time to response, CPU utilizations, network latency measurements, BIOS/operating system-level measurements, performance of virtual machines, Web page delivery times)
   - Frameworks for determining specific scenarios or conditions where graceful degradation of capabilities is required under high load
   - Technology maturity models that enable the company to benchmark aspects of their infrastructure versus the capabilities of a more fully realized operation (across dimensions, such as technology, operational processes, or others specified by the company)
   - Creating and using predictive models to indicate limitations of the current infrastructure, including validating these models with analytical techniques, such as simulations using load generators

- Scale-up/scale-out: assessing efficiency tradeoffs in hardware-based alternatives to grow capacity (e.g., replacing a current server with a more powerful one versus adding another server to an existing set).
- Hardware sizing, or assessing additional alternatives to address performance degradation, in order to identify performance improvements from capacity increases in CPU, memory, hard disk, and/or network hardware (e.g., addressing poor response times caused by insufficient network bandwidth)

Universality

The xDTM solution functions across heterogeneous environments/devices and is accessible worldwide according to the guidelines detailed below.

1. The solution is available across heterogeneous computing platforms.

Companies shall make their xDTM solution available across heterogeneous computing platforms to ensure it is broadly accessible to customers.

To be compliant with the xDTM Standard, an xDTM solution shall be available to a minimum of 90% of computer users in the regions served by the solution, through the solution's application compatibility with the operating systems and/or browsers in those regions.

For the regions where the solution is offered, companies shall document:

- The operating systems and desktop browsers for which their solution has passed application compatibility testing
- The percentage of users the solution is able to reach in the regions, as a result of their solution's compatibility

Companies shall make their xDTM solution available on mainstream computing devices, such as smart phones and tablets, to ensure it is broadly accessible to customers.

To be compliant with the xDTM Standard, an xDTM solution shall be available to a minimum of 90% of mobile device users in the regions served by the solution, though the solution's application compatibility with the mobile operating systems and mobile browsers in those regions.

For regions where the solution is offered, companies shall document:

- The mobile operating systems and browsers for which their solution has passed application compatibility testing
- The percentage of mobile users the solution is able to reach in the regions, as a result of their solution's compatibility

Note: When citing market reach data for platforms or devices, a company may use data from a referable source of their choosing.

Companies shall document whether their solution is available as a dedicated mobile app.

Companies shall document that their xDTM solution provides offline functionality, such that a digital transaction may be initiated or completed in situations where network or carrier service is not available.

Examples of offline capabilities include, but are not limited to:

- The ability to initiate a transaction while offline
- Preparing documents for sending while offline (via caching, for example)
- Completing automatic sending and required synchronization when network availability or carrier service returns

2. The solution is accessible worldwide.

Companies providing xDTM solutions shall ensure their solutions are broadly accessible to customers in the regions where they are providing their solution. For example, companies that serve a global audience shall strive to make their xDTM Solution accessible worldwide:

- Companies providing xDTM solutions shall document which geographies are targeted by their solution.
- Companies providing xDTM solutions shall document the languages available in the xDTM solution's user interface (for both transaction initiators and acceptors) and indicate which language(s) is designated as primary for that locale.

Interoperability

The xDTM Solution works across collaborative services environments and includes integration guidelines and APIs with the characteristics detailed below.

1. The solution has published integration guidelines.

Companies providing xDTM solutions shall publish integration guidelines, such as REST, SOAP, or other API's. These capabilities may be used to manage workflows within the xDTM solution, as well as provide a means for collecting information from another application or service and incorporating it into the xDTM solution. This includes form data, an electronic signature, and other indications of a transaction.

Companies shall document that the integration capabilities of their xDTM solutions, such as APIs, for example, support the required functionality shown below with respect to integrating with external applications or services.

Integration Area	Capabilities of the Integration Mechanism
Workflow	• Creating, sending, receiving, and editing documents and transactions • Specifying routing for transactions • Performing batch operations on documents
Secure Authentication	• Validation of both the user and authorized integrator for all transactions
Participant Authentication	• A secure, industry-standard API authentication mechanism • Acceptance authentication into the xDTM Solution • Authentication of transaction participants into the xDTM solution
Reporting	• Event-triggered status updates • Performance verification, such as the ability to provide failure notifications or support for transaction logs • Security reporting

Companies providing xDTM solutions shall document their API support for developers in the areas outlined below:

- Software Developer Kit (SDK)
- API documentation

- Code libraries and code samples
- Sandbox or developer testing capabilities, such as developer keys

2. The solution accepts multiple digital/public key (PKI) certificates.

The xDTM solution shall enable a document to be signed with a digital signature in regions or with governments or industries that require them, if the company is processing transactions in those regions.

- The xDTM solution shall accept digital/Public Key (PKI) certificates that conform to X.509 standards.
- The xDTM solution shall accept qualified certificates as defined in EU Directive 1999/93/EC or European Regulation 910/2014 (as applicable).
- The company shall indicate the certificate authorities or service providers that qualify as accepted providers of digital certificates by their solution.

The company providing the xDTM solutions shall maintain a certificate policy regarding their acceptance and use of certificates. The company shall document that the areas addressed by their policy include, but are not limited to:

- The policy used by the company to determine acceptable certificate authorities or service providers
- The types of identity verification the company requires of accepted certification authorities or service providers (corresponding to the level of certificate offered)
- The criteria for determining acceptable identity documents, for example, government-issued ID, required level of consistency with other sources of identification, or cases where an in-person visit to verify identify is required

3. Data will migrate to current standards over time to enable ongoing accessibility and transaction or document longevity.

Companies providing xDTM solutions shall document their policy requiring that data created or stored by their xDTM solution shall remain available or migrate to a format or data standard accessible to authorized users for an appropriate duration of time, such as the life of the transaction or legal requirements.

Companies shall document that their policy for data created or stored (or equivalent) includes, but is not limited to, the following areas:

- New formats: the policy used to determine if a new data standard or format shall be supported by the xDTM solution
- Backwards compatibility: the policy used to determine the number of future versions of the xDTM solution that will support a particular standard or format
- End of life: the policy used to determine when a particular data standard or format will no longer be supported by the company's xDTM solution

- Triggers: the conditions that initiate the assessments regarding new formats (e.g., the process is calendar-based, metric driven, or initiated upon receiving a customer request)
- Data: the types of information sources used as inputs into these determinations, such as external market or user data

An xDTM solution shall accept a range of data standards and formats, and companies shall document the supported standards and formats spanning the areas below (as applicable):

- Documents (e.g., .docx, .html, .rtf, .txt)
- Drawings (e.g.,.dwg, .dxf, svg, .vsd, .vss, .vst)
- Images (e.g.,.bmp, .gif, .jpg, .png, .tiff)
- Presentations (e.g., .dpt, .pot, .pps, .pptx)
- Spreadsheets (e.g., .csv, .xls, .xlsx, .xlt)
- Storage formats (e.g.,.pdf)

4. Limitations of the service's ability to support valid transactions are disclosed.

Companies providing xDTM services shall communicate updates and changes in their xDTM solution necessary for the solution to continue executing valid transactions.

Companies shall document their methods or programs for communicating the minimum requirements to use their service. Examples of document types or resources include, but are not limited to:

- Minimum software requirements (operating systems) and detail on security settings
- User roles required by the service, such as an administrator, notices generated by the service or requirements to create accounts
- Limitations to current features (e.g., a bulk send feature is limited to a certain number of recipients)
- Periodic communications on changes, such as quarterly release notes
- Core requirements and functionality of the solution (for example, a service specification)

Companies shall document their methods for communicating changes to their service. Example documents, resources, and communications include:

- Planned changes in requirements for using the service where particular technologies may no longer be supported (e.g., an older browser)
- Discontinued support for a previously supported feature, which could have implications for current users (e.g., discontinuing the use of SSL V3 due to a security-related decision) or could impact the ability of users of particular browsers to connect to the service, for example
- Timely information related to the evolution of the xDTM service in the form of release notes or similar communication to inform customers of service enhancements that

could introduce misalignments with aspects of a customer's own operations or technology infrastructure, such as application compatibility issues

Selected Glossary and References

AICPA SOC 1, Type 2
A SOC 1, Type 2 report describes the internal controls in place over financial reporting at an organization and requires a third-party service auditor to review and examine the organization's operations over a set period of time.

AICPA SOC 2, Type 2
A SOC 2, Type 2 report describes the controls in place at a service organization for security, availability, processing integrity and confidentiality. It's intended to provide additional assurance to users of the organization's services about the security and privacy of their data.

AES-128, AES-256
The Advanced Encryption Standard (AES), also known as Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The numbers 128 and 256 refer to the key lengths.

Audit Trail
An audit trail (also known as an audit log) is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected a specific operation, procedure, or event at any time.

Binding Corporate Rules (BCRs)
BCRs were developed to allow multinational corporations, international organizations, and groups of companies to make intra-organizational transfers of personal data across borders in compliance with EU Data Protection Law. They're an alternative to the U.S. Department of Commerce EU Safe Harbor and EU Model Contract Clauses.

Business Continuity
Business continuity encompasses a loosely defined set of planning, preparatory, and related activities that are intended to ensure that an organization's critical business functions will either continue to operate despite serious incidents or disasters that might otherwise interrupt them or be recovered within a reasonably short period.

Caching
A cache is a collection of data that duplicates original values stored elsewhere on a computer.

Carrier-Grade
Carrier-grade systems are tested and engineered to meet or exceed "five nines" high-availability standards and provide very fast fault recovery through redundancy (normally less than 50 milliseconds).

Chain of Custody
Chain of custody refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.

Code Library
A code library is a set of routines for a particular operating system. Depending on the environment, code libraries may be source code in an intermediate language or in executable form.

Credentials
A credential is an attestation of qualification, competence, or authority issued to an individual by a third party with relevant or de facto authority or assumed competence to do so.

Cyber Observable eXpression (CybOX)
CyBOX is a standardized language for encoding and communicating high-fidelity information about cyber-observable events, whether dynamic events or stateful measures that are observable in the operational cyber domain.

Data Breach
A data breach is the intentional or unintentional release of secure information to an untrusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak, and data spill.

Digital Certificate
Also known as public key certificate or identity certificate, a digital certificate is an electronic document used to prove ownership of a public key. The certificate includes information about the key, its owner's identify, and the digital signature of an entity that has verified the certificate's contents are correct.

Digital Signature
A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature shows recipients that a known sender created the message, and it prevents senders from denying they sent the message.

Digital Transaction Management (DTM)
DTM is a category of cloud services designed to digitally manage document-based transactions. DTM goes beyond content and document management to include e-signatures, authentication, and nonrepudiation; document transfer and certification; secure archiving (more than simply records management); and a variety of meta-processes around managing electronic transactions and the documents associated with them.

eIDAS
Also known as European Regulation 910/2014, eIDAS is a European regulation on electronic identification and trust services for electronic transactions in the internal market. It repeals E-Signatures Directive 1999/93/EC. This regulation seeks to create a system of mutual recognition

among Member States with regard to their national identification systems, and thereby aims to enhance trust and effectiveness within the European internal market for public and private cross-border online services and e-commerce.

Electronic Signature
An e-signature is any electronic means that indicates either that a person adopts the contents of an electronic message or, more broadly, that the person who claims to have written a message is the one who wrote it (and that the message received is the one that the person sent).

Endpoint Security
Endpoint security refers to a methodology of protecting the corporate network when accessed via remote devices, such as laptops or other wireless and mobile devices. Each device with a remote connection to the network creates a potential entry point for security threats.

ETSI EN 319 401
ETSI EN 319 301 is a standard from the European Telecommunications Standards Institute that specifies policies and practices requirements for Trust Service Providers (TSPs). Example TSPs include certificate issuers, signature generators, or similar providers of validation services. An objective of the Standard is to assure confidence in transactions through practices that minimize threats and risks.

European Regulation 910/2014
Also known as eIDAS, European Regulation 910/2014 is a European regulation on electronic identification and trust services for electronic transactions in the internal market. It repeals E-Signatures Directive 1999/93/EC. This regulation seeks to create a system of mutual recognition among Member States with regard to their national identification systems, and thereby aims to enhance trust and effectiveness within the European internal market for public and private cross-border online services and e-commerce.

European Union Directive 1999/93/EC
This is a European Union Directive on the use of electronic signatures in electronic contracts within the EU. It's commonly referenced as the test(s) that electronic signature technology has to pass to be used in various legally binding manners within the EU.

EU-US Privacy Shield
The EU-US Privacy Shield is a new framework for transatlantic data flows. It reflects the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old Safe Harbor framework invalid. The new arrangement provides stronger obligations on companies in the U.S. to protect the personal data of Europeans and tougher monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission (FTC).

Geographic Redundancy Objective (GRO)

GRO encompasses what data needs to be replicated off site, how often, and how far. It typically has its own set of requirements for recovery point and recovery time objectives that are often less stringent than the standard RPO and RTO.

Hardware Sizing
Hardware sizing is the process of estimating and optimizing the hardware required to deploy or scale a particular solution. It considers factors such as use case scenarios, availability requirements, required network bandwidth and speed, CPU/processing power, process concurrency, software performance (such as databases), and others.

HIPAA Privacy Rule
The HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically. The rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

Intrusion Detection
An intrusion detection system is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.

IP Blocking
IP address blocking prevents connection between a server or website and certain IP addresses or ranges of addresses.

ISO
The International Organization for Standardization (ISO) is an international standard-setting body composed of representatives from various national standards organizations. It promotes worldwide proprietary, industrial, and commercial standards.

ISO/IEC 27001:2013
ISO 27001:2013 is specification for an information security management system (ISMS). Organizations that meet the standard may gain an official certification issued by an independent and accredited certification body on successful completion of a formal audit process.

ISO 9001:2008
ISO/IEC 9001:2015 specifies requirements for a quality management system when an organization needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements and aims to enhance customer satisfaction through the effective application of the system.

Load Generator
A load generator is a system that is used to simulate load for executing performance testing, such as concurrency testing or SQL performance testing.

Log File Analysis
Log file analysis is an art and science analyzing, assessing, or otherwise seeking to make sense out of computer-generated records (also known as log or audit trail records).

Mean Time to Response
Mean time to response is how long it takes to receive a response—on average—to an executed request or expected event.

Metadata
Metadata is data that provides information about other data. There are two types of metadata, structural (data about the containers of data) and descriptive (uses individual instances of application data or the data content).

Network Latency
Network latency is how long it takes for a bit of data to travel across the network from one node or endpoint to another.

Network Time Protocol
One of the oldest Internet protocols in use, network time protocol is a convention for clock synchronization between computer systems over packet-switched, variable-latency data networks. It's intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time.

NIST Internet Time Service
The National Institute of Standards and Technology (NIST) provides the official time to the United States. The organization offers time-related protocols and technical services that may be used in business processes and technologies.

PCI DSS
The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle credit cards from the major card schemes, including Visa, MasterCard, American Express, Discover, and JCB. Private-label cards that aren't part of a major card scheme aren't included in the scope of the PCI DSS.

Penetration Testing
A penetration test is a software attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data.

Public Key Infrastructure (PKI)
A PKI is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public key encryption. The purpose of a PKI is to

facilitate the secure electronic transfer of information for a range of network activities, such as e-commerce, Internet banking, and confidential email.

Recovery Point Objective (RPO)
An RPO is the maximum targeted period in which data might be lost due to a major incident. RPO is determined by looking at the time between data backups and the amount of data that could be lost in between those backups.

Recovery Time Objective (RTO)
An RTO is the target time set for the recovery of IT and business activities after a disaster has struck. In other words, it's the maximum length a given application or system can be offline.

REST API
When Web services use representational state transfer (REST) architecture, they are called REST APIs (application programming interfaces). REST architecture involves reading a designated Web page that contains an XML file, which describes and includes the desired content. Once dynamically defined, consumers may access the interface.

Risk Register
A risk register is a scatterplot used as a risk management tool to fulfill regulatory compliance, acting as a repository for all risks identified and including additional information about each risk, e.g., nature of the risk, reference, owner, and mitigation measures.

Sandbox
A sandbox is a security mechanism for separating running programs and is often used to execute untested code or untrusted programs from unverified third parties, suppliers, untrusted users, and untrusted websites.

Scalability
Scalability is the capability of a system, network, or process to handle a growing amount of work, or its potential to be enlarged in order to accommodate that growth.

Secure Segmentation
Secure Segmentation is the practice of separating a computer network into separate zones, segments, or sub-networks. This provides the organization with more granular control on what portions of the infrastructure a person may be authorized to access and improves security by limiting visibility of the full network structure.

Security Threat Analysis
A security threat analysis analyzes application architectural information to develop a threat profile for the application components.

Skyhigh CloudTrust Program
The Skyhigh CloudTrust Program helps lower risk and streamline the evaluation process by providing an objective and comprehensive evaluation of a service's security controls and

enterprise readiness based on a detailed set of criteria developed in conjunction with the Cloud Security Alliance (CSA).

SMS Authentication
Two-factor authentication provides identification of users via a combination of two different components (such as something the user knows or possesses or something that is inseparable from the user). SMS authentication is a form of two-factor authentication that uses mobile devices as the "something that the user possesses."

SOAP API
Simple Object Access Protocol is a messaging protocol that allows programs that run on disparate operating systems (such as Windows and Linux) to communicate using Hypertext Transfer Protocol (HTTP) and its Extensible Markup Language (XML).

Software Developer Kit (SDK)
An SDK is typically a set of software development tools that allows the creation of applications for a specific software package or framework, hardware platform, computer system, video game console, operating system, or similar development platform.

SSAE 16
The Statement on Standards for Attestation Engagements (SSAE) 16 is an auditing standard for service organizations, superseding SAS 70. The latter's "service auditor's examination" is replaced by a "Service Organization Controls" (SOC) report.

Storage Solution/Storage Appliance/Storage Vault
A storage solution, storage appliance, or storage vault enables an owner to store an electronic asset in a manner that assures the authenticity of the electronically signed document or agreement (for example) and the identity integrity of the signers. A vault or storage solution also enables a digital asset to be transferred in a manner that assures the integrity of the transfer.

Structured Threat Information Expression (STIX)
STIX is a standardized XML programming language for conveying data about cybersecurity threats in a common language that both humans and security technologies can easily understand.

Third-Party Security Assessment Program
A third-party security assessment program helps you fully understand the companies that supply services or goods to a particular business and the risks they may bring. Proper management also ensures exposure to risks are minimized and properly mitigated, regulatory requirements are met, enhanced controls are implemented, and suppliers are properly identified and risk rated.

Tokenized Data

Tokenization is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, which has no extrinsic or exploitable meaning or value.

TRUSTe
TRUSTe assesses, monitors, and certifies websites, mobile apps, cloud, and advertising channels so companies can safely collect and use customer data to power their business. The company incorporates regulatory requirements and industry best practices from the United States as well as North America, European Union, and Asia-Pacific regions.

Trusted Automated Exchange of Indicator Information (TAXII)
TAXII is a U.S. Department of Homeland Security-led effort of the office of Cyber security and Communications. It defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organizational, product line, and service boundaries. TAXII isn't an information sharing program itself and doesn't define trust agreements, governance, or other non-technical aspects of collaboration. Instead, TAXII empowers organizations to share the information they choose with the partners they choose.

U.S. ESIGN Act
The Electronic Signatures in Global and National Commerce (ESIGN) Act is a U.S. federal law that facilitates the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.

U.S.-Swiss Safe Harbor Framework
The U.S.-Swiss Safe Harbor framework bridges the differences in approach to privacy protection between the U.S. and Switzerland in order to provide a streamlined means for U.S. organizations to comply with the Swiss Federal Act on Data Protection.

Version Retention Objective (VRO)
The VRO incorporates how many copies of a given file or application data set will be maintained and how long that copy will be maintained. There may also be a requirement for how quickly that data needs to be retrieved and delivered to the requesting party.

Vulnerability Management
Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities, especially in software and firmware; and it's an integral component to computer and network security.

X.509 Public Key Infrastructure (PKI) Standard
In cryptography, X.509 is an important standard for a PKI to manage digital certificates and public-key encryption; and it's a key part of the Transport Layer Security protocol used to secure Web and email communication. An X.509 certificate verifies that a public key belongs to the user, computer, or service identity contained within the certificate.