Industry Best Practice

Data Security Reporting

Developed by

The SPARK Institute, Inc.
SHAPING AMERICA'S RETIREMENT

Release 2.0

August 30, 2022

The SPARK (Society of Professional Asset-managers & Record Keepers) Institute, through the work of its Data Security Oversight Board, developed the following standards to help record keepers communicate, to plan consultants, clients and prospects, the full capabilities of their cyber security systems. These standards are not intended to provide a recommended level of cyber protection or guarantee against a data breach or loss.

Record keepers need to maintain a level of confidentiality around the products and processes used to secure their clients data. Conversely, clients and prospects have legitimate needs to understand how their data is protected. So, the intent of these standards is to establish a base of communication between record keepers and the public through the use of independent third-party audits of cyber security control objectives. In this way vendors can properly validate the robust nature of their cyber security systems and still provide assurances to clients and prospects.

Industry Best Practice Data Security Reporting

1. SPARK recommends members use the 17 identified critical data security control objectives, defined by the Data Security Oversight Board (DSOB), when reporting on their overall data security capabilities. These control objectives are consistent with and aligned to the Department of Labor Cybersecurity Program Best Practices (April 2021) and satisfy the requirement for "Reliable Annual Third-Party Audit of Security Controls" as applied to recordkeepers.

2. When reporting cyber security capabilities SPARK's best practice requires members to use an established industry reporting format. These include the SOC 2, HiTrust certification, an Agreed Upon Procedures (following AICPA guidance), or ISO 27001 certification. All reporting must be done by an independent third-party auditor and address the SPARK 17 control objectives. Reporting that does not contain the SPARK control objectives must be amended to include these for it to be in compliance with the industry's best practice. Additional control objectives and security frameworks can be added in the future through analysis and approval of the DSOB.

3. Each reporting option must include a mapping between the identified controls and the 17 SPARK control objectives.

4. The audit scope is defined as anywhere customer/plan provided Non-Public Information (NPI) or Personally Identifiable Information (PII) is processed or stored.

Personal Identifiable Information (PII) is defined as:

Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.

Non-Public Information (NPI) is defined as:

Any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application);

Any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or Any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

5. The audit report must identify the primary applications and processing systems that support the services offered. The SPARK member may use Section III of the SOC 2 or the cover page of an AUP to address what systems are within the scope of the audit and which systems are not.

Within the detailed control objectives section of the report auditors must reference each specific control objective, the test procedures, and the testing results. Therefore, the format for the detailed control report should look as follows:

Format for Detailed Controls Report

Controls	Test Procedures	Results
Each control tested is defined and aligned to one of SPARK's 17 key areas of security focus	**TEST PARAMETERS** – Define what was tested and how test was performed	Summarize test results (i.e., No exceptions noted or Exception Noted and provide details)

6. SPARK's Data Security Oversight Board is a permanent ongoing authority, with the responsibility to regularly review these standards and when necessary, issue updates. When changes are voted on and approved these changes will go into effect no less than 6 months from the date of public announcement. Ongoing changes to the Industry Best Practices will be authorized by the DSOB, announced to the public and go into effect no less than 6 months from the publication date.

SPARK Data Security – Best Practices

Appendix

Required Focus of Control Objectives

	CONTROL OBJECTIVE	DESCRIPTION	SAMPLE CONTROLS (for illustrative purposes only, not intended to be a list of controls)
1	Risk Assessment and Treatment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	*Technology risk assessments are completed*
2	Security Policy	Organizational information security policy is established.	*Security policies are approved and communicated*
3	Corporate / Organizational Security	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	*A CISO or ISO has been assigned*
4	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	*IT application records are maintained in a formal system of record*
5	Human Resource Security	The organization's personnel and partners are suitable for the roles they are considered for, are provided cybersecurity awareness education and	*Personnel are subject to initial and periodic background checks*

	CONTROL OBJECTIVE	DESCRIPTION	SAMPLE CONTROLS (for illustrative purposes only, not intended to be a list of controls)
		are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	
6	Physical and Environmental Security	Physical access to assets is managed and protected	*Data centers are secured 24x7x365 with on-site physical security controls*
7	Communications and Operations Management	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	*Networks and systems include standard data security tools such as firewalls, antivirus, intrusion detection, and patch management.*
8	Access Control	Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	*Unique, complex passwords are assigned to all employees*
9	Information Systems Acquisition Development	A system development life cycle (SDLC) to manage systems is implemented; a vulnerability management plan is developed and implemented, and vulnerability scans are performed.	*Regular penetration tests are conducted on customer-facing applications*
10	Incident and Event Communications Management	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	*Cyber incident procedures are documented and routinely tested*
11	Operational / Business Resiliency	Response plans (Incident Response and Business Continuity) and recovery	*The organization maintains and tests BCP and DR plans*

	CONTROL OBJECTIVE	DESCRIPTION	SAMPLE CONTROLS (for illustrative purposes only, not intended to be a list of controls)
		plans (Incident Recovery and Disaster Recovery) are in place and managed	
12	Compliance	Legal requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	*Policies and procedures are in place to enforce applicable privacy obligations*
13	Mobile	A formal policy shall be in place and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.	*A mobile policy is approved and enforced*
14	Encryption	Data-at-rest is protected, and Data-in-transit is protected.	*External transmissions are encrypted using FIPS approved algorithms*
15	Supplier Risk	Ensure protection of the organization's assets that is accessible by suppliers	*Suppliers are subject to periodic security reviews*
16	Cloud Security	Ensure protection of the organization's assets that are stored or processed in cloud environments	*Cloud providers are subject to periodic security reviews or can provide independent security assessments of their environment*
17	Ransomware	Processes and controls are in place to detect and respond to ransomware event	*Policies and procedures are in place for the detection, prevention and response to the risk posed by a ransomware event*

Key Terms and Definitions:

- A Service Organization Controls, SOC 2 ® report, provides independent examination, validation, and assurance of controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy controls based on compliance developed by the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria. [1] When the DOL's cybersecurity best practices state to have a reliable annual third-party audit of security controls, this is what a SOC 2 ® report provides.[2]
- HITRUST CSF is a certifiable framework that provides organizations globally a comprehensive, flexible, and efficient approach to regulatory/standards compliance and risk management.[3]
- AUP - An Agreed-Upon Procedures engagement is an attestation engagement in which a practitioner performs specific procedures on subject matter and reports the findings without providing an opinion or conclusion. [4]
- ISO certification can be a useful tool to add credibility, by demonstrating that your product or services meets the expectations of your customers. Certification – the provision by an independent body of written assurance (a certificate) that the product, service, or system in question meets specific requirements. Accreditation – the formal recognition by an independent body, generally known as an accreditation body, that a certification body operates according to international standards.[5]
- Controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. In the field of information security, such controls protect the confidentiality, integrity and availability of information.[6]

Key Links:

- SPARK Institute | Leading Voice for Retirement Plan Industry
- Retirement Plan Best Practices | Industry Standards Retirement | Retirement Plan Regulation & Security | SPARK Institute
- Cybersecurity & Fraud Resources - SPARK Institute

[1] AICPA.org website: SOC for Service Organizations (aicpa.org)
[2] DOL.gov Cybersecurity Tips for Hiring a Service Provider with strong security practices
[3] HITRUST alliance.net Product Tool/HITRUST CSF
[4] https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-19.pdf
[5] ISO.org "Certification"
[6] Security controls - Wikipedia

Document History and Signoff

The following table lists the previous and current revisions to this document in chronological order. For each revision one or more contributors is listed and the changes to the document briefly described.

DOCUMENT HISTORY

Version	Author	Description of Changes
2017.1 (09/27/2017)	SPARK authors	Document organization
2022.1 (08/30/22)	SPARK DSOB DSOB - SPARK Institute	Added: - One new control objective for Ransomware (#17) - Key terms and definitions section - Key Links section - Document history table including a next planned document review / update. Updated: - General rewrites of items within document Changes: - Removal of the SPARK Data Security example alternative reporting scenarios
2023.1 (09/01/2023)	Next Scheduled Review Date	

DOCUMENT SIGNOFF

Approver	Date
SPARK DSOB	August 30, 2022