Industry Best Practice

Data Security Reporting

Developed by

The SPARK Institute, Inc.
SHAPING AMERICA'S RETIREMENT

Release 1.0

September 20, 2017

The Spark 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 secrecy 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 16 identified critical data security control objectives, defined by the Data Security Oversight Board (DSOB), when reporting on their overall data security capabilities

2. When reporting cyber security capabilities SPARK's best practice requires members to use one of the following approved reporting alternatives. All reporting must be done by an independent third-party auditor and address the SPARK 16 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.

SPARK Data Security

Example Alternative Reporting Scenarios

Reporting Options	NIST	ISO	HiTrust	Custom Framework	Other Frameworks
SOC2	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable
HiTrust Certification	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable
AUP	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable
ISO Certification	N/A	Acceptable[1]	N/A	N/A	N/A

1) If accompanied by a detailed control mapping report that aligns to SPARK's 16 control objectives and attested to by independent third party auditor.

3. Each reporting alternative and framework must include a detailed report showing identified controls mapped appropriately to SPARK's 16 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 SOC2 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 16 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. So, within the first six months from the date of enactment of these new industry best practices the audit scope, the control objectives and appropriate frameworks will be reviewed. If changes are voted on and approved changes will be go into effect no less than 6 months from the date of public announcement. Following the first year of implementation audit scope, control objectives and appropriate frameworks will be reviewed annually and updated as appropriate. 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	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	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*