



SPARK INSTITUTE
SHAPING AMERICA'S RETIREMENT

PLAN SPONSOR & ADVISOR GUIDE TO CYBERSECURITY

SPARK Data Security Best Practices: Seventeen Control Objectives

October 2022

STRENGTHENING RETIREMENT INDUSTRY CYBERSECURITY



The threat of retirement account take-overs and fraud is on the rise — and will only increase — as criminals actively target retirement savings. At The SPARK Institute, we have long advocated for greater awareness of cyber risks and for controls that can better protect retirement assets against criminal cyber activity, led by the work of our Data Security Oversight Board (DSOB).

The latest milestone in our ongoing effort to strengthen cybersecurity throughout the retirement industry is the set of seventeen Control Objectives to help recordkeepers communicate the full capabilities of their cybersecurity systems to plan consultants, clients and prospects.

The intent of these standards is to establish a base of communication between recordkeepers and the public through third-party audits of cybersecurity Control Objectives. They are not intended to provide a recommended level of cyber protection or a guarantee against a data breach or loss.

These Control Objectives are consistent with and in alignment with the Department of Labor Cybersecurity Program Best Practices (April 2021) and satisfy the requirement for “Reliable Annual Third-Party Audit of Security Controls” for recordkeepers.

IMPORTANT DEFINITIONS



To better inform plan sponsors and participants of events that impact the security of their data — and to develop a standard for the recordkeeping industry in the absence of commonly accepted industry definitions — SPARK Institute also developed the industry best practices to define security breaches and cyber fraud.

These definitions do not supersede state and/or federal laws, but establish a base of communication between recordkeepers and plan sponsors. Using these terms, plan sponsors can assess a recordkeeper’s cybersecurity incident practice and controls more accurately and, together with the recordkeeper, develop mutually agreed-upon contractual protections.

Security Breaches



A security breach is a confirmed compromise of an information system within the authority or responsibility of the recordkeeper that results in:

1. The unauthorized acquisition, disclosure, modification or use of unencrypted personal data or encrypted personal data where the encryption key has also been compromised.
2. A likely risk of identity theft or fraud against the data subject. A good faith but unauthorized or unintentional acquisition, disclosure, modification or use of personal data by an employee or contractor of the recordkeeper or a party who has signed a confidentiality agreement with the recordkeeper does not constitute a security breach if the personal data is not subject to further unauthorized acquisition, disclosure, loss, modification, or use.

A few typical examples of security breaches are:

- **Attack** - A successful attack on a recordkeeper's network or information system that results in unauthorized acquisition of participant records.
- **Intrusion** - An intrusion into a recordkeeper's external cloud account that results in the attacker acquiring unencrypted personal data.
- **Lost unencrypted laptop** - The loss of an unencrypted laptop that stores personal data when it is likely that the loss may result in identity theft or fraud.
- **Data file loss** - A data file provided by the recordkeeper to a third party who has not signed a data confidentiality agreement when it is likely that the loss may result in identity theft or fraud.



Cyber Fraud











Cyber fraud is a confirmed compromise of a participant's financial account. The fraudster gains possession or control of the participant's personal information that results in wrongful financial or personal gain or illegal access to the account.

Some typical examples of cyber fraud include:

- **Phishing** - A participant discloses their account username and password via a phishing email link. The fraudster uses these credentials to compromise the participant's online account and withdraw money from it.
- **Malware** - Keystroke logging malware captures a participant's credentials and results in the compromise of the participant's online account
- **Account takeover** - An attacker successfully takes over a participant's account and changes other participant information and/or attempts to transfer money.
- **Compromised third-party aggregation technology** - An attacker successfully gains access to a participant's account through the compromise of a third-party account aggregation technology.
- **Impersonation** - An attacker gains access to a participant's account by successfully impersonating the participant via the recordkeeper's call center.










SPARK'S SEVENTEEN CONTROL OBJECTIVES

SPARK advises member firms to have service providers and their auditors summarize and document their reports according to these Control Objectives.

CONTROL OBJECTIVE	THE ORGANIZATION HAS:	SAMPLE CONTROLS
 1 Risk Assessment and Treatment	An understanding of the cybersecurity risk to operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Completed technology risk assessments.
 2 Security Policy	Established organizational information security policy.	Approved and communicated security policies.
 3 Organizational Security	Established coordinated information security roles and responsibilities that align with internal roles and external partners.	Assigned Chief Information Security Officer or Information Security Officer.
 4 Asset Management	Identified the data, personnel, devices, systems, and facilities to achieve business purposes and manages them consistent with their relative importance to business objectives and risk strategy.	Maintained IT application in a formal system of record.
 5 Human Resource Security	Ensured its personnel and partners are suitable for the roles they are considered for, provides them with cybersecurity awareness education, and trains them to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	Initial and periodic background checks for personnel.
 6 Physical & Environmental Security	Protected physical access to assets and provides ongoing management.	24x7x365 secured data centers with on-site physical security controls.
 7 Communications & Operations Management	Ensured that technical security solutions are managed to protect 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	Limited access to assets and associated facilities to authorized users, processes, or devices, and to authorized activities and transactions.	Unique, complex passwords assigned to all employees.

SPARK'S SEVENTEEN CONTROL OBJECTIVES

SPARK advises member firms to have service providers and their auditors summarize and document their reports according to these Control Objectives.

CONTROL OBJECTIVE	THE ORGANIZATION HAS:	SAMPLE CONTROLS
 9 Information Systems Acquisition Development	Implemented a system development life cycle to manage systems; developed and implemented a vulnerability management plan; performs vulnerability scans.	Conducting regular penetration tests on customer- facing applications.
 10 Incident & Event Communications Management	Executed response processes and procedures and maintains them to ensure timely response to detected cybersecurity events.	Documented and routinely tested cyber incident procedures.
 11 Business Resiliency	Established regularly managed incident response, business continuity, and incident recovery and disaster recovery plans.	Tested and maintained business continuity and disaster recovery plans.
 12 Compliance	Ensured the understanding and management of legal requirements regarding cybersecurity, including privacy and civil liberties obligations.	Established policies and procedures to enforce applicable privacy obligations.
 13 Mobile	Adopted a formal policy and security measures to protect against the risks of using mobile computing and communication facilities.	Approval and enforcement of a mobile policy.
 14 Encryption	Ensured the protection of both data-at-rest and data-in-transit.	Encrypted external transmissions using Federal Information Processing Standard-approved algorithms.
 15 Supplier Risk	Ensured protection of the organization's assets that are accessible by suppliers.	Periodic security reviews of suppliers.
 16 Cloud Security	Ensured protection of assets stored or processed in cloud environments.	Periodic security reviews or independent security assessments of cloud providers.
 17 Ransomware	Processes and controls in place to detect and respond to a ransomware events.	Established policies and procedures for the detection, prevention and response to the risk posed by a ransomware event.

DOCUMENTATION & INDEPENDENT AUDITING



1. SPARK recommends members use the seventeen Control Objectives when reporting on their overall data security capabilities.

2. SPARK's best practices require members to use an established industry reporting format, including any one of these options:

- SOC 2
- HiTrust certification
- Agreed-Upon Procedures (following the Association of International Certified Professional Accountants guidance)
- ISO certification

An independent third-party auditor must do all reporting and address the seventeen Control Objectives.

3. Each reporting option must include a mapping between the identified controls and the seventeen 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. Here are summary definitions of NPI and PII:

- NPI is any information an individual provides to your firm to obtain a financial product or service (for example, name, address, income, Social Security number, or other information on an application). NPI also includes any information your firm receives about an individual resulting from a transaction involving your financial products or services (such as name, address, client relationship) and any information you get about an individual in connection with providing a financial product or service (such as information from court records or credit reports).

- PII is any representation of information that enables the identity of an individual to be reasonably inferred by either direct or indirect means. PII also includes any information that directly or indirectly identifies an individual through a combination of data elements such as gender, race, birthdate, or geographic location. In addition, information permitting the physical or online contact to a specific individual is the same as PII.

PII can be maintained in either paper, electronic or other media.

Documentation & Independent Auditing

5. The audit report must identify the primary applications and processing systems that support the services offered. SPARK members may use Section III of the SOC 2 or the cover page of Agreed Upon Procedures 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, using this format to document results:

FORMAT FOR DETAILED CONTROLS REPORT

SPARK CONTROL OBJECTIVES	TEST PROCEDURES	RESULTS/CRITERIA
Define, align and test each control based on SPARK's seventeen Control Objectives.	Define what was tested and how each test was performed.	Summarize test results (no exceptions, or exceptions noted with details provided).

NEXT STEPS

When reviewing or selecting a recordkeeper, plan sponsors and advisors should first request a copy of their SPARK cybersecurity reports for each of the seventeen Control Objectives. The data provided in these reports should be the basis for your evaluation of a service provider's cybersecurity capabilities.

The SPARK Institute also provides extensive cybersecurity information on its [website](https://www.sparkinstitute.org/resources/cybersecurity-and-fraud-resources/). [https://www.sparkinstitute.org/resources/cybersecurity-and-fraud-resources/], including SPARK Data Security Industry Best Practice Standards Version 2022.11 (August 30, 2022), which contains more complete information.



SPARK INSTITUTE
SHAPING AMERICA'S RETIREMENT

ABOUT THE SPARK INSTITUTE

The SPARK Institute, Inc. is a member-driven, non-profit organization and leading voice in Washington, DC for the retirement industry. SPARK helps shape national retirement policy by developing and advancing positions on critical issues that affect plan sponsors, participants, service providers, and investment providers. Collectively, SPARK Institute's members serve approximately 100 million participants in 401(k) and other defined contribution plans.