Crowe Horwath.

Smart decisions. Lasting value.™

Cybersecurity and SOC Reports

What you need to know

Sean Katzenberger, CISA

Principal (Partner)

Risk Consulting

Crowe Horwath LLP

Agenda

- Cybersecurity definition
- 2016 Breach Statistics
- Common Breach Vectors
- Service Organization Reports (SOC) Overview
- Questions

Simplest Definition of Cybersecurity

- “Measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack”*

- Regardless of the definition, cybersecurity objectives still continue to b
  - The triad of security – CIA of “CRITICAL DATA”
    - Confidentiality
    - Integrity
    - Availability

  - Who does it impact?
    - Anyone, individual or organization, connected to a network or the internet

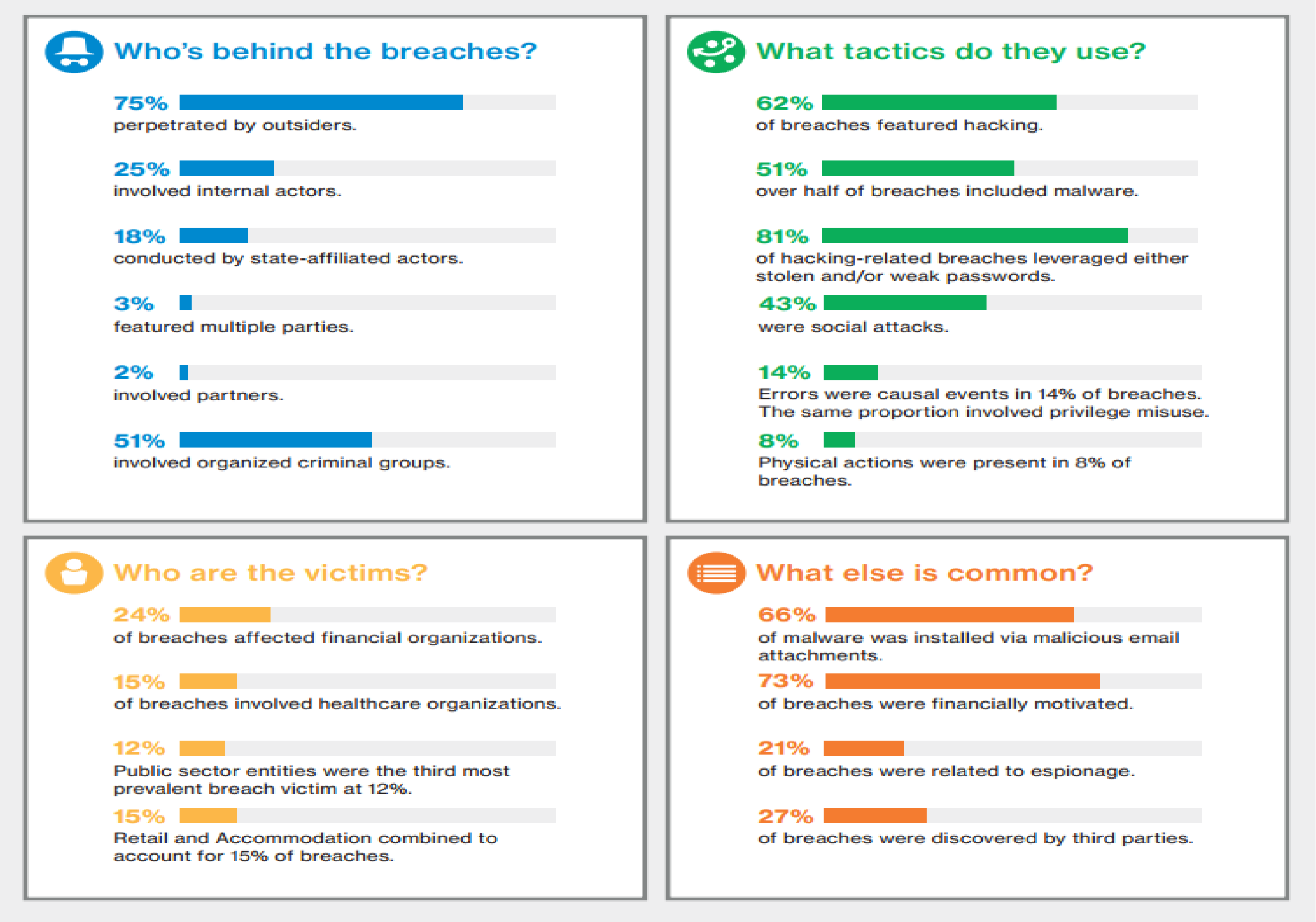
* Source: Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/cybersecurity

2016 Breach Statistics Summary

- Information gathered from the Executive Summary of the Verizon 2017 Data Breach Investigations Report (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/)

Key Points

- **81%** of hacking-related breaches leveraged either stolen and/or weak passwords
- **66%** of malware was installed via malicious email attachments
- **61%** of data breach victims in 2017 report were businesses with under 1,000 employees.



Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.

21% of breaches were related to espionage.

27% of breaches were discovered by third parties.

2016 Breach Statistics Summary

- Stolen/re-used credentials
- Viruses/Malware
- More than 80% of breaches "have a root cause in employee negligence"
  - Misconfiguration/Default Configuration
  - Lack of Patching
  - Weak Passwords
  - Social Engineering

- Awareness Training is Key!

2016 Breach Statistics Summary

- Sometimes, employees don’t understand the risks:
  - “**One-third** of employees say they break IT policies because they don’t believe they’re doing anything wrong when doing so.”*
  - “**61%** say its up to IT staff, not them, to safeguard information and devices”*

- What are the big risks?
  - Phishing
  - Email
  - Social engineering
  - Drive-by attacks
  - Access to third parties

* Source: Don Reisinger, “Younger Workers Pose Big Security Risks,” Baseline, Dec. 21, 2011, http://www.baselinemag.com/c/a/Security/Younger-Workers-Pose-Big-Security-Risks-888439/

2016 Breach Statistics Summary

- The Ponemon Institute's study called *U.S. Cost of a Data Breach* found that **42** percent of breaches (as identified from survey respondents) were caused by a third-party vendor.
    - Source: http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf
- Most organizations don't have a comprehensive list of the vendors they share data with.
  - Lines of business have the ability to engage vendors with little to no involvement of security personnel.
- Organizations perform minimal oversight of vendors' control environments.

Common Cybersecurity Risks

- The top cybersecurity risk areas in our experience

Key Risk Areas	Risk Examples	Comments
Security Governance	Phishing / Social Engineering Shadow IT (mobile, personal cloud)	Organizations have been providing training for a while. However employees continue to be the weakest link to security. Organizations must find solutions to **make security part of the organization's culture**, empowering employees to understand and manage the risks independently.
Change Management	Patch Management Unsecured deployments	Vulnerabilities are identified regularly, and with the proliferation of technologies and applications, organizations are unable to keep these technologies up to date. In addition, there is a continue struggle between innovation and security. Employees are still incentivized by meeting deadlines and staying on budget, with minimal security expectations. Organizations need to set the right tone as it relates to security, including providing the right incentives to employees to manage critical risk effectively.
Third Parties	Data Protection Denial of Service	Organization's reliance on third parties has increased significantly, providing them more access than ever to sensitive data, and increasing the criticality third party solutions play in day to day operations. Organizations need to develop programs around identification and management of critical vendors commensurate with their potential impact on the business.

Common Cybersecurity Risks

Key Risk Areas	Risk Examples	Comments
Incident Response	Inappropriate response during an incident	As public awareness of breaches and their impact continue to rise, potential impacts on companies are also increasing. Organizational perspectives are shifting from incident avoidance to breach mitigation. However, organizations fail to properly plan their response when an incident does occur. Organizations need to clearly define and test incident response procedures that triage, respond, and remediate incidents when they occur.
Balance	Improper balance between security risk and business risk	Organizations continue to struggle to find the right balance between innovation and security, often taking reactionary approaches to prioritizing strategies. With the heightened sensitivity to breaches, organizations may over correct and emphasize security to a point that other business goals are negatively impacted. Organization's need to establish programs to proactively identify and manage risks to levels acceptable to the organization.

Service Organization Controls (SOC) Reports – Overview

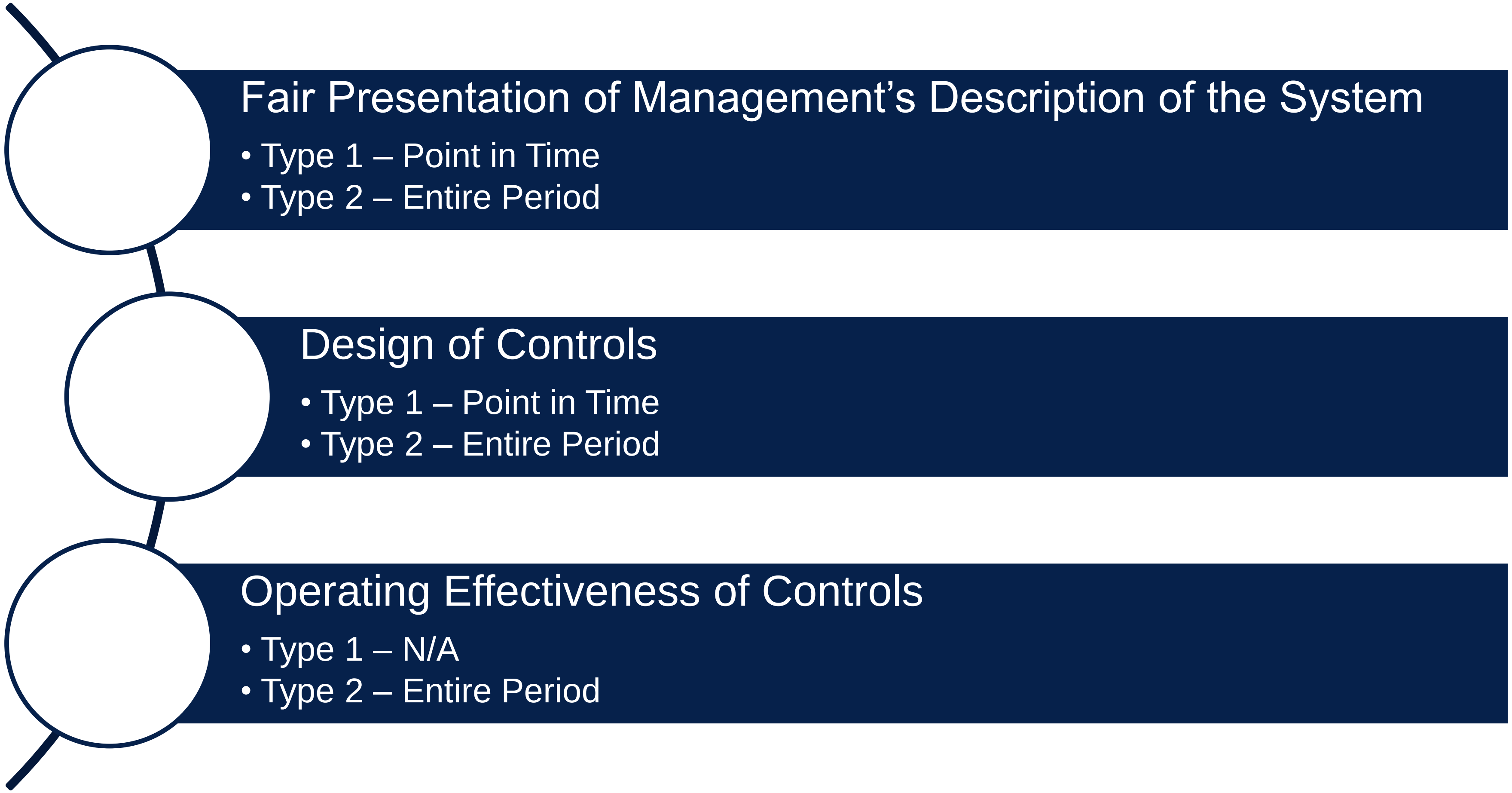
- AICPA created separate reports on internal controls over financial reporting and reports on other types of controls.

- The AICPA has added additional reporting options.
  - The three reporting options now are:
    - SOC 1
    - SOC 2

Types of SOC Reports

Report	Report's focus	Audience
SOC 1	Report on internal controls over financial reporting	Restricted Use
SOC 2	Report on controls related to Security, Availability, Processing Integrity, Confidentiality and/or Privacy (Trust Services Principles)	Restricted Use

Key Point – Type 1 vs. Type 2



Fair Presentation of Management’s Description of the System

- Type 1 – Point in Time
- Type 2 – Entire Period

Design of Controls

- Type 1 – Point in Time
- Type 2 – Entire Period

Operating Effectiveness of Controls

- Type 1 – N/A
- Type 2 – Entire Period

Introduction of SSAE 18 / SOC 1

- All SOC 1 reports **dated on or after May 1, 2017** will be performed under the new SSAE 18 standard that will replace the SSAE 16 standard.

- The AICPA completed the Clarity Project for Attestation standards with the issuance of SSAE 18 (Statement on Standards for Attestation Engagements (SSAE) No. 18, Attestation Standards: Clarification and Recodification). The Clarity Project was established in an effort to make standards easier to read and understand. Further the project focus was to eliminate the same paragraphs (with slight differences) in multiple standards and to conform with the recodification of financial audit standards.

- The SSAE 18 AT-C Section 320 supersedes the SSAE 16 Standard, therefore we will no longer refer to SOC 1 reports as SSAE 16 reports.

- SSAE 18 also impacts other attestation standards (AT101, AT201). For example, the prior AT101 standard was replaced by SSAE 18 Section AT-C 105, 205 and 210 and the prior AT801 standard (SSAE 16) was replaced to SSAE 18 Section AT-C 320.

SSAE 18 – New Requirements for Service Organizations

- SSAE 18 AT-C Section 320 requires additional monitoring of subservice organizations. Monitoring procedures could include:
  - reviewing and reconciling output reports,
  - holding periodic discussions with the subservice organization
  - making regular site visits to the subservice organization,
  - testing controls at the subservice organization by members of the service organization's internal audit function,
  - reviewing SOC reports on the subservice organization's system and
  - monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

- Management's description of systems is required to include a description of their vendor management procedures.

- The scope the service auditor's testing is required to contain information regarding the monitoring of subservice organizations (i.e. addition of a control objective).

SOC 2 - Trust Services Principles

Security – The system is protected against unauthorized access, use, or modification to meet the entity’s commitments and system requirements.

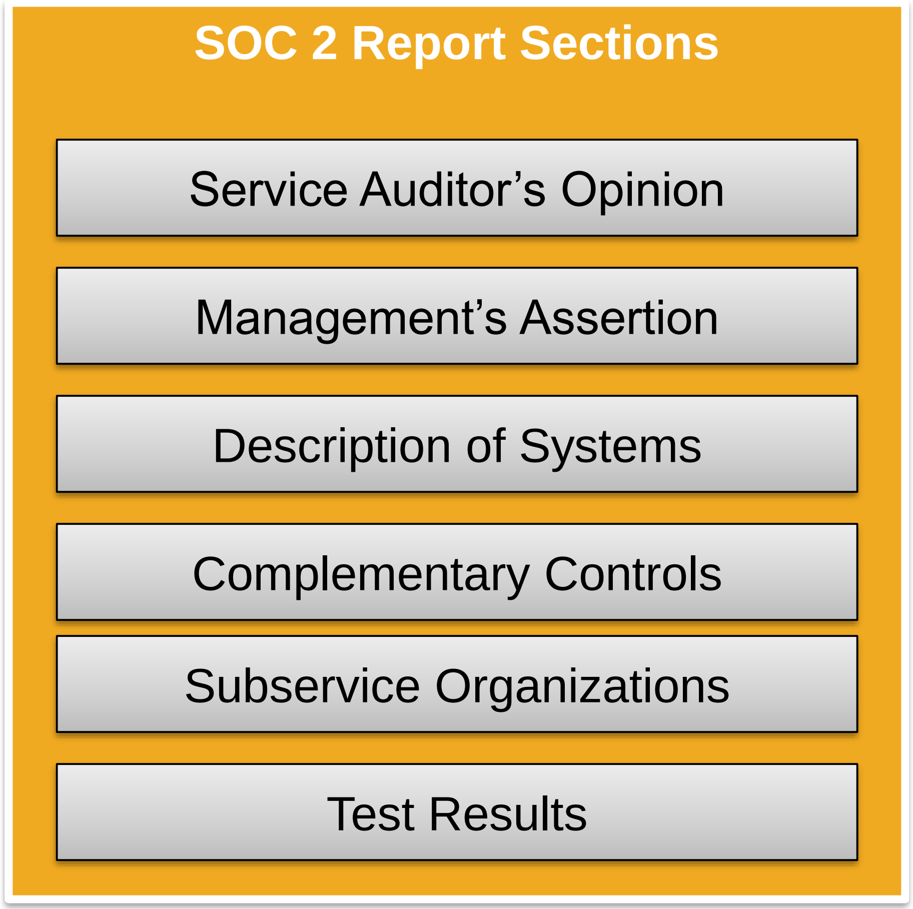
Availability – The system is available for operation and use to meet the entity’s commitments and system requirements.

Processing Integrity – System processing is complete, valid, accurate, timely, and authorized to meet the entity’s commitments and system requirements.

Confidentiality – Information designated as confidential is protected to meet the entity’s commitments and system requirements.

Privacy – Personal information is collected, used, retained, disclosed and disposed to meet the entity’s commitments and system requirements.

SOC Report Sections



SOC 2 Report Sections

- Service Auditor’s Opinion
- Management’s Assertion
- Description of Systems
- Complementary Controls
- Subservice Organizations
- Test Results

SOC Report Sections

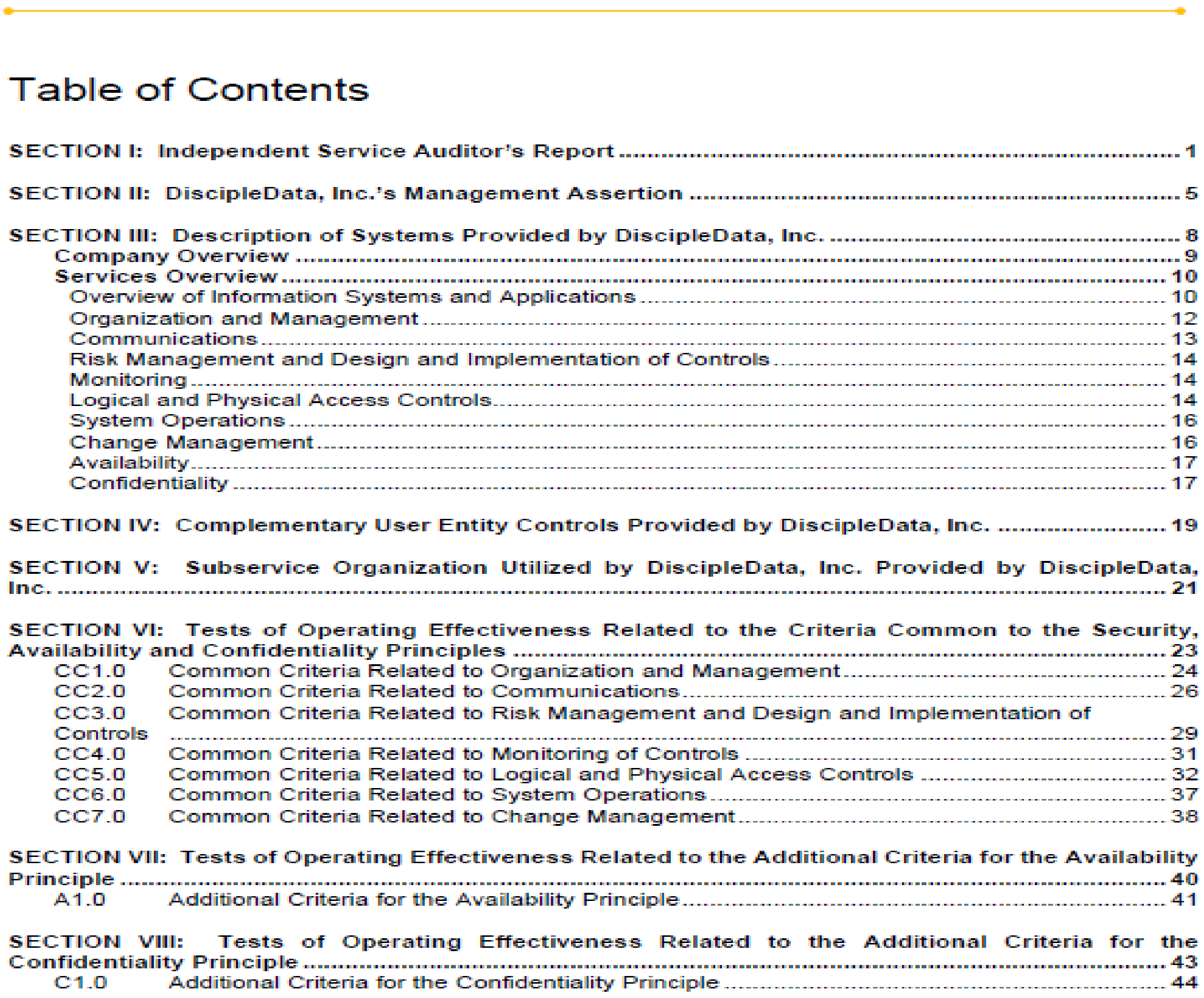
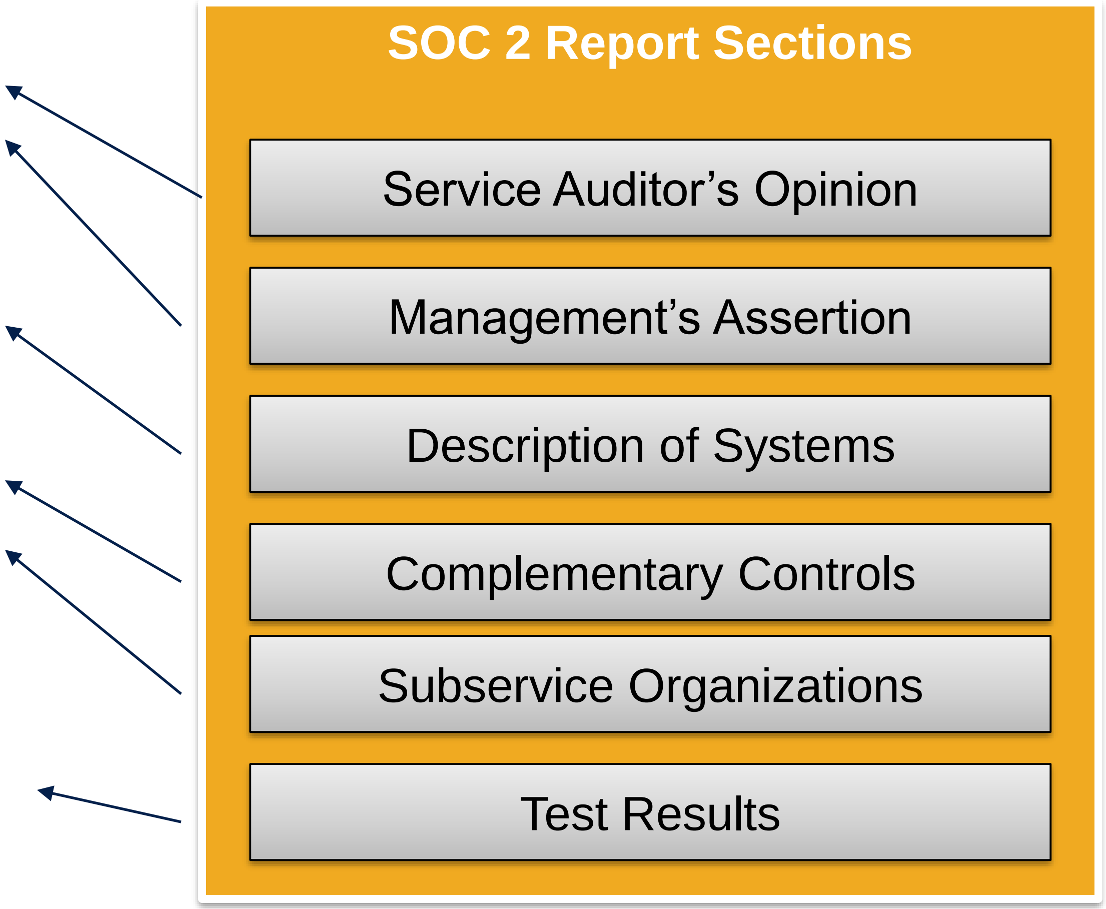


Table of Contents

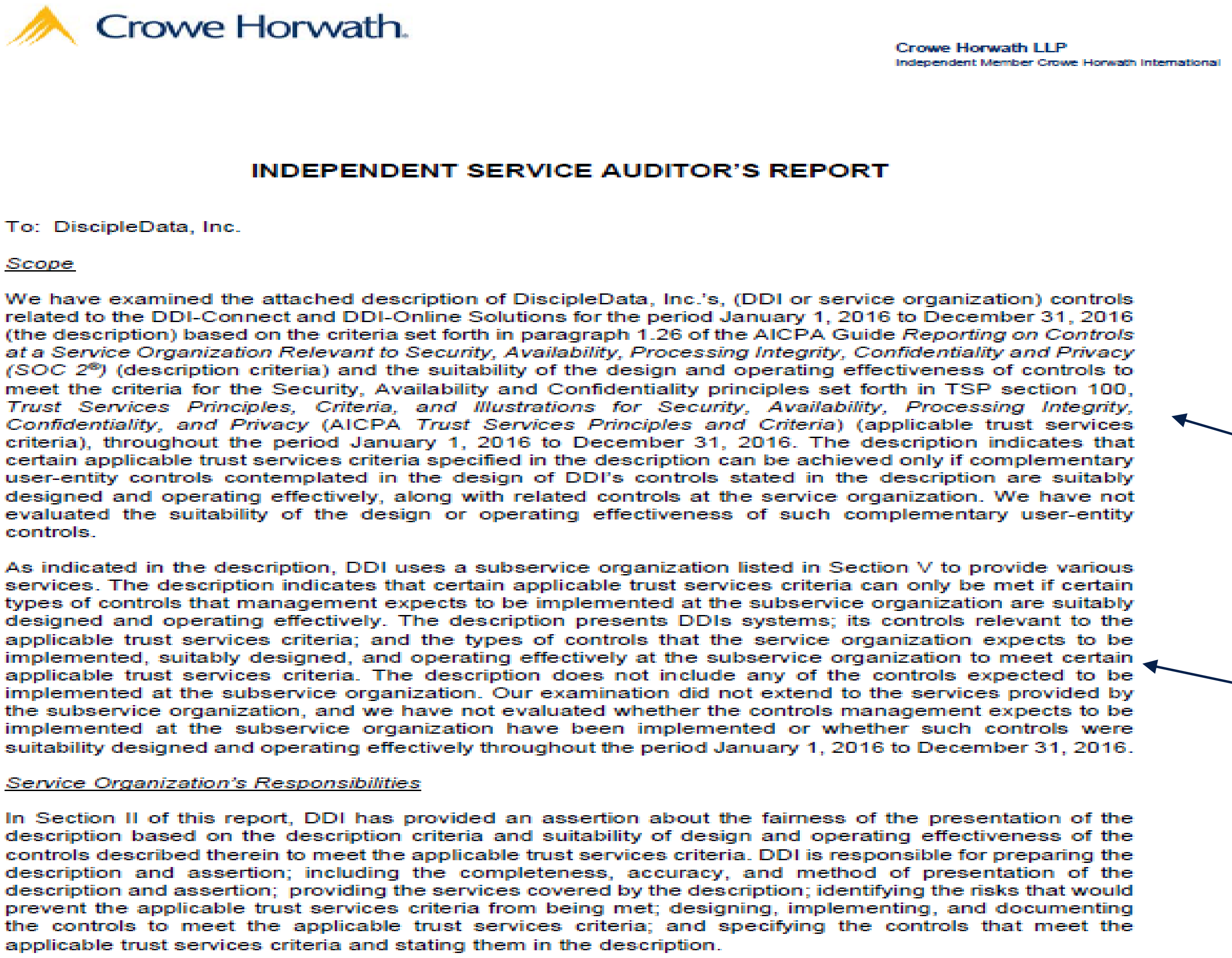


SOC 2 Report Sections

- Service Auditor's Opinion
- Management's Assertion
- Description of Systems
- Complementary Controls
- Subservice Organizations
- Test Results

Section I: Service Auditor's Opinion

- Service Auditor's Opinion
- Management Assertion
- Description of Systems
- Complementary Controls
- Subservice Organization
- Test results



Crowe Horwath.

Crowe Horwath LLP
Independent Member Crowe Horwath International

INDEPENDENT SERVICE AUDITOR'S REPORT

To: DiscipleData, Inc.

Scope

We have examined the attached description of DiscipleData, Inc.'s, (DDI or service organization) controls related to the DDI-Connect and DDI-Online Solutions for the period January 1, 2016 to December 31, 2016 (the description) based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy (SOC 2®)* (description criteria) and the suitability of the design and operating effectiveness of controls to meet the criteria for the Security, Availability and Confidentiality principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA *Trust Services Principles and Criteria*) (applicable trust services criteria), throughout the period January 1, 2016 to December 31, 2016. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of DDI's controls stated in the description are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

As indicated in the description, DDI uses a subservice organization listed in Section V to provide various services. The description indicates that certain applicable trust services criteria can only be met if certain types of controls that management expects to be implemented at the subservice organization are suitably designed and operating effectively. The description presents DDIs systems; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization, and we have not evaluated whether the controls management expects to be implemented at the subservice organization have been implemented or whether such controls were suitability designed and operating effectively throughout the period January 1, 2016 to December 31, 2016.

Service Organization's Responsibilities

In Section II of this report, DDI has provided an assertion about the fairness of the presentation of the description based on the description criteria and suitability of design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. DDI is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

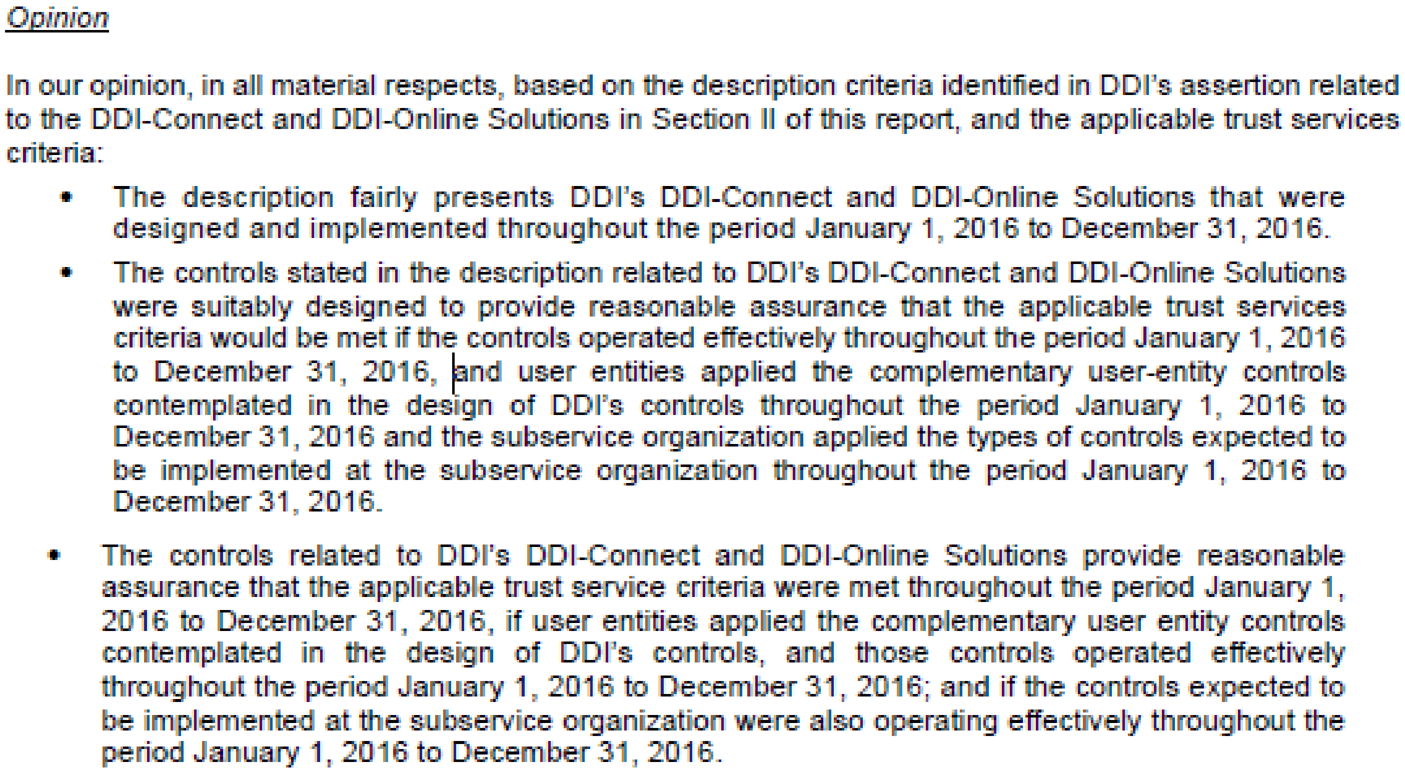
What to Review

1. **Scope Paragraph** – Systems, Trust Principles (e.g. Security), Time Period, etc…

2. **Subservice Organization Carve-out** - Consider: how important / significant / material are the services provided by the sub-servicer? If your service organization is contracting out critical or sensitive pieces of their control environment to a third-party, you may want to request the third party's SOC report as well.

Section I: Service Auditor’s Opinion, Cont.

- Service Auditor’s Opinion
- Management Assertion
- Description of Systems
- Complementary Controls
- Subservice Organization
- Test results



Opinion

In our opinion, in all material respects, based on the description criteria identified in DDI’s assertion related to the DDI-Connect and DDI-Online Solutions in Section II of this report, and the applicable trust services criteria:

- The description fairly presents DDI’s DDI-Connect and DDI-Online Solutions that were designed and implemented throughout the period January 1, 2016 to December 31, 2016.
- The controls stated in the description related to DDI’s DDI-Connect and DDI-Online Solutions were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period January 1, 2016 to December 31, 2016, and user entities applied the complementary user-entity controls contemplated in the design of DDI’s controls throughout the period January 1, 2016 to December 31, 2016 and the subservice organization applied the types of controls expected to be implemented at the subservice organization throughout the period January 1, 2016 to December 31, 2016.
- The controls related to DDI’s DDI-Connect and DDI-Online Solutions provide reasonable assurance that the applicable trust service criteria were met throughout the period January 1, 2016 to December 31, 2016, if user entities applied the complementary user entity controls contemplated in the design of DDI’s controls, and those controls operated effectively throughout the period January 1, 2016 to December 31, 2016; and if the controls expected to be implemented at the subservice organization were also operating effectively throughout the period January 1, 2016 to December 31, 2016.

What to Review

1. **Opinion -** Unqualified Opinion
   a) Description
   b) Design
   c) Operating Effectiveness

Section II: Management's Assertion

Service Auditor's Opinion

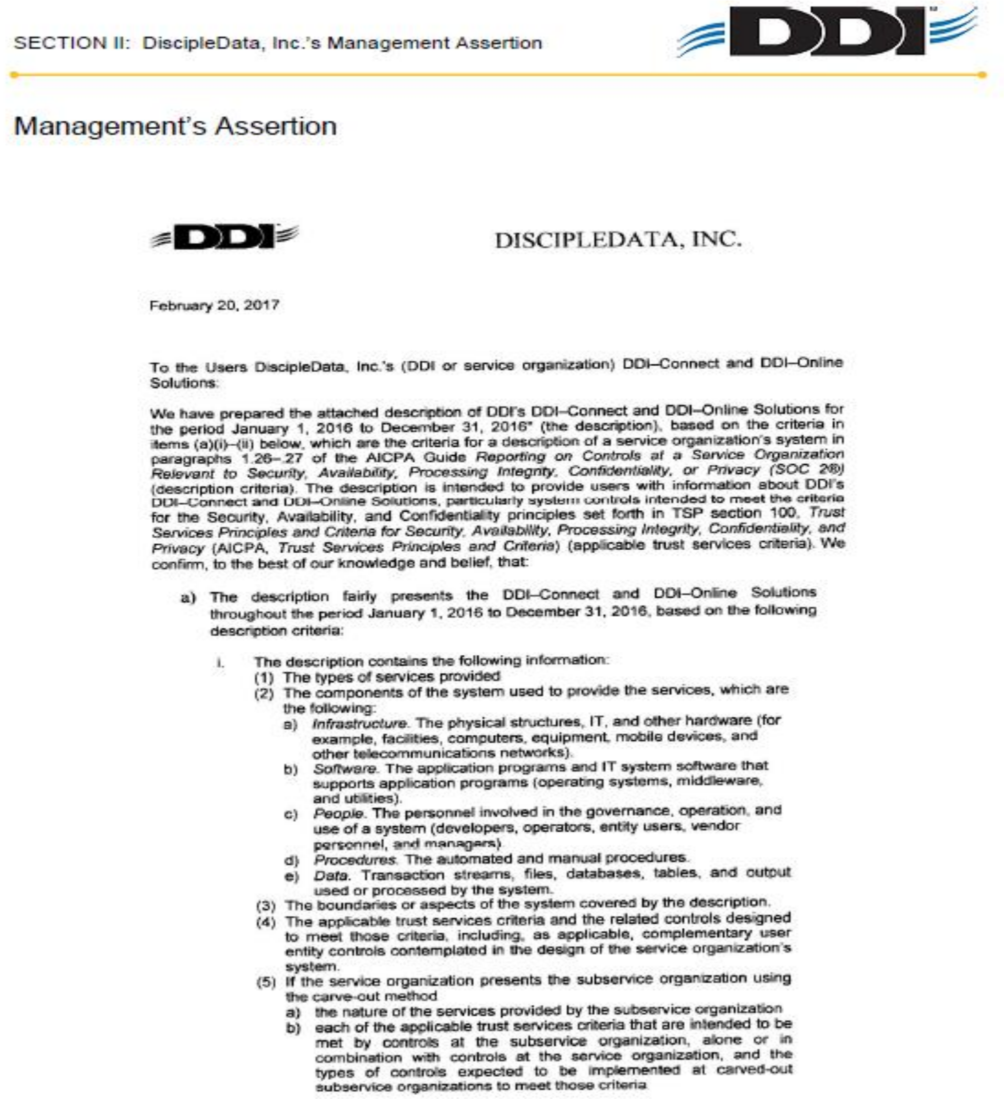
Management Assertion

Description of Systems

Complementary Controls

Subservice Organization

Test results



SECTION II: DiscipleData, Inc.'s Management Assertion

Management's Assertion

DISCIPLEDATA, INC.

February 20, 2017

To the Users DiscipleData, Inc.'s (DDI or service organization) DDI–Connect and DDI–Online Solutions:

We have prepared the attached description of DDI's DDI–Connect and DDI–Online Solutions for the period January 1, 2016 to December 31, 2016" (the description), based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.26–.27 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria). The description is intended to provide users with information about DDI's DDI–Connect and DDI–Online Solutions, particularly system controls intended to meet the criteria for the Security, Availability, and Confidentiality principles set forth in TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

a) The description fairly presents the DDI–Connect and DDI–Online Solutions throughout the period January 1, 2016 to December 31, 2016, based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided

(2) The components of the system used to provide the services, which are the following:

a) *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).

b) *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).

c) *People*. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers)

d) *Procedures*. The automated and manual procedures.

e) *Data*. Transaction streams, files, databases, tables, and output used or processed by the system.

(3) The boundaries or aspects of the system covered by the description.

(4) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user entity controls contemplated in the design of the service organization's system.

(5) If the service organization presents the subservice organization using the carve-out method

a) the nature of the services provided by the subservice organization

b) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria

Key Points

1. Management must have a "reasonable basis" for its assertion. This typically means that management must perform some procedures to asses the adequacy of the description.

2. Management's responsibilities:
   Fair Presentation (of the description)
   Suitability of Design
   Operating Effectiveness (Type 2 only)

Section III: Description of Systems

Service Auditor’s Opinion

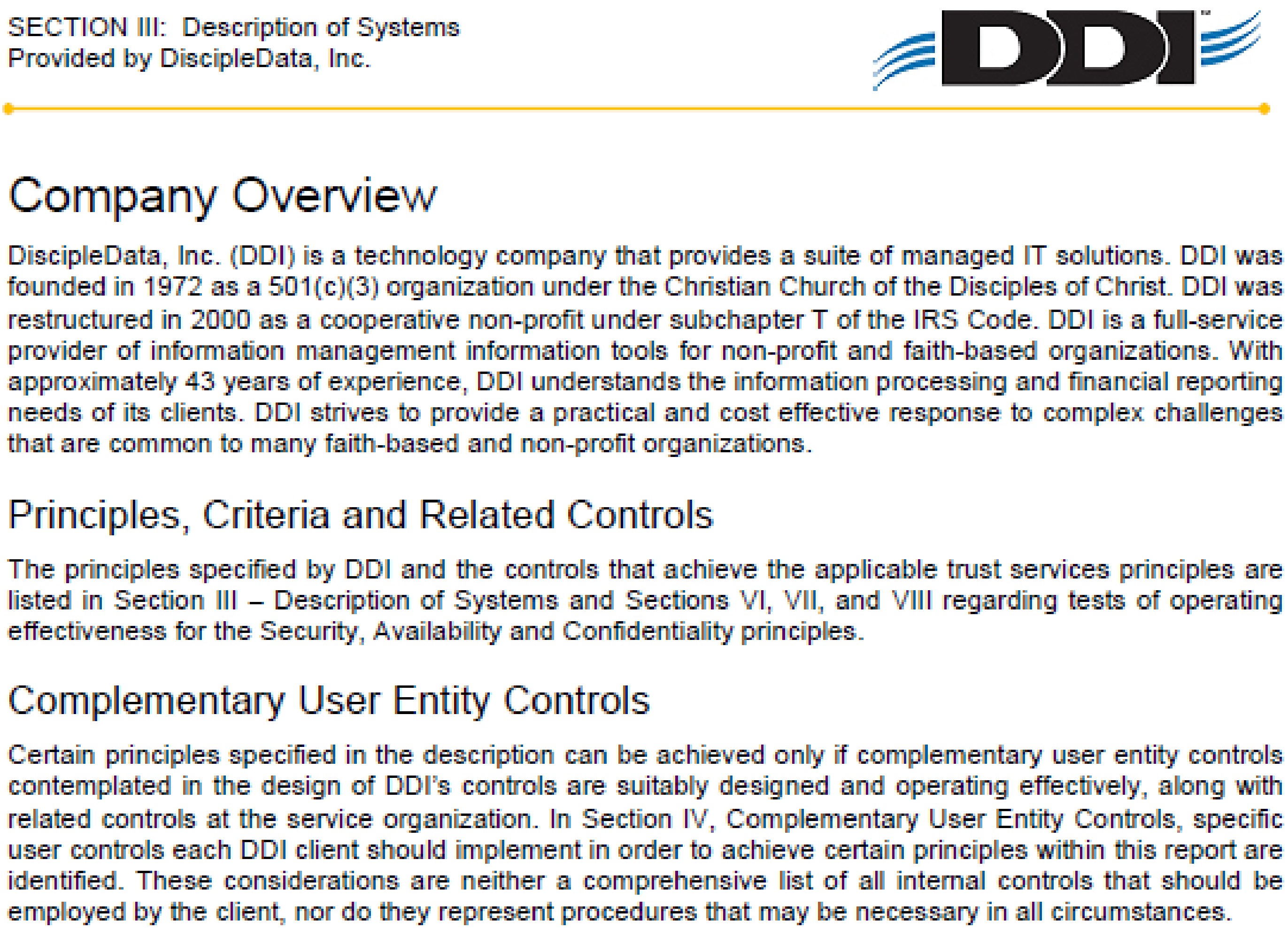
Management Assertion

Description of Systems

Complementary Controls

Subservice Organization

Test results



SECTION III: Description of Systems
Provided by DiscipleData, Inc.

Company Overview

DiscipleData, Inc. (DDI) is a technology company that provides a suite of managed IT solutions. DDI was founded in 1972 as a 501(c)(3) organization under the Christian Church of the Disciples of Christ. DDI was restructured in 2000 as a cooperative non-profit under subchapter T of the IRS Code. DDI is a full-service provider of information management information tools for non-profit and faith-based organizations. With approximately 43 years of experience, DDI understands the information processing and financial reporting needs of its clients. DDI strives to provide a practical and cost effective response to complex challenges that are common to many faith-based and non-profit organizations.

Principles, Criteria and Related Controls

The principles specified by DDI and the controls that achieve the applicable trust services principles are listed in Section III – Description of Systems and Sections VI, VII, and VIII regarding tests of operating effectiveness for the Security, Availability and Confidentiality principles.

Complementary User Entity Controls

Certain principles specified in the description can be achieved only if complementary user entity controls contemplated in the design of DDI’s controls are suitably designed and operating effectively, along with related controls at the service organization. In Section IV, Complementary User Entity Controls, specific user controls each DDI client should implement in order to achieve certain principles within this report are identified. These considerations are neither a comprehensive list of all internal controls that should be employed by the client, nor do they represent procedures that may be necessary in all circumstances.

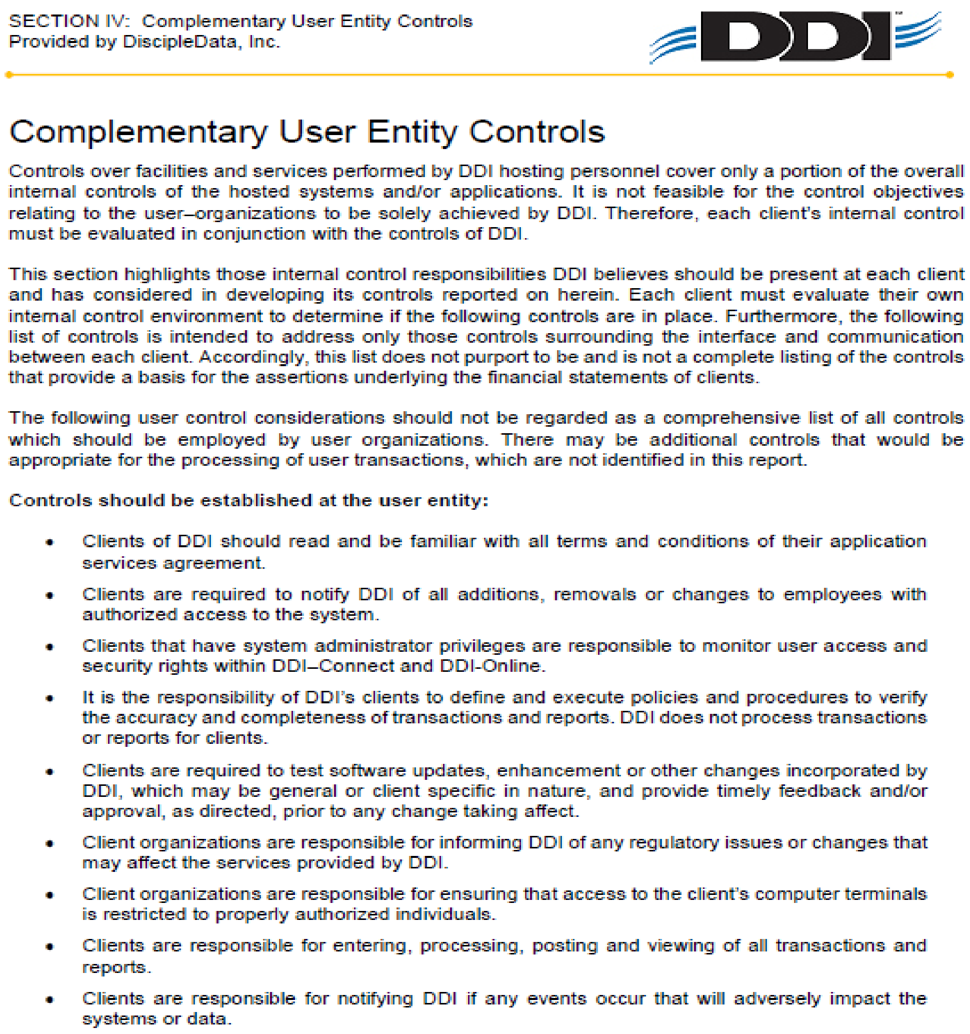
What to Review

1. Consider adequacy of the control objectives and controls.

2. Vendor Management Controls.

Section IV: Complementary User Entity Controls

- Service Auditor’s Opinion
- Management Assertion
- Description of Systems
- **Complementary Controls**
- Subservice Organization
- Test results



SECTION IV: Complementary User Entity Controls
Provided by DiscipleData, Inc.

Complementary User Entity Controls

Controls over facilities and services performed by DDI hosting personnel cover only a portion of the overall internal controls of the hosted systems and/or applications. It is not feasible for the control objectives relating to the user–organizations to be solely achieved by DDI. Therefore, each client’s internal control must be evaluated in conjunction with the controls of DDI.

This section highlights those internal control responsibilities DDI believes should be present at each client and has considered in developing its controls reported on herein. Each client must evaluate their own internal control environment to determine if the following controls are in place. Furthermore, the following list of controls is intended to address only those controls surrounding the interface and communication between each client. Accordingly, this list does not purport to be and is not a complete listing of the controls that provide a basis for the assertions underlying the financial statements of clients.

The following user control considerations should not be regarded as a comprehensive list of all controls which should be employed by user organizations. There may be additional controls that would be appropriate for the processing of user transactions, which are not identified in this report.

Controls should be established at the user entity:

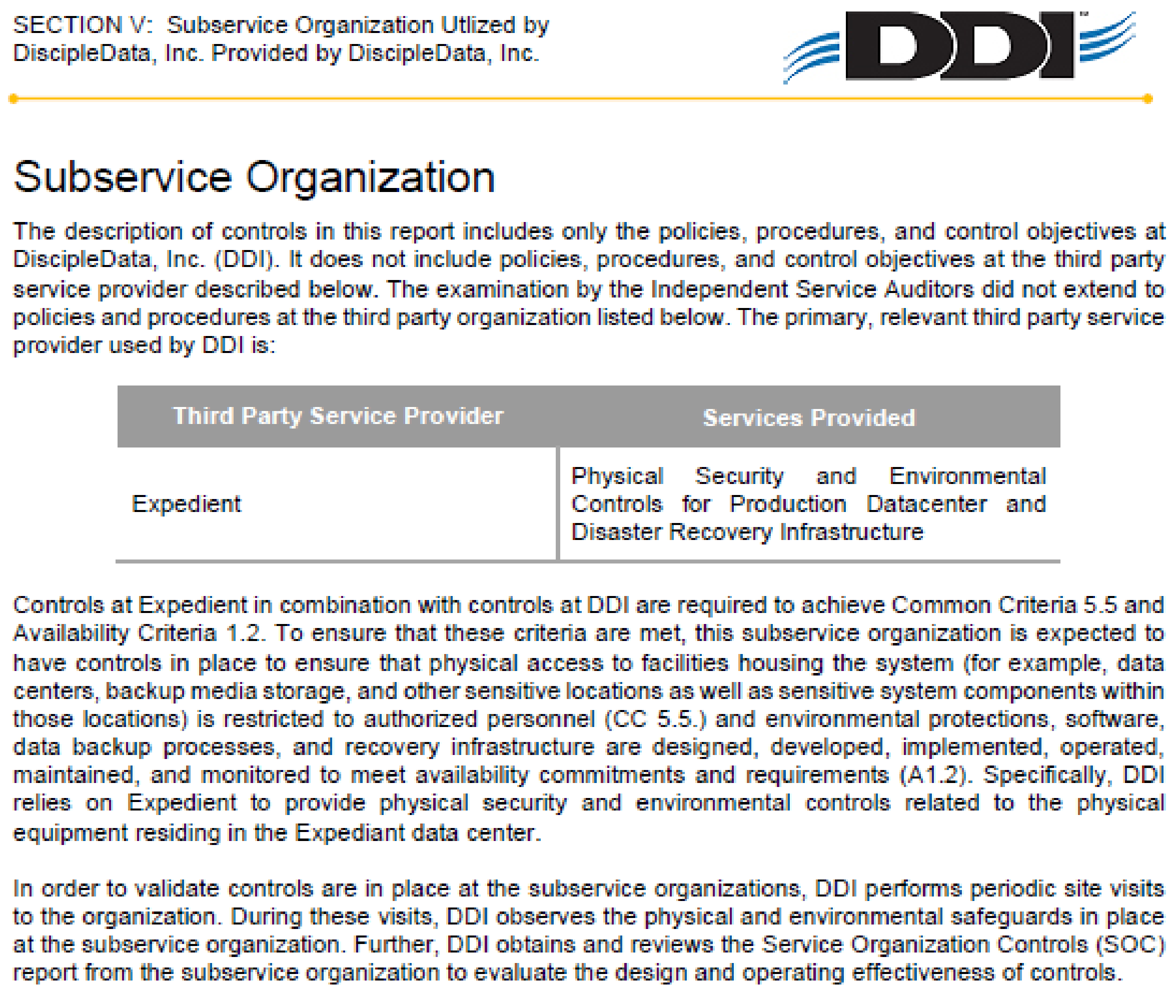
- Clients of DDI should read and be familiar with all terms and conditions of their application services agreement.
- Clients are required to notify DDI of all additions, removals or changes to employees with authorized access to the system.
- Clients that have system administrator privileges are responsible to monitor user access and security rights within DDI–Connect and DDI-Online.
- It is the responsibility of DDI’s clients to define and execute policies and procedures to verify the accuracy and completeness of transactions and reports. DDI does not process transactions or reports for clients.
- Clients are required to test software updates, enhancement or other changes incorporated by DDI, which may be general or client specific in nature, and provide timely feedback and/or approval, as directed, prior to any change taking affect.
- Client organizations are responsible for informing DDI of any regulatory issues or changes that may affect the services provided by DDI.
- Client organizations are responsible for ensuring that access to the client’s computer terminals is restricted to properly authorized individuals.
- Clients are responsible for entering, processing, posting and viewing of all transactions and reports.
- Clients are responsible for notifying DDI if any events occur that will adversely impact the systems or data.

What to Review

1. The control objectives/TSPC specified in the SOC report can only be achieved if the specified complementary user entity controls are suitably designed, implemented and operating effectively by the user entity (a/k/a you, the user of the service).

2. Both the service org & user entity must implement controls in order for the application’s control environment to be complete. *This is your main responsibility!*

Section V: Subservice Organization



SECTION V: Subservice Organization Utlized by DiscipleData, Inc. Provided by DiscipleData, Inc.

Subservice Organization

The description of controls in this report includes only the policies, procedures, and control objectives at DiscipleData, Inc. (DDI). It does not include policies, procedures, and control objectives at the third party service provider described below. The examination by the Independent Service Auditors did not extend to policies and procedures at the third party organization listed below. The primary, relevant third party service provider used by DDI is:

Third Party Service Provider	Services Provided
Expedient	Physical Security and Environmental Controls for Production Datacenter and Disaster Recovery Infrastructure

Controls at Expedient in combination with controls at DDI are required to achieve Common Criteria 5.5 and Availability Criteria 1.2. To ensure that these criteria are met, this subservice organization is expected to have controls in place to ensure that physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel (CC 5.5.) and environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements (A1.2). Specifically, DDI relies on Expedient to provide physical security and environmental controls related to the physical equipment residing in the Expediant data center.

In order to validate controls are in place at the subservice organizations, DDI performs periodic site visits to the organization. During these visits, DDI observes the physical and environmental safeguards in place at the subservice organization. Further, DDI obtains and reviews the Service Organization Controls (SOC) report from the subservice organization to evaluate the design and operating effectiveness of controls.

Service Auditor's Opinion

Management Assertion

Description of Systems

Complementary Controls

Subservice Organization

Test results

<u>What to Review</u>

1. How important is the subservice organization to you and protection of your data?
2. DDI - Common Criteria affected by Expedient's Physical Security and Environmental controls.
3. DDI - Validation of Expedient Physical Security and Environmental controls.

Section IV: Test Results

Service Auditor's Opinion

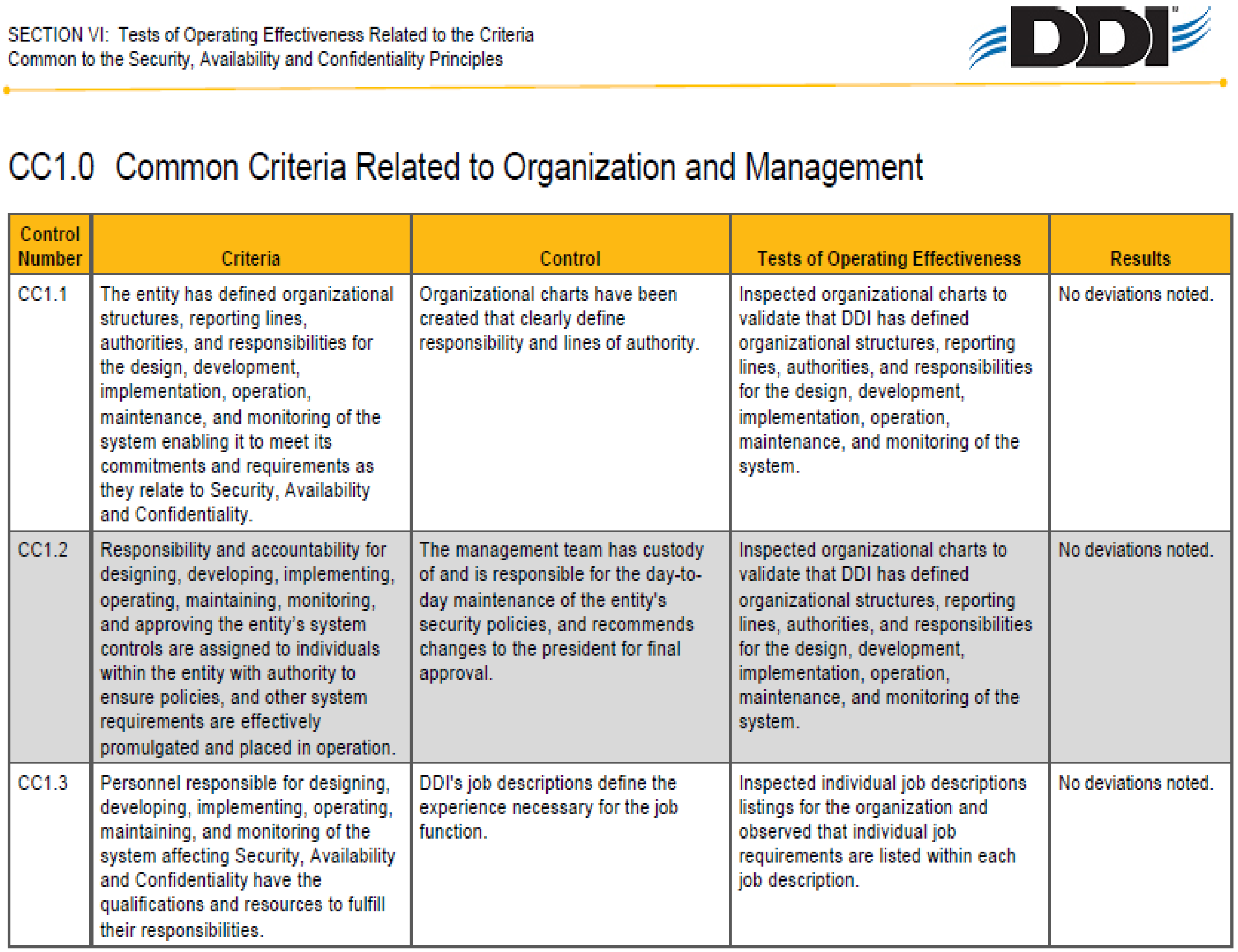
Management Assertion

Description of Systems

Complementary Controls

Subservice Organization

Test results



SECTION VI: Tests of Operating Effectiveness Related to the Criteria
Common to the Security, Availability and Confidentiality Principles

CC1.0 Common Criteria Related to Organization and Management

Control Number	Criteria	Control	Tests of Operating Effectiveness	Results
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and requirements as they relate to Security, Availability and Confidentiality.	Organizational charts have been created that clearly define responsibility and lines of authority.	Inspected organizational charts to validate that DDI has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No deviations noted.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies, and other system requirements are effectively promulgated and placed in operation.	The management team has custody of and is responsible for the day-to-day maintenance of the entity's security policies, and recommends changes to the president for final approval.	Inspected organizational charts to validate that DDI has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No deviations noted.
CC1.3	Personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring of the system affecting Security, Availability and Confidentiality have the qualifications and resources to fulfill their responsibilities.	DDI's job descriptions define the experience necessary for the job function.	Inspected individual job descriptions listings for the organization and observed that individual job requirements are listed within each job description.	No deviations noted.

What to Review

1. **Criteria** – Objective
2. **Control** – DDI's Control to meet the criteria
3. **Tests of OE** – Crowe test procedure to verify control design and operating effectiveness.
4. **Results** – Crowe's results

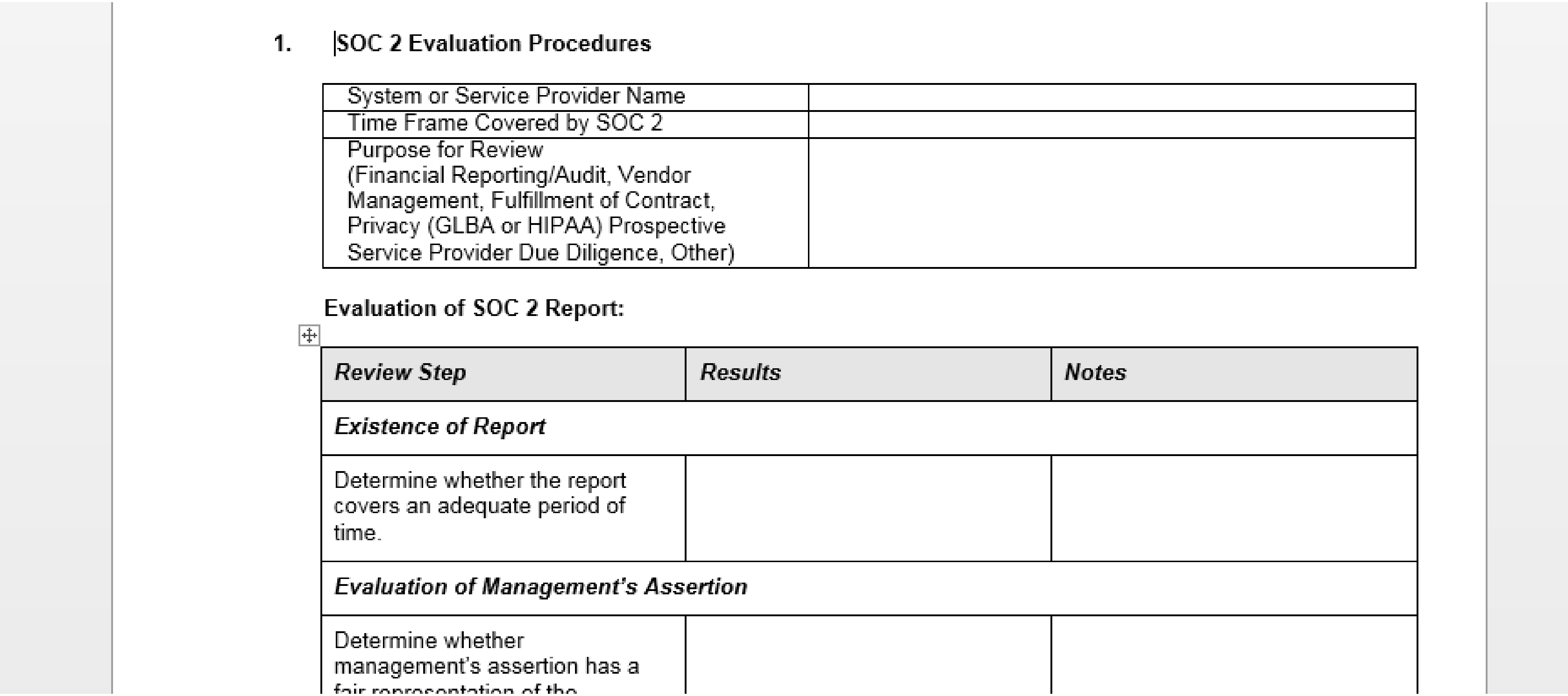
SOC Report Review Recap

Organizations should obtain and formally review SOC reports.

The review should focus on the following:

- Report Type
  - Type 1 or Type 2
- Areas of Coverage/Scope
- Opinion
  - Unqualified or Qualified
  - Subservice Organizations
- Description of Systems Content
- Test Results/Impact of Exceptions Noted
- Evaluation of User Control Considerations

SOC 2 Evaluation Procedures



1. **SOC 2 Evaluation Procedures**

System or Service Provider Name	
Time Frame Covered by SOC 2	
Purpose for Review (Financial Reporting/Audit, Vendor Management, Fulfillment of Contract, Privacy (GLBA or HIPAA) Prospective Service Provider Due Diligence, Other)	

Evaluation of SOC 2 Report:

Review Step	***Results***	***Notes***
Existence of Report		
Determine whether the report covers an adequate period of time.		
Evaluation of Management's Assertion		
Determine whether management's assertion has a fair representation of the		

For more information, contact:

Sean Katzenberger
Direct 317.208.2426
Mobile 317.402.6181
sean.katzenberger@crowehorwath.com

Crowe Service Organization Control Services
http://www.crowehorwath.com/service-organization-control-services/

Crowe Cybersecurity Watch Blog
http://www.crowehorwath.com/cybersecurity-watch/