WE GREATLY APPRECIATE THE CONTRIBUTIONS OF OUR MANY CRVPM'S WHO PROVIDED INPUT TO HELP US MAKE THE COURSE A BETTER ONE

COMPLIANCE EDUCATION INSTITUTE, LLC

Certified Regulatory Vendor Program Manager CRVPM Reference Manual

---

Compliance Education Institute, LLC is a division of RISC Associates, Inc.

Ocean, NJ 07712
Phone 800.310.5580 • Fax 732.922.0113

Table of Contents

Intro

Introduction

The information contained within this **Certified Regulatory Vendor Program Manager (CRVPM) Reference Manual** is intended to provide a vendor program manager with the information needed to build a compliant 3rd Party Oversight program regardless of whether it is being created from the ground up or it is an existing one being revised.

Just as controls that an institution implements vary based upon the size and complexity of the institution, so do the recommended practices within this manual. They must be adapted to the institution's environment. However, the components that make up a compliant program are the same for institutions of all sizes. The preparation for exams and audits is also basically the same for institutions of all sizes although auditors and examiners may request different sample sizes from different asset size institutions.

The fact that you are in possession of this manual indicates that you have passed the Certified Regulatory Vendor Program Manager course and are now a CRVPM. As regulatory focus evolves and shifts with the ever-changing dynamics in technology, cybercrime and business process outsourcing, this reference manual will be updated in order to prepare the CRVPM for exams and audits.

Throughout this manual the following terms will be used:

VPM: Vendor Program Manager

VMO: Vendor Management Office

VOC: Vendor Oversight Committee

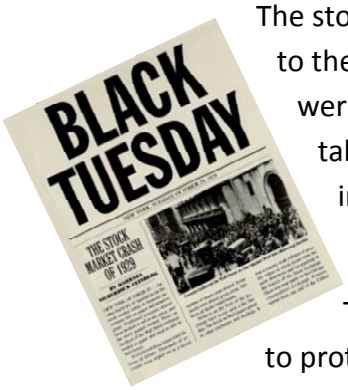
Contact us at the phone number of email address below for support, questions or comments. We are GLBA 501(b) regulatory experts and specialize in vendor management programs, risk assessments, audits, policy, business impact analyses and business continuity plans and incident response plans.

Compliance Education Institute, LLC : **800.310.5580**

support@compliance-edu.com

Section 1

Historical Perspective



The stock market crash of 1929 and the Great Depression are often attributed to the nationwide commercial bank failure. Commercial banks at that time were blamed for overly aggressive investment in the stock market and taking improper risk positions which is widely blamed for the crash. Thus, in 1933 two members of Congress put their names on what is known today as the Glass-Steagall Act.

This act separated investment and commercial banking activities in order to protect the assets of the bank's customers. In addition, banks were not allowed to engage in insurance underwriting due to the risk involved.

1999 saw the Glass-Steagall Act repealed by the Gramm-Leach-Bliley Act, also known as the ***Financial Services Modernization Act of 1999***, signed into law by Bill Clinton on November 12, 1999. Many argued that allowing commercial banks to engage in other activities helped to mitigate their risk by allowing them to diversify and the GLB Act allowed banks to provide a broader range of services.

Historical Perspective

GLB Act, Title V–Privacy (*Refer to FIL-22-2001 for Interagency Guidelines*)

Subtitle A—Disclosure of Nonpublic Personal Information

Sec. 501. Protection of nonpublic personal information

Requires the following agencies and authorities (*described in Subsection 505*) to establish financial institution standards for protecting the security and confidentiality of the banks' customers' non-public personal information:

- FDIC, OCC, NCUA, FRB, CFPB
- Federal Trade Commission (FTC)
- Securities and Exchange Commission (SEC)
- State Insurance Authorities

501(a) PRIVACY OBLIGATION POLICY—It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

501(b) FINANCIAL INSTITUTIONS SAFEGUARDS—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

- (1) to insure the security and confidentiality of customer records and information
- (2) to protect against any anticipated threats or hazards to the security or integrity of such records
- (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer

Act of 2002 specifically prohibits a registered public accounting firm from performing certain non-audit services for a public company client for whom it performs financial statement audits.

Risk Management Activities: Financial institutions may outsource various risk management activities, such as aspects of interest rate risk and model risk management. Financial institutions should require service providers to provide information that demonstrates developmental evidence explaining the product components, design, and intended use, to determine whether the products and/or services are appropriate for the institution's exposures and risks. Financial institutions should also have standards and processes in place for ensuring that service providers offering model risk management services, such as validation, do so in a way that is consistent with existing model risk management guidance.

http://www.federalreserve.gov/bankinforeg/srletters/sr1319.htm

http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf

FFIEC Social Media Guidance: December 11, 2013

The FFIEC issued its final Guidance on Social Media in December 2013. The Guidance regarding ***Third Party Concerns*** is quoted below.

Working with third parties to provide social media services can expose financial institutions to substantial reputation risk. A financial institution should regularly monitor the information it places on social media sites. This monitoring is the direct responsibility of the financial institution, as part of a sound compliance management system, even when such functions may be delegated to third parties. Even if a social media site is owned and maintained by a third party, consumers using the financial institution's part of that site may blame the financial institution for problems that occur on that site, such as uses of their personal information they did not expect or changes to policies that are unclear. The financial institution's ability to control content on a site owned or administered by a third party and to change policies regarding information provided through the site may vary depending on the particular site and the contractual arrangement with the third party. A financial institution should thus weigh these issues against the benefits of using a third party to conduct social media activities. A financial institution should conduct an evaluation and perform due diligence appropriate to the risks posed by the prospective service provider prior to engaging with the provider. To understand the risks that may arise from a relationship with a given third party, the institution should be aware of matters such as the third party's reputation in the marketplace; the third party's policies, including policies on

Why Comply: Penalties & Benefits

Reputational Risk Mitigation:

A reputation can take decades to build and only seconds to destroy. Financial institutions used to build their reputations through community investment and by building partnerships with local businesses. But with the advent of outsourcing key business and technical functions, customers are often dealing directly with an institution's vendors and the institution is in less control of the customer experience. **Thus, Due Diligence, Ongoing Monitoring and Periodic Reviews are increasingly important.**

Improved Risk Management:

Establishing a standard process to evaluate the Physical, Technical and Administrative controls that need to be in place to protect the institution and its customers ensures that risk is properly assessed and managed consistently across all vendors, thus greatly improving vendor risk management.

Improved Risk Management:

Establishing a standard process to evaluate the Physical, Technical and Administrative controls that need to be in place to protect the institution and its customers ensures that risk is properly assessed and managed consistently across all vendors, thus greatly improving vendor risk management.

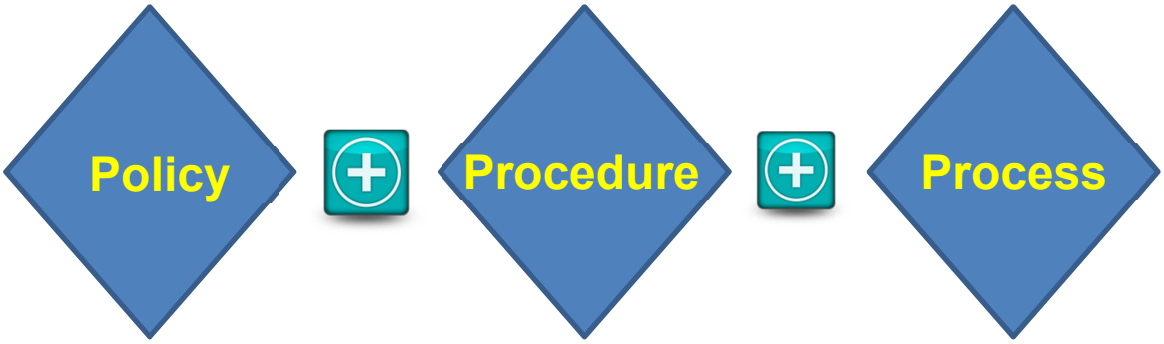
Understanding Who You Do Business With:

Categorizing **(stratifying**) your vendors provides the institution, its examiners and its auditors with a better view of the types of vendors that you do business with. In gaining that understanding, the risk that the institution is faced with becomes better defined and more easily addressed, and effort can be placed in managing risk where it is needed most.

Section 4

Program Components

PROGRAM: (noun): a series of inter-related steps to be carried out inclusive of policy, procedure and process in order to achieve a goal or set of goals



Governance	Due Diligence	Gather
	Risk Rating	Review
	Contract Review	Assess
	Periodic Review	Monitor
	Contract Tracking	Report

Vendor Management Program Components:

Vendor Inventory	Due Diligence	Risk Rating
Contract Review	Contract Tracking	Periodic Review
Policy	Ongoing Monitoring	Reporting

11. Assess the extent to which the activities are subject to specific laws and regulations	A thorough study of the legal and compliance regulations must be conducted so that the institution understands the regulatory issues that both itself and the vendor will be faced with and the capabilities that a vendor must have to ensure compliance. The institution must also have a way in which to monitor the vendor for compliance with all laws and regulations. Privacy Information security Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Fiduciary requirements
12. Consider whether the selection of the third party is consistent with the institution's broader corporate policies and practices including its diversity policies and practices.	Does the institution have a policy that commits a percentage of projects to small businesses, minority-owned businesses, etc. and will outsourcing this function help it achieve its goals with respect to its policy?
13. Detail how the institution will select, assess, and oversee the third party.	This should be covered in the institution's vendor management program and should include policy for conducting: Due Diligence, Risk Assessment Ongoing Monitoring Periodic Review (Financial Review, Performance Review, Contract Compliance, etc.)
14. Present to and be approved by the institution's board of directors when critical activities are involved.	The Board **MUST** review and approve the business case for outsourcing critical functions prior to even searching for vendors and conducting due diligence

Consulting: Auditors, vendors that conduct Penetration Testing and Vulnerability Assessments, Risk Assessments of various types (BSA, OFAC, AML, ACH)

Risk Rating & Criticality: Prioritizing Your Efforts

The point of the initial risk rating is to determine the **INHERENT RISK**. This is the risk that examiners are initially interested when they request a list of your High Risk vendors. It's the risk that you need to understand when initially evaluating a vendor to determine the controls that are required.

The **RESIDUAL RISK** is the risk after controls (quality of controls). This helps you understand whether to do business with the vendor.

Whether implementing a new program or revising an existing one, it is important to prioritize efforts. Once the vendor inventory has been refined, Critical and High Risk vendors should be identified so that attention can be placed on them in terms of ensuring that they are brought to current state. **High Risk vendors are not necessarily critical to the institution**.

Critical Vendor: **a critical vendor is one that cannot easily be replaced and/or one, if services are interrupted or terminated, cause significant operational and/or financial impact.** For example, a document shredding company is inherently high risk because it has access to sensitive but it can easily be replaced and there's no operational or financial impact if they go out of business without warning.

Then the VPM should work down the list to Moderate Risk and Low Risk. Most organizations have only a handful of Critical vendors in comparison to the entire inventory.

To determine initial Inherent Risk Rating use the methodology discussed earlier in this course by examining the criteria below. **Please note that it is up to the Board of Directors to determine the tolerance for risk and what defines it:**

Access to NPPI - automatically High Risk if any of the following are true:

Process

Store

Manage

Centralized Document Repository

One of the most common issues facing institutions that are preparing for exams or audits is locating requested documentation. All too often contracts, controls reports and other critical documents are kept in someone's desk or reside in their email or in some other non-central place that is difficult to locate.

A centralized document repository should be kept on a network fileshare so that all documentation is easily located and backed up. Ideally, all hardcopy documentation should be converted to electronic format.

Developing Questionnaires/Score Cards

Now that the vendor inventory has been refined and vendor categories have been developed, it's time to develop Due Diligence, Contract Review and Periodic Review questionnaires/scorecards and a list of critical documents for each category of vendor. A separate risk rating questionnaire can be developed or Due Diligence questions can be added to it for a combined view. Following are lists of question categories and question sets that you should consider using. You might also have your own questions that you'd like to add or use in place of those listed. Based upon the type of service that the vendor provides (vendor category) you should decide which questions to use. For example, you would not ask a groundskeeping vendor for a SSAE 16 or ask about their DR Plan.

Please note that these questions can be answered Yes/No or point values and weighting factors can be assigned. In addition, you could provide subtotals for each question category in order to obtain a more detailed view of risk. You should work with your Vendor Oversight Committee to determine the scores and weights as well as the ranges that equate to High, Moderate, Low risk.

Risk Rating

Question Category	Question	Score	Weight	Total
Access to NPPI	Does the vendor process NPPI?			
Access to NPPI	Does the vendor View/Add/Modify/Delete NPPI?			
Access to NPPI	Does the vendor store NPPI?			
Access to NPPI	Does the vendor transport NPPI?			

	and/or audits?			
Operational	Are the vendor's facilities management (access control, sharing of facilities, etc.) controls adequate? Make note of any reviews, reports or onsite visits to substantiate it and attach document if appropriate.			
Operational	Does the vendor conduct employee background checks?			
Operational	Does the vendor provide sufficient logical security precautions (firewalls, encryption, etc.)? Document them or attach a report if appropriate.			
Operational	Are the vendor's internal controls and security safeguards adequate as shown by reports or audits (SAS70 for example)?			
Operational	Is the vendor knowledgeable of regulations pertaining to the services they are providing? (GLBA 501(b), SOX, CFPB Consumer Law.)			
Operational	Is the vendor's insurance coverage adequate?			
Operational	Is the vendor's privacy protection policy adequate? Make note of any policy review conducted and attach document if appropriate.			
Profile	Does the product/service that the vendor offers meet the institution's business and technical requirements?			
Profile	Will the vendor's product/service meet current and future needs?			
Profile	Does the vendor rely upon subcontractors?			
Profile	Does the vendor have significant experience working with financial institutions?			
Profile	Is the vendor's Business Continuity Plan adequate to support the institution's business?			
Profile	Were at least three (3) Vendor references checked?			
Profile	Were all reference checks satisfactory? If not, list questionable or negative comments of note revealed during the reference checks.			
Profile	Has the Product/Service that the vendor offers been evaluated?			
Profile	Does the vendor have a current state license?			
Profile	Has due diligence for this existing vendor been conducted? If so please provide any supporting documentation.			
Profile	Has due diligence been conducted for this existing vendor? If so, please provide documentation.			

Contract Review

Question Category	Question	Score	Weight	Total
BCP/DR	Does the contract address the vendor's responsibility for backing up or otherwise protecting program and data files?			
BCP/DR	Does the contract specify that the vendor provide the institution with operating procedures that are to be carried out in the event business resumption contingency plans are implemented?			
BCP/DR	Does the contract address the vendor's responsibility for maintaining disaster recovery and contingency plans?			
Cost Compensation	Does the contract specify conditions under which the cost structure may be changed?			
Cost Compensation	Does the contract describe the cost and responsibility for purchasing and maintaining hardware/software associated with the service?			
Cost Compensation	Does the contract indicate which party is responsible for payment of legal, audit and examination fees associated with			

Cloud Computing

Be prepared to identify the type(s) of service model(s) that is or will be used:

- **Software as a Service (SaaS**) – application software is hosted in the cloud; commonly used for email applications such as Hotmail or Gmail, time reporting systems, customer relationship management (CRM) systems such as SalesForce,com, etc.
- **Platform as a Service (PaaS**) – development platform such as Java, .Net, etc. for developing systems is hosted in the cloud
- **Infrastructure as a Service (IaaS**) – infrastructure resources such as data processing, data storage, network systems, etc. are provided via the cloud
- **Data as a Service (DaaS**) – data is provided or accessed via the cloud such as access to LexisNexis data, Google data, and Amazon data

Issues that the institution must be able to address:

- All network traffic is encrypted in the cloud provider's internal network and during transition from the cloud to the institution's network.
- All data stored on the service providers systems are being encrypted with unique keys that only authenticated users from this institution can access.
- Unless the institution is using private cloud model, determine what controls the institution or service provider established to mitigate the risks of multi-tenancy.
- If a financial institution is using the Software as a Service (SaaS) model, determine whether regular backup copies of the data are being made in a format that can be read by the financial institution. (Backup copies made by the service provider may not be readable.)
- Determine whether the cloud service provider has an internal IT audit staff with adequate knowledge and experience or an adequate contractual arrangement with a qualified third-party audit firm.

Section 7

Best Practices

Best practices are not always practical practices so review each of those included in this section and adapt as necessary based upon your particular environment.

Program Framework

1. **Analyze**: If you're the new Vendor Program Manager or if you are implementing a new program or revising an existing one, it is important to first understand the structure of the previous one even if it only consisted of a spreadsheet to track vendors.
    A. Review the current process for vendor selection and vendor management and determine whether there are any regulatory, policy or process deficiencies.
    B. Determine where the bottlenecks are and why.
    C. Determine whether there is any duplication of effort.
    D. If possible, determine whether the institution misses cancellation deadlines on auto-renew contracts. This will help build a business case for the new process.
    E. Understand the current risk rating process.

2. **Executive Sponsorship** is the key factor for the success of a vendor management program. Senior management must be engaged to support the efforts of the VMO and communicate that support to the rest of the institution. In order to garner that support, build your business case and explain the following to the Executive Sponsor:
    A. Reasons to Comply
    B. Benefits of a Vendor Management Program
    C. Regulatory Penalties for Non-Compliance

3. **Establish a Vendor Oversight Committee** (VOC) composed of Risk, Finance, Compliance, Audit, IT, VMO, Legal and Executive Management:
    A. Reinforces governance of policy and process so that stakeholders (sponsors) are more incline to be cooperative
    B. Brings multiple skill sets to the task at hand so that expertise is applied where needed. For example, IT should be reviewing SSAE16 SOC 2 & SOC 3
    C. Mitigates multiple dimensions of risk
    D. Instills a sense of ownership and importance in the decision-making process

4. **Engage Stakeholders** by conducting a meeting sponsored by Executive Management in order to build a partnership with the stakeholders.
    A. Articulate the benefits of a compliant vendor management program in order to convey the value and efficiencies that will be realized
    B. Discuss the regulatory penalties for non-compliance.
    C. Discuss the corporate policy for compliance (and possibly the penalties for non-compliance but be cautious not to sound threatening and alienate the stakeholders)

5. **Strategy for Success**: within every organization there are those who are adverse to change and those who are willing to embrace it. Thus, it is important to create success stories within your institution that can be used as examples for those who are not proponents of the new process.
    A. **Find a sponsor** within the organization who is typically cooperative and willing to try something new that will make life simpler.
    B. **Set up a pilot program** with that sponsor.
    C. **Fine-tune the program** so that it becomes efficient and productive within your institution's environment.
    D. **Roll out the program** to others on a controlled basis, noting the success with the original sponsor to ensure the continued success.

Type 2: a report that is the same as a Type 1 report but also includes (1) the service auditor's opinion on the operating **effectiveness of the controls** in meeting the applicable criteria and (2) a description of the service auditor's tests of the operating effectiveness of the controls and the results of those tests.

SOC 3: Report on Controls at a Service Organization Relevant to TRUST SERVICES which include Security, Availability, Processing, Integrity, Confidentiality, Privacy. **A general-use report that provides only the auditor's report on whether the system achieved the trust services criteria**. There is no description of tests and results or opinion on the description of the system. It also permits the service organization to use the SOC 3 seal on its website. SOC 3 reports can be issued on one or multiple Trust Services principles.

Strategic Risk: arises from adverse business decisions, or the failure to implement appropriate business decisions in a manner that is consistent with the institution's strategic goals.

Technical Safeguards: Computer Passwords, Firewalls, Intrusion Prevention & Detection Systems

Transaction Risk: risk of loss arising from problems with service or product delivery.

Trust Services: a set of professional attestation and advisory services based on a core set of principles and criteria that addresses the risks and opportunities of IT-enabled systems and privacy programs.

Security. The system is protected against unauthorized access (both physical and logical).

Availability. The system is available for operation and use as committed or agreed.

Processing integrity. System processing is complete, accurate, timely, and authorized.

Confidentiality. Information designated as confidential is protected as committed or agreed.

Privacy. Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles issued by the AICPA and CPA Canada.

The trust services principles and criteria of security, availability, processing integrity, and confidentiality are organized in four broad areas:

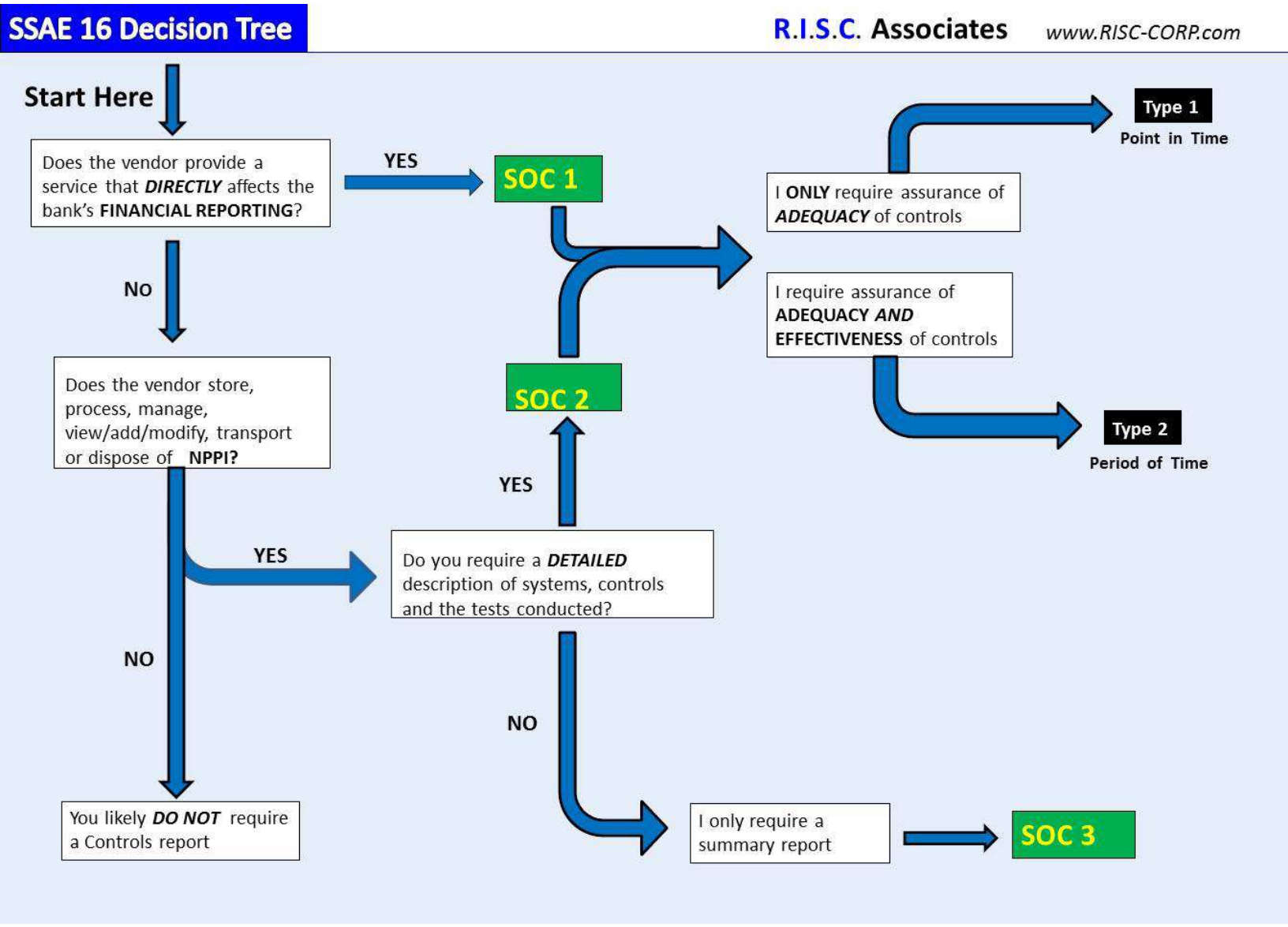
Policies. The entity has defined and documented its policies relevant to the particular principle.

Communications. The entity has communicated its defined policies to responsible parties and authorized users of the system.

Procedures. The entity placed in operation procedures to achieve its objectives in accordance with its defined policies.

Monitoring. The entity monitors the system and takes action to maintain compliance with its defined policies.

Appendix A: SSAE 16 Decision Tree



INDEX

A

B

C

D

E

F

