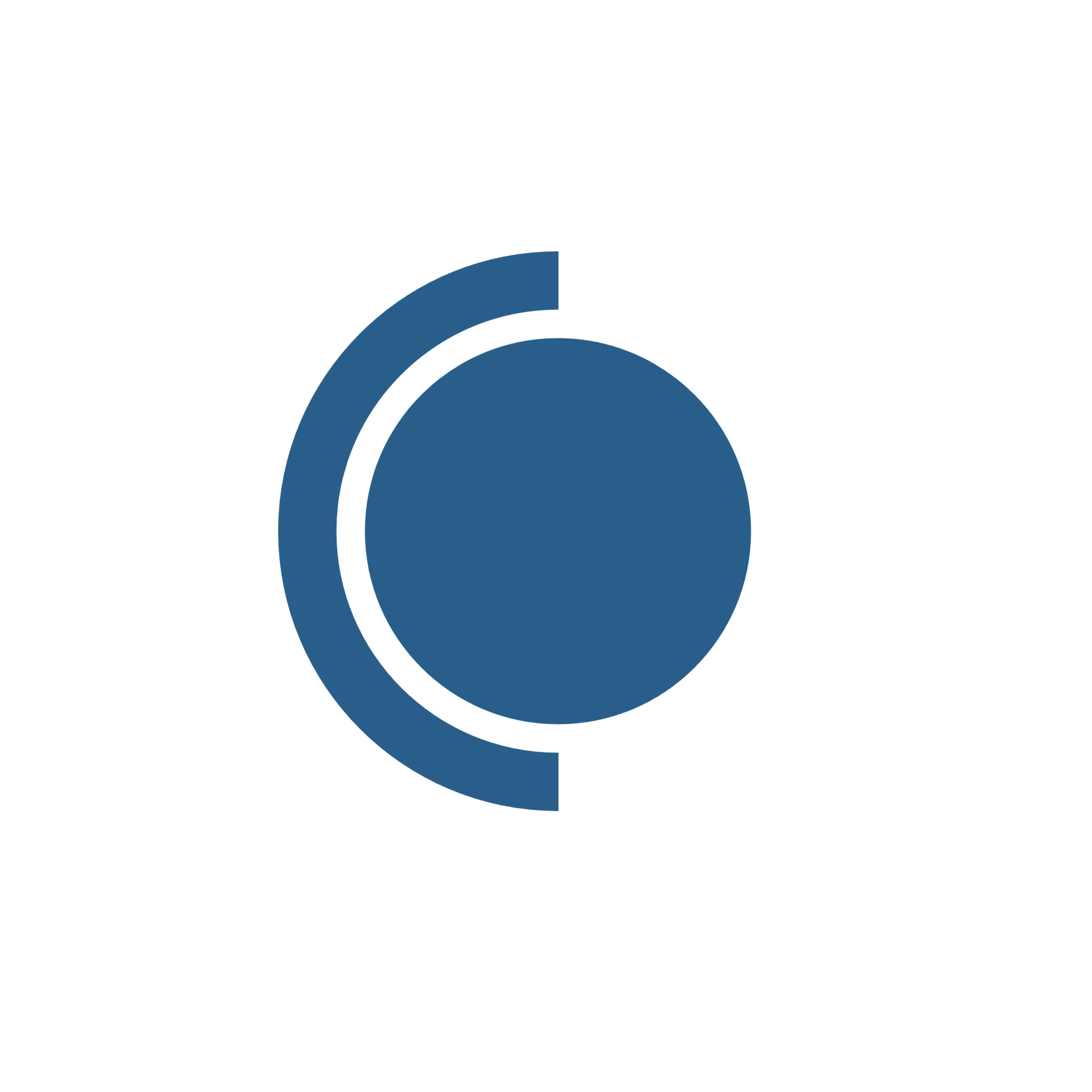


** Table of Contents**



[**Align your security program with your organization’s mission and business objectives** 5](#_Toc179793794)

[**Utilize Committees to formalize cybersecurity decision making** 5](#_Toc179793795)

[**Measure your Information Security Program through meaningful metrics** 6](#_Toc179793796)

[**Implement Policies, Procedures and Controls** 6](#_Toc179793797)

[**Develop a security risk management program** 7](#_Toc179793798)

[**Implement a Security Framework to align with best practices, and industry standards and requirements** 8](#_Toc179793799)

[**Establish a culture of security: Develop a sound Security Awareness and Training program** 9](#_Toc179793800)

[**Apply defense-in-depth measures: Assess the security controls to identify and manage risk** 10](#_Toc179793801)

[**Network Security** 10](#_Toc179793802)

[**Application Security** 10](#_Toc179793803)

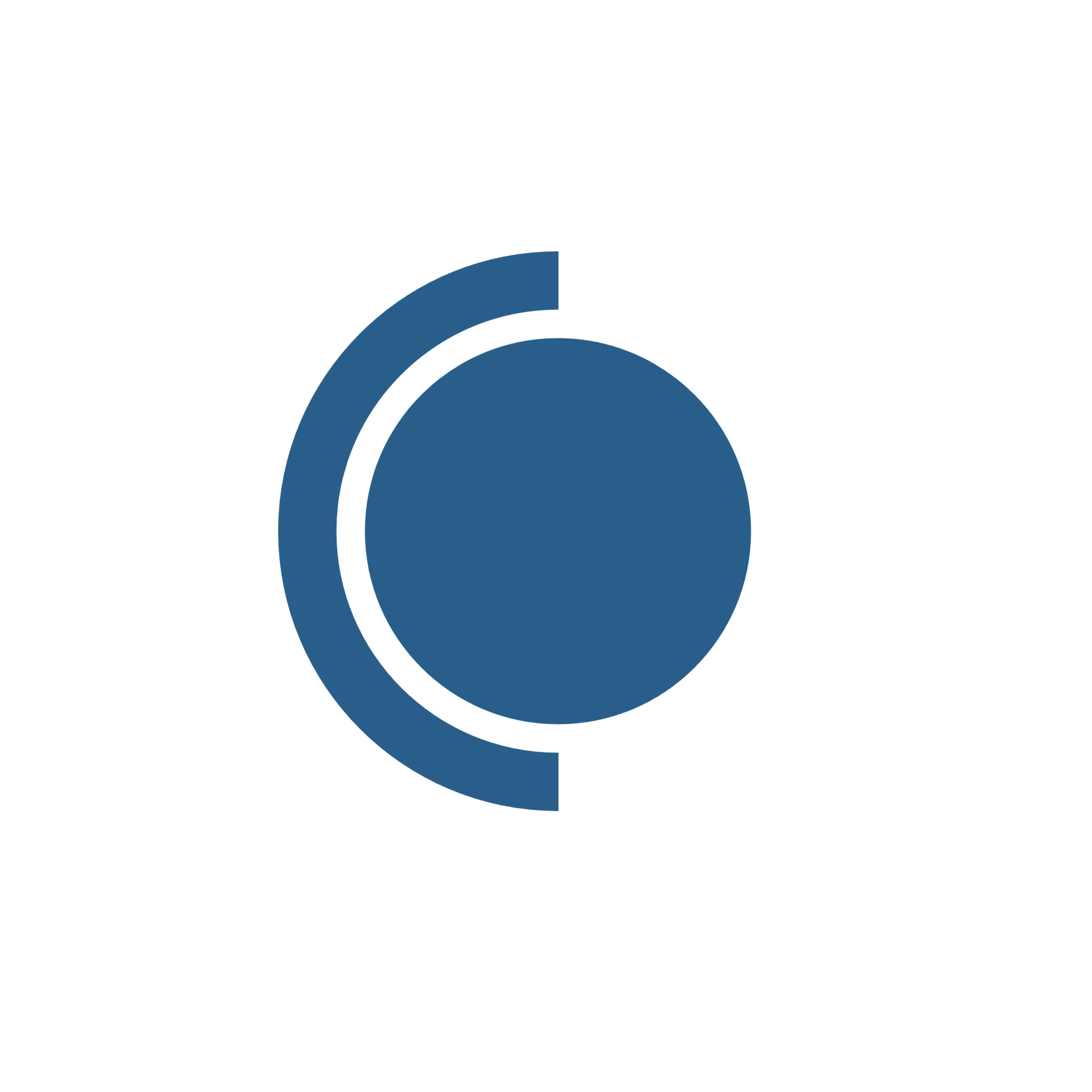
[**Identity & Access Management** 11](#_Toc179793804)

[**Physical Security** 11](#_Toc179793805)

[**Develop a 3rd Party Vendor Risk Management program** 12](#_Toc179793806)

[**Develop a comprehensive Disaster Recovery, Business Continuity and Data Backup Plan** 13](#_Toc179793807)

[**Develop and implement an Incident Response Plan: Train your staff and test your plan periodically** 13](#_Toc179793808)

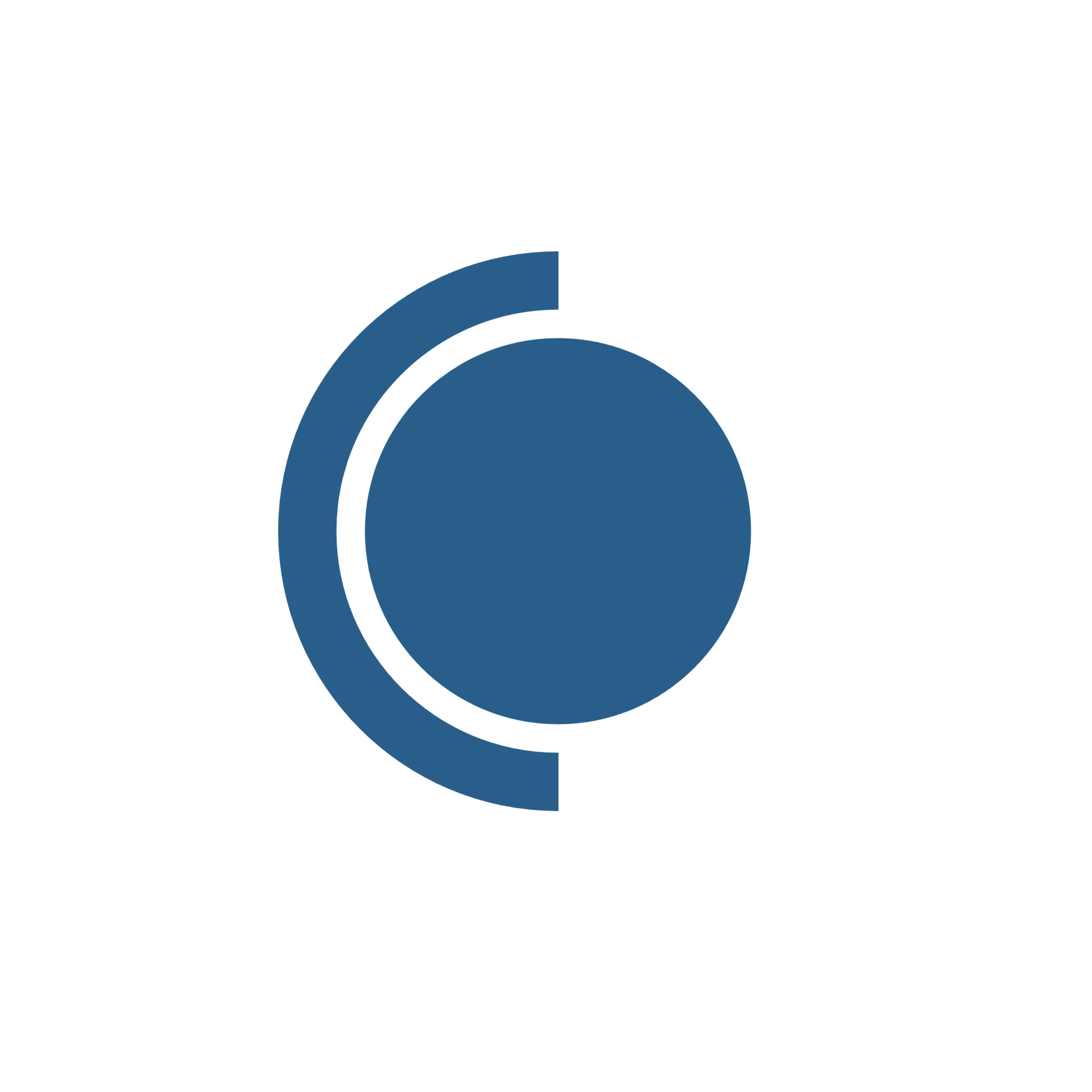


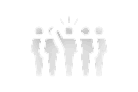
**Action Plan**

|  |  |  |
| --- | --- | --- |
| **Action Step** | **Status** | **Observations** |
| Leadership Initiatives |  |  |
| Appoint a CISO |  |  |
| Align Program to Mission |  |  |
| Utilize Committees |  |  |
| Implement Policies, Procedures and Controls |  |  |
| Develop a Security Risk Management Plan |  |  |
| Implement a Security Framework |  |  |
| Establish a culture of security: Develop a security awareness and training program |  |  |
| Apply Defense in Depth |  |  |
| Network Security |  |  |
| Application Security |  |  |
| Identity and Access Management |  |  |
| Physical Security |  |  |
| Develop a 3rd Party Risk Management Program |  |  |
| Develop a Comprehensive DR, BC and DB Plan |  |  |
| Develop and implement an Incident Response Plan |  |  |



This Information Security Program Development Guide provides a high-level overview of the components that are needed to effectively manage the cybersecurity risks organizations face.



 **Leadership and Oversight**

Cybersecurity regulations require banks and and businesses to name an individual to the role of Information Security Officer (ISO) or Chief Information Security Officer (CISO). The regulations do not specify the qualifications or even the primary responsibility, only that it must be a name individual, not a committee or department and that they must have the requisite experience and skills to manage the program. “Identify the security official who is responsible for the development and implementation of the policies and procedures required by” by the regulations.

Many organizations do not put sufficient thought in both the selection of an ISO and in the responsibilities that will be ascribed to the role. The information security officer is a leader. They are responsible for

* Overseeing the security program
* Writing policies and procedures and ensuring the organization complies with them,
* Advocating for and acquiring “buy-in” for the information security program and the policies and procedures that align with that program.
* The training program that will equip the staff to defend against security and privacy intrusions.
* Chairing the committee or committees burdened with decision making regarding the information security program with such questions as what policies to adopt or how to respond to a security incident.

Despite the weight of these responsibilities, many organizations assign the role to a person based, not on requirements and fitness for the job but on availability. For these organizations, the ISO often spends less than 25% of their work hours on information security related issues and it is often far less. The ISO tends to be reactive rather than proactive in management of information security. Best practice organizations will select an information security leader with the qualifications for the role, provide them authority within the organization to lead and make changes to stay ahead of risks and provide them with the resources, including staff, software and the support of executive management to effectively manage the program.

Questions to consider:

* Are the responsibilities of the CISO clearly identified and described in a document such as a job description?
* Are the roles and responsibilities of the Security Official crafted to reflect the size, complexity and technical capabilities of the organization?
* Does the information security officer have the resources and the authority to effectively fulfill the requirements of the job?
* What percentage of the information security officers time is spent on time related to information security?
* Does the information security officer have experience, training and credentials to be effective in the role?

## **Align your security program with your organization’s mission and business objectives**

The organizations information security program and the information security officer leading the program should be guided by the organizations mission and strategic objectives. These objectives are often, as they should be, driven by the board of directors of the organization. In addition to the audit committee and the executive overseeing risks to the organization, the board should help define priorities for the information security program and provide the necessary budget and resources consistent with those priorities.

Questions to consider:

* Does your organizations board of directors provide oversight and direction for oversight and direction for compliance programs including the privacy and security functions?
* Does the CISO or some other compliance leader report at least annually to the board of directors or the board’s audit committee on strategic information security risks to the organization.

## **Utilize Committees to formalize cybersecurity decision making**

Information security leaders should not make decisions in a vacuum. Rather, decisions, some of which can be extremely consequential such as policies that may have a detrimental impact on productivity or on the degree of risk acceptable to the organization, should be made collaboratively with other key stakeholders such as the office of the executive managing physicians practicing within the organization, nursing staff, Information Technology, Operations and Compliance. Two such crucial committees would be the Privacy and Security Policy Committee (which may go by another name at your organization if you have one) and the Security Incident Response Team (SIRT) or committee (discussed more fully below). Depending on the nature of the committee, committees should meet either at regularly scheduled intervals (as is often the case with Policy review committees) or when needed (as is often the case with a SIRT).

Questions to consider:

* Do you have any committees that provide oversight and direction to the activities of the Information security program?
* Do the committees have an appropriate representative sampling of other functional areas that are potentially impacted by decisions of the Information Security Program?
* Do the committees meet on a regular basis or when need as appropriate based on the purpose of the committee?

## **Measure your Information Security Program through meaningful metrics**

# **Implement Policies, Procedures and Controls**

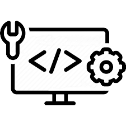
One of the first orders of business for the development of any information security program is the implementation and enforcement Information Security policies, procedures, and controls as needed to comply with the regulations and to reduce risks to a reasonable and appropriate level

Every enterprise has a set of compliance requirements to meet based on the industry they operate in. In the banking industry the regulations that address the privacy and security of customers banking information is primarily Gramm Leach Bliley Act (GLBA). Compliance requirements are expressed as a set of standards that are defined within the regulation and documented in the Code of Federal Regulations (CFR). The GLBA regulations are enumerated under 16 CFR § 314.The requirements of GLBA should be addressed in your information security program as well as applicable state law and contractual obligations with other parties. Your program needs to identify all legal requirements and outline the policies, procedures and controls needed to comply. Compliance, or non-compliance, should be identified as a risk and steps should be taken to comply with regulations to minimize these risks. Compliance, IT and security teams need to coordinate and work together to make sure all compliance-related policies are in alignment with what’s legally required.

Failure to properly address compliance in your Information Security Program can have severe consequences, such as litigation or an investigation by the Office of the Comptroller Currency or the Federal Trade Commission for NBFCs. Failing to comply can result in large fines, damage to reputations and substantial legal fees.

But information security program is more than compliance. Compliance is a crucial but, by itself, an inadequate driver to determine what policies that should be implemented by the organization. Policies should include elements based on best practices, security frameworks adopted by the organization and in response to security incidences.

Questions for Consideration

* Have you created a regulatory policy map to determine whether you have the policies needed to comply with GLBA, state regulations and other obligations?
* Beyond compliance, do you have a framework and process in place to determine the policies, procedures and controls that need to be in place in order to effectively protect non-public personal information (NPI) and other sensitive information?

# **Develop a security risk management program**

The GLBA regulations and all information security frameworks require organizations to develop a risk management strategy that is driven by the GLBA safeguard regulations that require banks to Conduct an Accurate Risk assessment. This regulation requires organizations to know what their risks are and to mitigate them to a reasonable and appropriate level. The risk assessment and risk mitigation efforts require a set of activities that are aimed at lowering the level of cyber-attack risk to an “acceptable level.” What that is will depend on the nature of your business, systems, and data.

The risk management portion of your Information Security Program will affect many other areas of the program, and usually includes the following elements:

* Risk Assessment: All risks within the scope of your information security program are identified, and categorized based on potential severity and likelihood taking into account your organization’s culture and technical systems. In banking, risk assessments are usually qualitative, not quantitative, which means the assessment does not quantify the potential dollar cost of risks or the cost of the controls to manage the risk.
* Risk Mitigation Based on the results of the risk analysis, organizations should outline the concrete steps of how to mitigate and minimize risks to a reasonable and appropriate level and with the oversight of the CISO and other stakeholders.
* Risk Monitoring: Controls should be continually monitored for changes in risk levels or new deficiencies or weaknesses that may rise to the surface over time as a result of security incidences, the results of periodic audits and log reviews. New policies and controls should be deployed to manage and lower risk to an appropriate level.

Questions to consider:

* Does your organization conduct an annual security risk assessment?
* Does your organization conduct a risk assessment when considering a significant operational change such as a move to new software or when moving to new facilities?
* Does your organization have controls in place to monitor risks to the network and organization such as network alarms, and routine audits of system logs?



# **Implement a Security Framework to align with best practices, and industry standards and requirements**

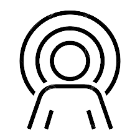
As more organizations begin to move away from a compliance driven approach information security to a risk-based approach, they are often confronted with the question: What is a reasonable amount of effort we should put into our cyber-defense program for an organization of our size and complexity? The GLBA regulations aren’t helpful. They leave many questions unanswered because the focus of the regulations is too narrow and provide little guidance on how to implement addressable safeguards.

A cybersecurity framework serves as a roadmap for organizations to understand what can and should be done. Cybersecurity roadmaps are derived from a consensus of expert communities of information security professionals across industries. They also have the benefit of allowing organizations to scale because many have workable “tiers” based on the size and complexity of organizations. The provide a set of recommended controls, policies, procedures and practices appropriate to most organizations. Some examples of well-established and adopted frameworks include:

* The Center for Internet Security (CIS) Top 20
* NIST Cybersecurity Framework (CSF)
* ISO 27000

Implementation of a Cybersecurity Framework can take years. But organizations that begin to implement one will see immediate benefits in greater clarity in decision making and better direction as the information security program evolves.

Questions for Consideration:

* Have you adopted an information security framework?

# **Establish a culture of security: Develop a sound Security Awareness and Training program**

An ongoing information security training and awareness program is one of the most important elements of an Information Security Program. People are sometimes the weakest link in protecting NPI and training and awareness is the most critical way to minimize those risks. An information security program should provide an ongoing training and security awareness program and structure.

A training program can be provided to staff multiple ways such as through live classroom sessions, quizzes, online training, workshops, and simulated phishing programs. Security training awareness needs to be included as a part of any new employee training and onboarding procedures. In addition, security awareness programs should include modules and methods related to social engineering attacks and teaching staff to recognize bogus emails, texts or other communications so they don’t fall prey to these efforts on the part of bad guys. One way to promote this awareness, in particular, that is quite effective is “phishing simulation” training. Phishing simulations are conducted by the organization, not by the bad guys, but use identical techniques and methods to malicious parties. Simulations allow employees who are most prone to these attacks to be identified and receive remedial training if necessary.

Also, make sure that training and awareness is a part of your employee’s evaluation policies and standards. Employees should take these efforts seriously and making training material mastery is useful to include in employees’ evaluations. Ideally an information security program includes testing and quizzes that document the trainee’s mastery of the material.

Questions to consider:

* Do your organizations training program include both initial orientation training for new employees AND annual training for all employees?
* Does your organization use phishing simulations to help employees recognize bogus emails from hackers and malicious actors?

# 

# **Apply defense-in-depth measures: Assess the security controls to identify and manage risk**

Organizations need to apply defense in depth, or multiple layers of defense in order to effectively protect assets.

### **Network Security**

An information security program should include all the critical elements necessary for assuring the protection of IT assets, networks and systems. Network security should focus on defining, analyzing, and monitoring the security of your network. It should provide strong cyber-defenses as well as address potential gaps that hackers might seek to exploit.

Your network security program should cover all of these main areas:

* Vulnerability Scanning
* Patch Management
* Updated Security Applications (firewalls, proxies, antivirus software, etc.)
* Network Architecture Design (and review)
* Endpoint Controls & Analysis

Network security is a shared responsibility, from the executive leadership team, the board of directors, IT staff down, front line staff and even housekeeping and maintenance employees. The IT security team can define the technical policies and procedures that should be followed and work with executive and management personnel to ensure the right business practices are outlined and followed to minimize the risk of a network security breach.

### **Application Security**

Application security controls thwart risks that arise out of vulnerabilities associated with your applications. Applications could include software developed in-house, third-party on-premise applications or software hosted in the cloud by third parties. Your program needs to identify strategies to address risks associated with any applications that could potentially be exploited, applications should be appropriately categorized based on how critical they are and the sensitivity of the data they contain.

These risk classifications provide guidance and clarity to your cyber security and IT to help them make informed decisions about what types of controls and protections are required for each application. Some important components of an application security framework will often include:

* Penetration Testing
* Vulnerability scanning
* Source Code Review
* Patch Management

The information security team will be the participants implementing the application security program. All relevant technical cybersecurity staff should include throughout the development lifecycle from design, development, implementation and maintenance. This helps the cybersecurity team to identify potential weak points in application that could be a targeted for attack so controls and strategies can be implement to minimize the risk.

### **Identity & Access Management**

The information security program should include processes for identifying employees that have access to critical systems and data (i.e identity and access management). These identification methods could include identity cards with photograph, name, age, or employee ID number or biometric data or other forms of personally identifiable information (PII). This can be in addition to usernames and passwords that personnel typically require to access systems and data.

In addition, the information security program should define processes by which employee roles will be determined and access granted based on that role. This can be based on key principles such as least privilege, need-to-know, and business function.

### **Physical Security**

The physical & environmental security element of an Information Security Program is crucial to protect assets of the organization, such as computers, facilities, personnel, papers, and media from physical threats. Controls typically implemented to promote physical security include:

* CCTV
* Environmental monitoring devices
* Water sprinklers
* Smoke detectors
* Fencing
* Locks
* Security guards
* Adequate Lighting
* Access control cards issued to employees.

Physical spaces within an organization should be classified based on factors such as the information they hold or might provide access to, and controls should be deployed

based on the criticality and sensitivity of the area. Your information security program might, for example, require that visitors are only allowed in designated spaces unless accompanied by staff or that administrative staff doesn’t have keys to file cabinets with highly sensitive information.

Areas holding the most critical or sensitive data should require multiple forms of authentication. Physical security controls should be constantly measured and tested to ensure employee compliance and readiness.

Questions to consider:

* Have you applied a defense in depth approach when deploying security controls to manage risk?

# **Develop a 3rd Party Vendor Risk Management program**

As more organizations move to core applications hosted in the cloud, the burden and risks associated with 3rd parties has grown exponentially. Cloud hosted vendors will be responsible for certain kinds of risk that would have been part of on-premise deployments of computers but shift to the vendor when moving to the cloud. For example, the physical security of facilities and infrastructure shifts to the vendor. But substantial portions of information security remain the responsibility of banking organizations. As more and more data, and more critical and sensitive data shifts to 3rd party vendors, it is necessary for entities to actively understand what the risks are associated with these third party and to take steps to categorize these risks and manage them according. Many organizations don’t even have a good handle on who their business associates are, much less on what risks they pose.

3rd party risks can be ascertained by gathering a listing of those vendors and business associates that are storing, managing and transmitting sensitive information, quantify the amount of data being processed and the sensitivity of that data and whether the function being provided by the vendor is mission critical and time sensitive. For example, a failed backup vendor is an important risk to address. The amount and sensitivity of the data is often significant, but most organizations can operate if there is a temporary blip in the

quality of backups. But vendors providing real-time access to software and data necessary to run an organization are in a different category.

3rd party vendors should be risk stratified and then the program should manage those risks accordingly with appropriate interventions such as annual attestations from the vendor, 3rd party certification such as with a SOC audit or HITRUST certification, onsite audits, etc.

Questions to consider:

* Do you know who your business associates are? Are they logged in a central database or spreadsheet of some sort?
* Do you know and have documented the risks associated with 3rd party vendors? And do you manage those risks accordingly?

# **Develop a comprehensive Disaster Recovery, Business Continuity and Data Backup Plan**

A Disaster recovery, Business Continuity and Data Backup plan provides organizations with the tools to deal with a breach or attack, understand how to respond to emergencies such as severe weather events or hacking incidences. Organizations should conduct Business Impact Assessments to consider the potential impact of incidences and to determine factors such the appropriate amount of downtime and data loss after (and during) a disaster scenario.

A business continuity and disaster recovery program should define metrics and objectives for recovery time, and conduct root cause analysis to understand how a failure occurred. The program should include recovery procedures, call trees, action triggering criteria, and the scope of action for each employee role to ensure your systems and data are recovered as quickly as possible after an incident.

Questions to consider:

* Do you have a written, comprehensive business continuity, disaster recovery and data backup plan in place?
* Do you periodically test your procedures to ensure they are effective when needed?

# **Develop and implement an Incident Response Plan: Train your staff and test your plan periodically**

No information security program is complete without policies and procedures detailing how organizations will respond to a cyber breach or incident. Organizations should designate the key employees who will comprise the Security Information Response Team (SIRT) following and incident and will describe the steps that will be applied and documented including the steps that will be take to contain or eliminate the impact of the incident.

Well defined incident response policies and procedures allow organizations to limit the damage resulting from a breach or incident as well as reduce the likelihood of a recurrence in the future. An incident response procedure often includes the following elements although these are sometimes combined into similar processes:

* Incident Detection & Identification
* Triage & Incident Analysis
* Threat Containment
* Incident Resolution
* Root Cause Analysis
* Incident Reporting

Your incident response policy should develop security controls, people, processes, and technologies that facilitate the incident response process and mitigate the risks as quickly and effectively as possible. In addition to internal staff, your incident response plan may include third-party partners such as cyber forensic experts, legal teams, compliance leadership, etc. A well-developed incident management policy will not only help address a threat quickly but do so in a cost-effective manner.

Questions to consider:

* Do you have a clearly defined incident response and reporting policy and procedure?
* Does the program include root cause analysis and the response to incidences, such as implementing new controls or updating policies, to help prevent the recurrence of incidences?
* Does the incident response program include guidance on whether an incident might be classified as a breach so that appropriate actions can be taken such as conducting a risk analysis?