DATA FLOW DIAGRAMS

Mapping Your Way to Better Security

PREPARED BY:

YHB CPAs & Consultants
RISK ADVISORY SERVICES

EXECUTIVE SUMMARY

Today's business landscape is fast paced, and ever-changing. If you are always reactive instead of proactive, generally, you are losing. Despite this, there is one fact that never changes: threat-actors are always looking for a way in. For hundreds of years protecting your business was about physical security, and while still vital, the evolution of technology has made cybersecurity king.

I know what you are thinking, 'there is that word again...cybersecurity. We have already addressed it with firewalls, encryption, anti-virus, etc.,' and the truth is you most likely have implemented all of those items. But how do you know if you are truly secure, if you have not first identified the data in which you are protecting. Thus enters the data flow diagram.

A data flow diagram is an illustrative representation of where specific data resides and flows through an entity's system, either your own or your vendors' systems, during a business process. The key takeaways from this definition are as follows:

- Data is identified both at rest AND in transit
- Data may reside within your system AND at a vendor, both of which are entities
- All of this is identified during a specific business process

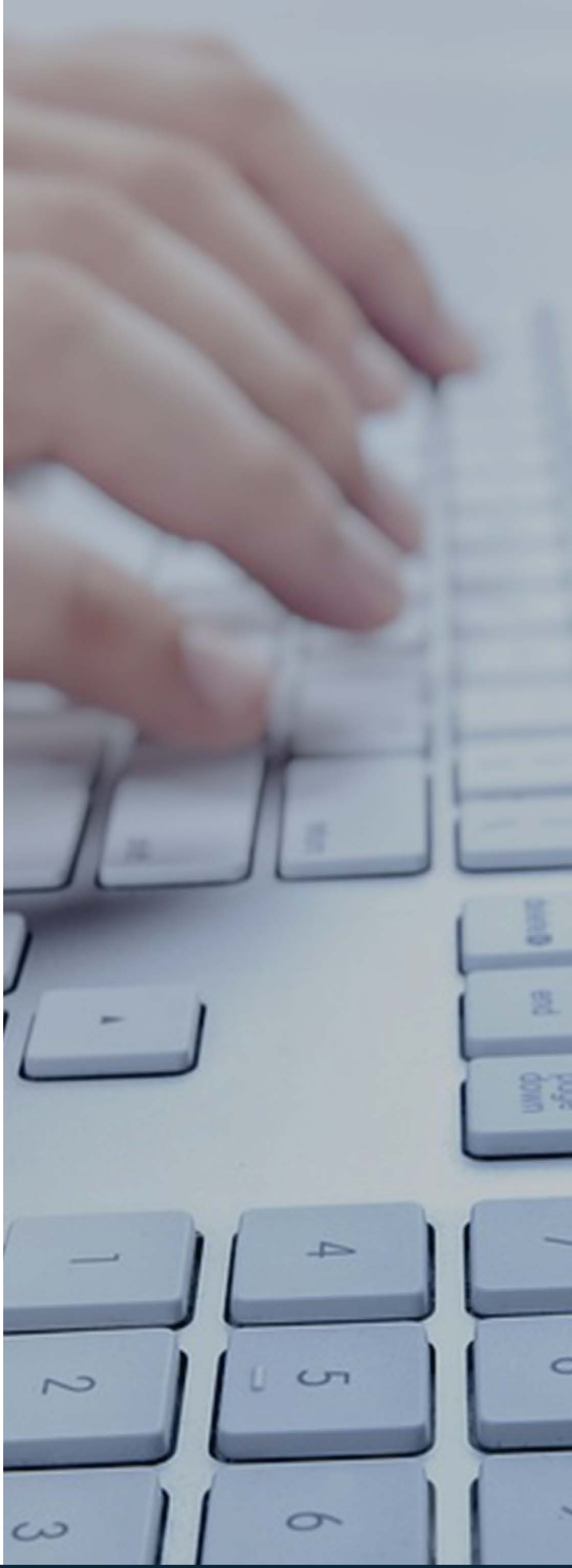
The beauty of a data flow diagram is that it allows you to visualize the interconnected nature of internal systems and external vendor systems so as to ensure data security throughout the process lifecycle. If your payroll processor has you send and receive sensitive data, i.e. employee payroll information, over unencrypted channels, then not even the best internal cybersecurity posture in the world will protect your data during that phase of the business process. A breach in a similar customer related process would open the bank to financial and reputational loss, as well as a host of regulatory problems.

Data flow diagrams are focused on individual (or interconnected) business processes. It is understandable that an organization may have literally hundreds of business processes. That is why the development of data flow diagrams must be completed from start to finish, as opposed to just drawing some circles and squares on a piece of paper. The process is as follows:

- Risk Assessments – Corporate governance, vendors, cybersecurity, and key business processes
- Inventory Listings – Hardware, software, and data – both at rest and in transit
- Develop the diagrams

The following white paper will provide an in-depth review of the history, the 'why', the process, and an example for the creation of data flow diagrams. Data flow diagram development is itself, a process, and an involved one at that. One that at the end of the day will require a significant investment of time from a significant number of people. A cost benefit analysis of the situation, however, will show a significant dividend via improvements in both data security and your overall cybersecurity profile maturity.

CONTENT

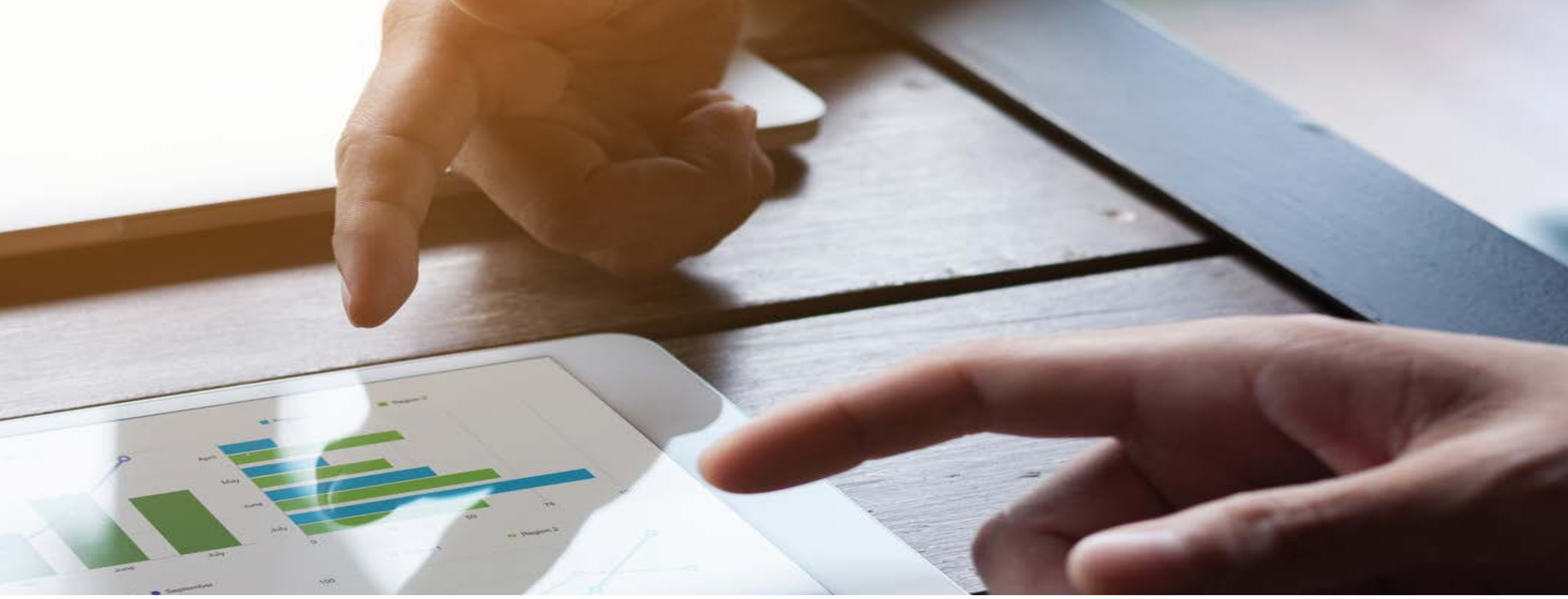


Introduction

Over the past few years, many organizations have been using the FFIEC Cybersecurity Assessment Tool, or NIST Cybersecurity Framework, as a basis to establish a mature framework of controls over digital assets. In these available frameworks and tools, there are references regarding the creation of a data flow diagram. We often get questions around what a data flow diagram is and how to create one. This document is intended to provide that guidance.

The root question is really the "why?" Organizations want to know why they need to create a data flow diagram. In answering that question, it is helpful to understand the history of some key players, the various references within handbooks and other tools, and what a data flow diagram is. We will tackle those points in the following sections.

Once the foundation has been established, we outline a practical process to develop and implement a data flow diagram. It is important to understand that not all organizations are created the same, nor are they at the same point in their cybersecurity maturity. Therefore, the steps will seem laborious to some organizations, while others will feel like it is putting a bow on the neatly packaged gift.



Part 1: Historical Perspective

There are several major organizations involved in developing cybersecurity frameworks and assessment tools. The base of this white paper will focus on the Federal Financial Institution Examination Council (FFIEC) and the National Institute of Standards and Technology (NIST). The FFIEC developed the Cybersecurity Assessment Tool which many financial institutions use to assess the current cybersecurity landscape within their organization. It assists in identifying strengths in the current control structure and areas of focus. NIST's Cybersecurity Framework is a comprehensive model and is used in part to develop the Cybersecurity Assessment Tool.

This initial section will lay out a brief history of both organizations and the important work done by each. Understanding the source and the documents which reference data flow diagrams will hopefully begin to contextualize their importance.

Federal Financial Institution Examination Council

In October 1978 the 95th Congress passed the Federal Institutions Regulatory and Interest Rate Control Act (H.R.14279)[1], which was signed by President Jimmy Carter on November 10, 1978. The result was Public Law 95-630, containing 21 Titles. The 10th Title of this legislation is known as the "Federal Financial Institutions Examination Council Act of 1978." The newly minted council, Federal Financial Institution Examination Council (FFIEC), was established to "proscribe uniform principles and standards for the Federal examination of financial institutions by the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, the Federal Home Loan Bank Board, and the National Credit Union Administration, and to make recommendations to promote uniformity in the supervision of these financial institutes." The FFIEC now comprises the principals of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.

[1] https://www.congress.gov/bill/95th-congress/house-bill/14279

FFIEC Guidance

Information Technology Examination Handbook[2]

The FFIEC announced the publication of the 1996 FFIEC Information Systems Examination Handbook (IS Handbook)[3] on September 19, 1996. The Handbook was sponsored by the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and the Office of Thrift Supervision. Guidance provided to examiners and financial institutions on the effectiveness of information technology can now be found in a series of IT Booklets[4] supporting the IS Handbook ranging from topics such as: Audit, Business Continuity Planning, Development and Acquisition, Information Security, Outsourcing Technology Services, etc. Much like NIST documentation, these are great tools for examiners to utilize when evaluating a financial institution.

Cybersecurity Assessment Tool

As technology has become increasingly pervasive in Federal Institutions (FIs), the FFIEC sought to further focus principles outlined in the IT Handbook to cybersecurity preparedness. They developed and released the Cybersecurity Assessment Tool (CAT) in June 2015.[5] The voluntary tool incorporated cybersecurity-related principles from the IT Handbook, regulatory guidelines and concepts from other industry standards including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[6]

National Institute of Standards and Technology

The National Institute of Standards and Technology, a part of the U.S. Department of Commerce, can traces its roots back to 1824.[7] Congress enacted an agency within the Treasury Department to establish and promote the consistent use of uniform weights and measures. In 1890 Congress established the Office of Construction of Weights and Measures and by 1894 had authorized the Office to define and establish the units of electrical measure. Under President Theodore Roosevelt, the name was changed to the National Bureau of Standards (NSB) and added the responsibility of addressing the growing use of electricity.

In 1988 Ronald Reagan signed into law the Omnibus Trade and Competitiveness Act (Public Law 100-418) which changed the name of the NBS to the National Institute of Standards and Technology. The agency was given the added task of helping the U.S. industry increase its competitiveness in the global marketplace. Today, NIST's mission is "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."[8]

NIST Guidance

Special Publication 800

Under President Barack Obama, in October 2013 the 113th Congress passed the Federal Information Security Modernization Act of 2014 (Public Law 113-283)[9] . The result for NIST was the Special Publication (SP) 800 series. The series comprises guidelines, recommendations, technical specifications,and annual reports of NIST's cybersecurity activities.

[2] https://www.ffiec.gov/handbook.htm

[3] https://www.ffiec.gov/press/PDF/FFIEC_IT_Handbook_Information_Security_Booklet.pdf

[4] https://www.ffiec.gov/handbook.htm

[5] https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf

[6] https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf

[7] https://www.nist.gov/physical-measurement-laboratory/nist-guide-si-preface

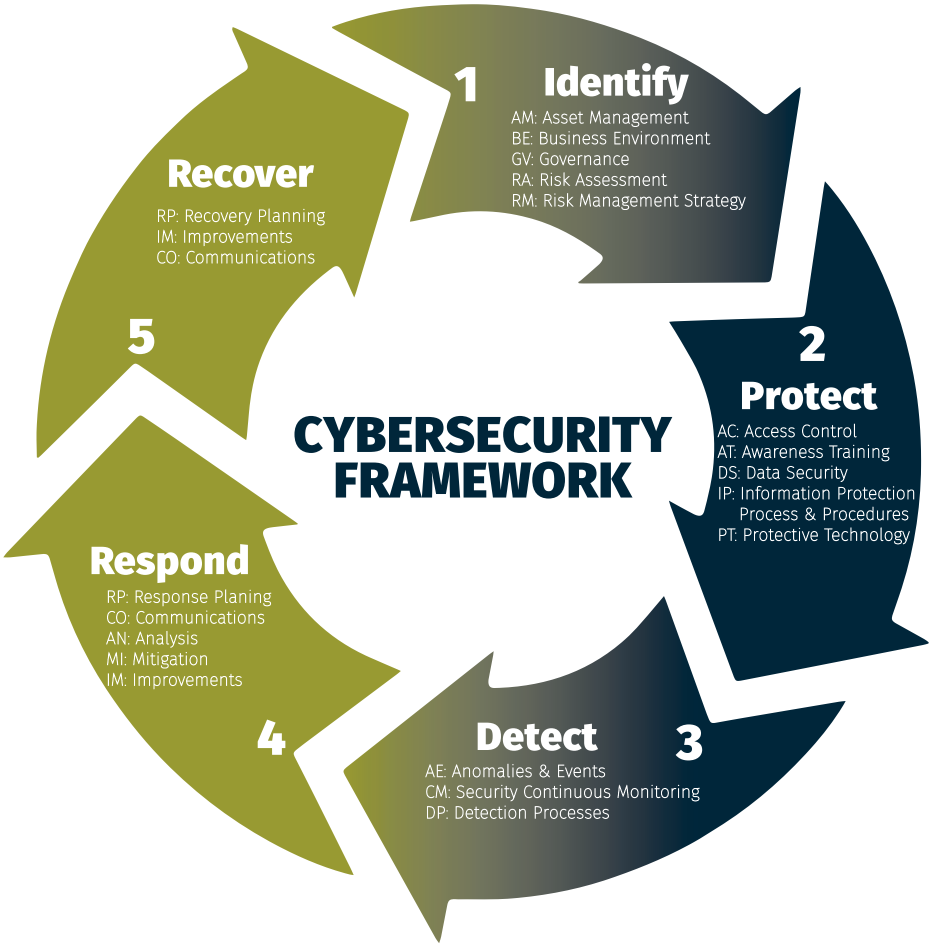
[8] https://www.nist.gov/about-nist/our-organization/mission-vision-values

[9] https://congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

Cybersecurity Framework

The Executive Order (13636) – Improving Critical Infrastructure Cybersecurity[10] issued by President Barack Obama stated, "The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible."

The Framework for Improving Critical Infrastructure Cybersecurity version 1, released in February 2014, focuses on using business drivers to guide cybersecurity activities and to consider cybersecurity risks as part of the organization's risk management process. The Framework included three parts: Core, Profile, and Implementation Tiers. The Framework Core included the following five categories.



[10] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Part 2: FFIEC Cybersecurity Audit Tool

The intent behind the CAT is to enhance Management's governance oversight and maintenance of the cybersecurity program. The following benefits were identified:

- Identifying factors contributing to and determining the institution's overall cyber risk.
- Assessing the institution's cybersecurity preparedness.
- Evaluating whether the institution's cybersecurity preparedness is aligned with its risks.
- Determining risk management practices and controls that are needed or need enhancement, and actions to be taken to achieve the desired state.
- Informing risk management strategies.

The Assessment Tool consisted of two parts: development of an Inherent Risk Profile and understanding of Cybersecurity Maturity.

Inherent Risk

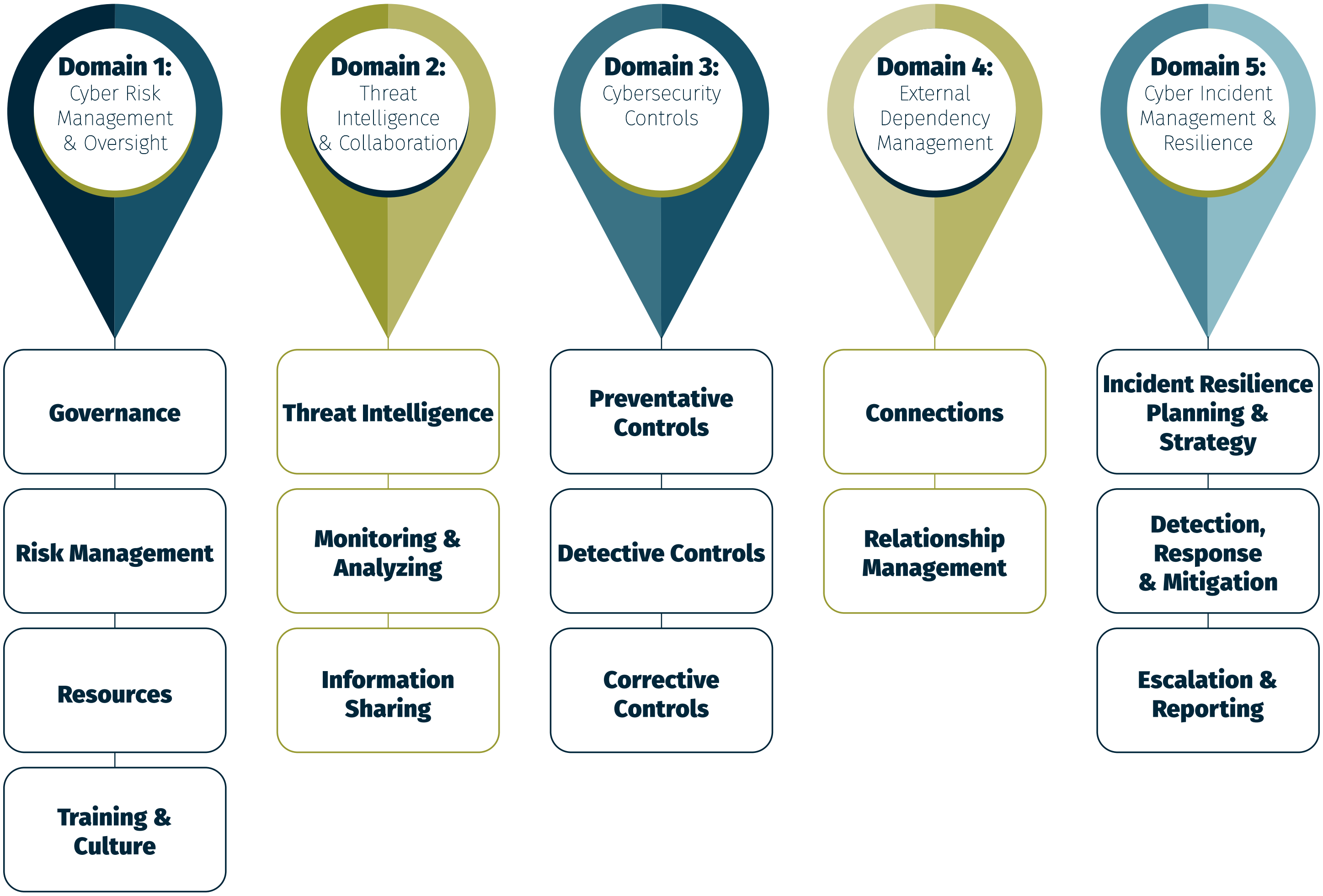
Inherent risk incorporates the type, volume, and complexity of the institution's operations and threats directed at the institution. It is designed to identify the level of risk posed by the following:

- Technologies and Connection Types: covers the number of Internet Service Providers (ISPs) and third-party connections, internally hosted versus outsourced systems, number of unsecure connections, use of wireless access, end-of-life systems, cloud services and use of personal devices
- Delivery Channels: addressed whether products and services are available through online and mobile delivery channels and extent of Automated Teller Machines (ATMs)
- Online/Mobile Products and Technology Services: includes various payments systems, such as debit and credit cards, P2P payments, originating automated clearing house (ACH), retail wire transfers, wholesale payments, merchant remote deposit capture, treasury services, trust services, global remittance, correspondent banks, and merchant acquiring activities
- Organizational Characteristics: categories such as mergers and acquisitions, number of direct employees and cybersecurity contractors, changes in staffing, number of users with privileged access, changed in IT environment, locations of business presence, and locations of operations and data centers
- External Threats: considers the volume and sophistication of the attacks targeting the institution

The Inherent Risk is measured on a range of *Least Inherent Risk* to *Most Inherent Risk*. These measurements are given further definition within the CAT based on the specific risk being addressed.

Cybersecurity Maturity

Cybersecurity maturity assists management in measuring the institution's level of risk and corresponding controls. The maturity model includes statements to determine whether an institution's behaviors, practices, and processes can support cybersecurity preparedness within the following domains:



Domain 1: Cyber Risk Management & Oversight

- Governance
- Risk Management
- Resources
- Training & Culture

Domain 2: Threat Intelligence & Collaboration

- Threat Intelligence
- Monitoring & Analyzing
- Information Sharing

Domain 3: Cybersecurity Controls

- Preventative Controls
- Detective Controls
- Corrective Controls

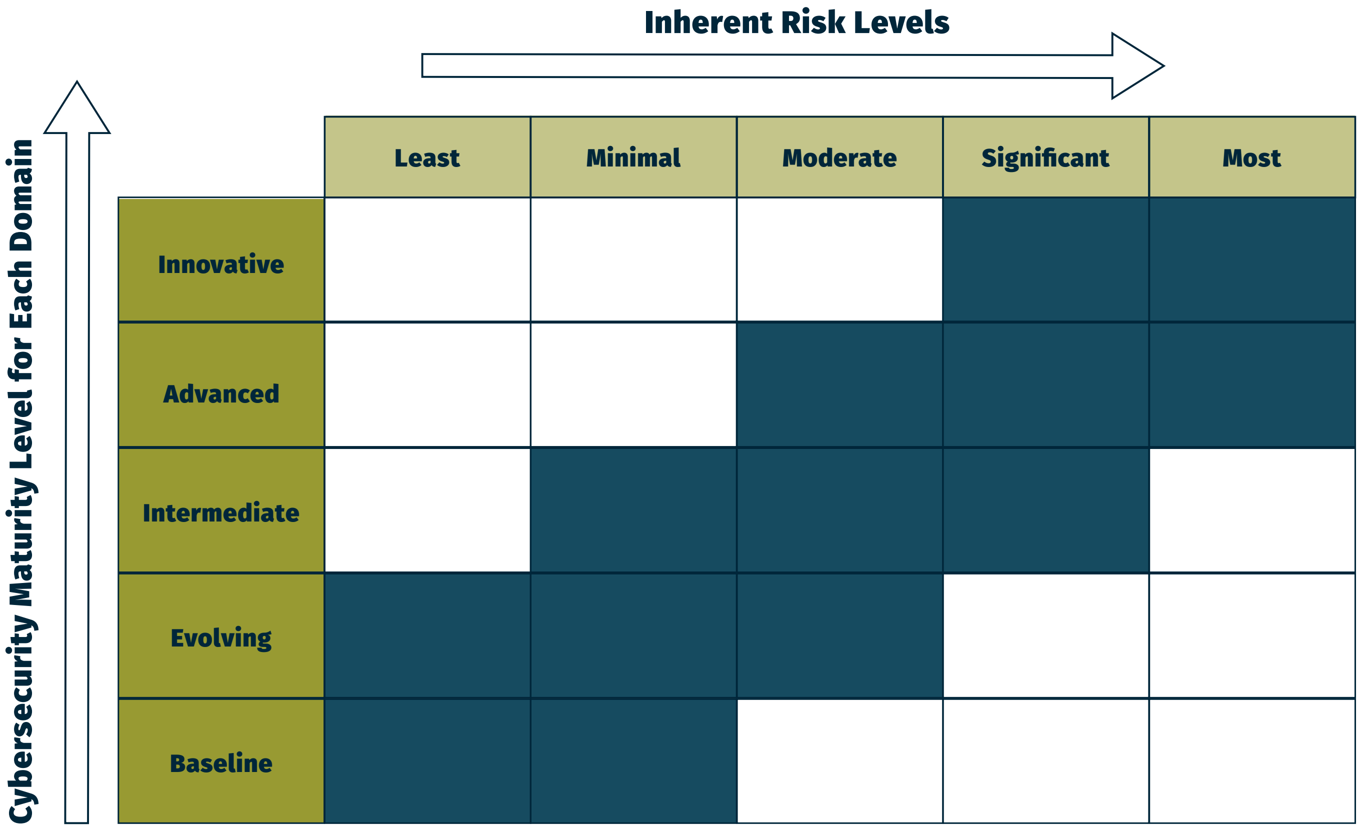
Domain 4: External Dependency Management

- Connections
- Relationship Management

Domain 5: Cyber Incident Management & Resilience

- Incident Resilience Planning & Strategy
- Detection, Response & Mitigation
- Escalation & Reporting

An institution is measured at a maturity level of *baseline, evolving, intermediate, advanced, or innovative*. All statements in each maturity level, and the preceding maturity levels, must be attained and sustained to achieve that domain's maturity level. In order to assess a domain at Intermediate, the organization would have to meet all declarative statements for Baseline and Evolving.



Inherent Risk Levels

Cybersecurity Maturity Level for Each Domain

	Least	Minimal	Moderate	Significant	Most
Innovative				■	■
Advanced			■	■	■
Intermediate		■	■	■	
Evolving	■	■	■		
Baseline	■	■			

In May 2017, the FFIEC released an updated Cybersecurity Assessment tool. While the Inherent Risk and the declarative statements stayed the same, there was one significant change used to further contextualize the Institution's control environment. The updated version included an additional answer of "Yes with Compensating Controls" as a response to declarative statements. This allows the institution to state they have met a declarative statement when the entire environment is taken into consideration, though certain controls may not be directly identified in the CAT.

Part 3: Data Flow Diagrams

A Data Flow Diagram (DFD) is a graphical depiction of the flow of data and information through a system. The word 'data' encompasses any unprocessed characters, text, words, numbers, etc. If data is processed into meaning then information has been created. Think about the statistics behind baseball. The number of plate appearances adds little value by itself. However, if the number of plate appearances is divided by the number of times a batter hits the ball, information has been created; the player's batting average. A DFD encompasses a combination of data and information flowing throughout the organization. It is important to note the term data in DFD ultimately includes both data and information.

The focus of a DFD is creating a pictorial representation of a business process, including those individuals and systems that interact with the process and the data and information involved. An individual should be a department or title rather than an individual name. The use of an individual's name would cause for errors in the DFD if the person left the organization, changed roles, or additional individuals interact with the process. There are a few key distinctions between a DFD and other common diagrams and flow charts.

- There is no start or end symbol. Rather it presents the external sources of –or destinations of- the data.
- There is a limited set of elements and symbols used to visualize the process. These are universal across all DFDs.
- Data stores or system files are shown along with the data that flows into and out of them
- Specific data elements and/or data categories are identified as they move between entities, processes, systems, and data stores

The payroll process is a common process understood and experienced by most organizations. Let us use this as an example to talk through the various elements of a data flow diagram. It is important to keep scope in mind as this is being developed, or the diagram can become very detailed very quickly.

When writing a paper, planning a meeting, going on a trip, the best place to start to keep focused is an outline or agenda. This applies equally with a DFD diagram. The technical term for this type of diagram is a Context Diagram, which is limited to the process, indicated by a larger circle, the entities, and the data flowing into and out of the circle by the entities. Having identified what the process is going to be, Payroll Process, what or who interacts with this process?

- Employees submit hours, declare deductions, receive a check
- Human Resources enter employees into the application and setup deductions (healthcare, dependents, retirement, etc.)
- Managers approve time
- Federal/State Government receive taxes
- Financial Investment firm manages the retirement allocations
- Health Insurance company receives payment for employee health plan

These are all examples of individuals, departments, and outside organizations that interact with the Payroll process. There will also be systems that will receive the payroll role information:

- Time Entry system (time clock, time and attendance application, etc.)
- Financial System maintains Salaries and Wages Expense
- Systems used to communicate with Financial Institutions to complete direct deposit
- Tax calculation software
- Health insurance systems used to track Health Savings Accounts

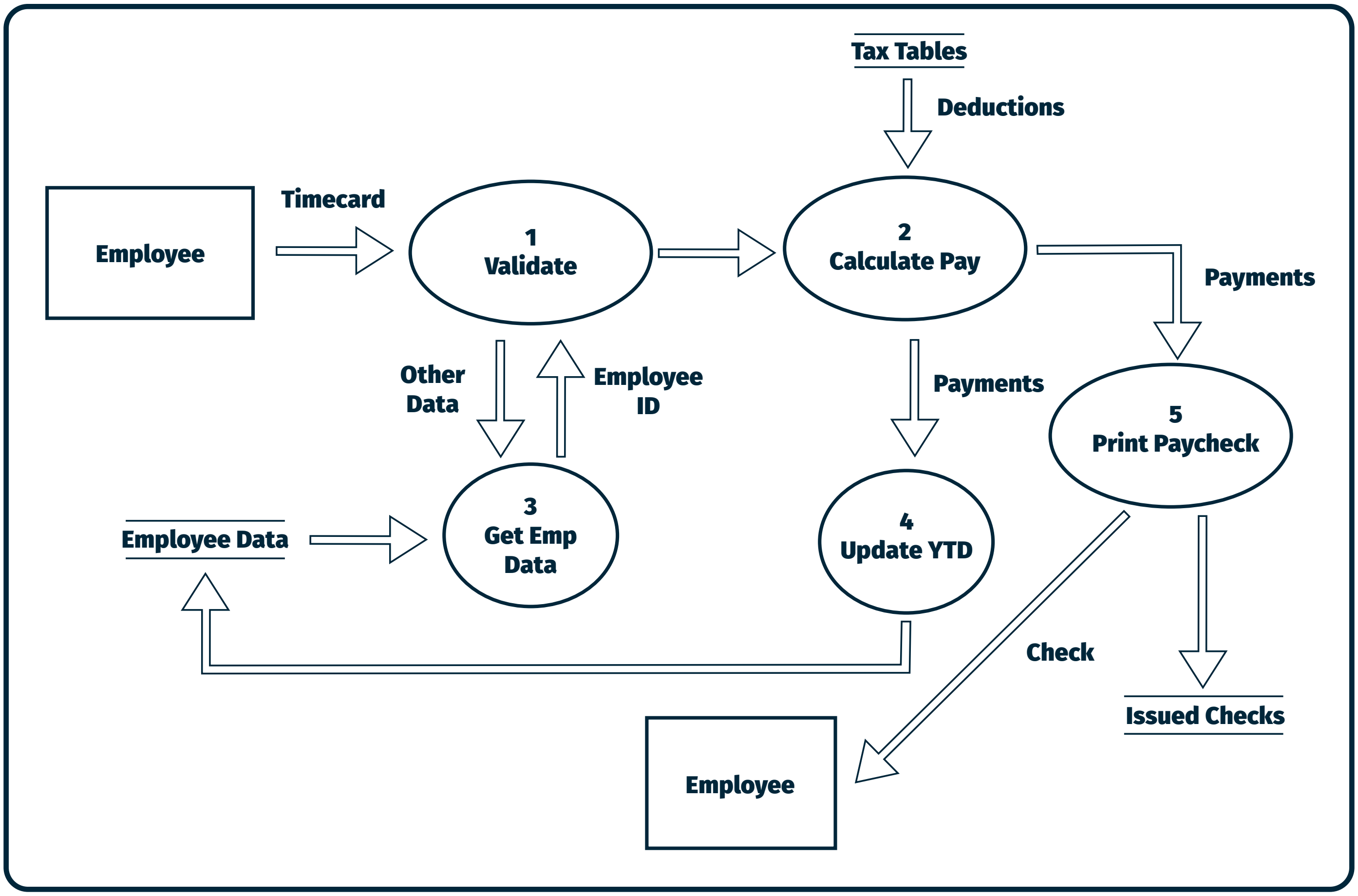
The next question is where does all the data reside? Some of these are going to be obvious because they are internally stored. Others are going to be more complex as it involves a 3rd party. It will be important to reach out to these 3rd parties in a real data flow diagram to ensure a complete picture.

- Internal/Hosted payroll system database
- General Ledger database
- Excel/PDF files on a network drive
- Embedded in the Financial Investment firm’s website, stored on a server controlled by the organization

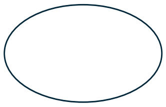
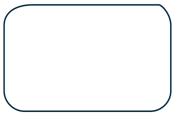
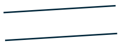
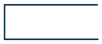
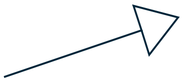
The last thing that needs to be done, is to evaluate all of the data that is flowing between these entities and data stores. Data cannot flow directly from an entity to a data store. It has to flow through a process. It is worth stopping here and noting that for as relatively simple as the payroll process is, the complexity of this project is already mounting, but we have not even drawn a circle on a page. Furthermore, we have yet to address network communication and data encryption. This is one of the main reasons there is a fear of moving forward with data flow diagrams. How do we effectively limit its scope?

The agenda, or Context Diagram, is simply a big circle on a page with lines going in and out to the different entities and systems noted above. That large circle is then broken down into a Level-1 Diagram. The current Context Diagram will be broken down into individual processes as a more detailed understanding is identified. The desired result is a well-developed Level-1 Diagram.

The following diagram is an example Level-1 Data Flow Diagram. It is not nearly as complex as our example above could have been. The diagram shows the external party (employee) and data stores (Tax table, Emp. Data and Issued cheques). Note all of the processes in the middle are verbs. This is a key characteristic of a DFD.



This chart identifies and describes the universal symbols used within a DFD. All of them are easy to create in Microsoft Word, Excel, or Visio.

Element	Description	Symbol
Buisness Process	The activities with a systems that use or generate data	
Entity or Data Source / Hardware	The entities that interact with the system (e.g., customers, employees, vendors, technology)	
Data Store or Data File	Physical and electronic data storage	 OR 
Data Flow	The flow of data identified with a directional arrow	

Several best practices to help guide the development of a successful diagram:

- A title and short description should be included at the top of the diagram. This will help quickly identify the information included.
- A process starts with a verb
- An entity is a noun
- Every entity must be connected with at least one data flow
- Each line must have a directional arrow to identify how the data is flowing from one entity to another
- Arrange the data flow arrows so they do not cross each other. The diagram will become confusing if the arrows are not easy to follow.
- Every data store should have data flowing into it and data flowing out of it.
- The diagram should fit on a single page and be limited to five to seven processes. A diagram that gets too granular or includes too many processes will become hard to follow.   This is simply a suggestion, not a requirement of the DFD.
- Limit symbols to the four identified above.

We have identified a process that we believe helps develop the critical data flow diagrams and maintain a reasonable size and scope. The process is outlined below with a practical example to explore.

Data Flow Diagram References

With the technical walkthrough of a data flow diagram complete, let us look back at the cybersecurity tools discussed above, and focus in on their references to data flow diagrams or areas that may impact a data flow diagram.

The FFIEC and NIST are only two of the sources that indicate the importance of developing data flow diagrams. A quick search online will yield several other governing bodies that have identified their importance. Below are several references extracted from documentation and guidance developed by both organizations.

FFIEC IT Handbook – Information Security Booklet

Section	Action Summary	YHB Comments
II.C.9 Network Controls	Management should secure access to computer networks through multiple layers of access controls by doing the following: • Establishing zones according to risk profile and criticality of assets • Maintain accurate network diagrams and data flow charts • Implementing appropriate controls over wired and wireless networks	As new technologies are brought into the organization and vendors are changed, it is important to reassess the data flow diagrams. They are not meant to be a one-time exercise that is never revisited.

Section	Action Summary	YHB Comments
Network Components and Topology	Management should also develop data flow diagrams to supplement its understanding of information flow within and between network segments as well as across the institution's perimeter to external parties. Data flow diagrams should identify: • Data sets and subsets shared between systems; • Applications sharing data; and • Classification of data (public, private, confidential, or other) being transmitted. Data flow diagrams are also useful for identifying the volume and type of data stored on various media. In addition, the diagrams should identify and differentiate between data in electronic format, and in other media, such as hard copy or optical images	The FFIEC is trying to further guide the important information to be included: data stores, applications/system, and type of data.

Domain	Description	FFIEC IT Handbook Reference
4 – External Dependency Management	**Connections/Connections**: The critical business processes that are dependent on external connectivity have been identified.	**IS.B.9:** The institution's system architecture diagram should include a system characterization and data flow analysis of networks (where feasible), computer systems, connections to business partners and the Internet, and the interconnections between internal and external systems.
4 – External Dependency Management	**Connections/Connections:** Data flow diagrams are in place and document information flow to external parties.	**IS.B.10:** Financial institutions outsourcing strategy also should be considered in identifying relevant data flows and information processing activities. The financial institution's system architecture diagram and related documentation should identify service provider relationships, where and how data is passed between systems, and the relevant controls that are in place.

NIST Cybersecurity Framework

Category	Sub-Category	YHB Comments
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-3:** Organizational communication and data flows are mapped
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected, and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed

Note: DE.AE-1 is specifically included because this supports one of the main reasons a data flow diagram should be developed. In the event anomalous activity is detected, a data flow diagram in conjunction with a network diagram will help speed up the process in understanding the impact.

NIST 800-53

Technical Access Control	Selected Description	YHB Comments
AC-4 Information Flow Enforcement	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information	NIST 800-53 AC-4 clearly identifies why a network diagram is not enough. A network diagram is not going to identify the information that is flowing between systems.
CA-2 Baseline Configuration	The organization develops, documents and maintains under configuration control, a current baseline configuration for the information system. Maintaining the baseline configuration involves creating new baselines as the information system changes over time.	Again, as configurations change it is important to revisit these diagrams and update them as needed.
CA-3 Information System Connections	The organization carefully considers the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within the organization and external to the organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the information systems.	This may help frame a discussion around encryption of data (at rest and in transit) when determining how applications (internal and external) interface and what controls need to be put into place.

Part 4: Addressing the "Why?"

Information asset protection, as clearly noted above, is critical in an institution's cybersecurity landscape. Information includes, but is not limited to, customer data, employee data, financial data and transactions, propriety systems and data, etc. Senior leadership, board of directors, employees, customers, 3rd party vendors, and governing and regulatory entities all have a vested interest in protecting this information. It is incumbent on the institution to develop the right controls to do this.

Data flow diagrams will help the institution identify potential weaknesses within the interconnectivity of internal systems and 3rd party entities. They will help identify the location of critical data and pinpoint keys places to ensure data is properly encrypted at rest and in transit. In the context of the FFIEC CAT, DFDs will help open a dialog with 3rd party entities to ensure the protection of the organization's data as it transverses the external environment and storage on devices that may be hosted within the physical infrastructure of the 3rd party or at some unknown location in the cloud. We find it extremely important to open these communications with you vendors so as to gain this understanding of how and where data is stored. Generally, consumers expect the company to have an understanding of where their data resides, and how it is being protected. They will not accept a failure to fully understand data ownership even though it is hosted by a vendor.

From a practical standpoint, the DFD is important because one has to be developed in order to meet baseline in Domain 4: External Dependency Management of the FFIEC CAT. The FFIEC Baseline Declarative Statement reads "Data flow diagrams are in place and document information flow to external parties." Based on this declarative statement, Intermediate cannot be achieved until all Baseline statements have been met. As such, Advanced cannot be met until all Intermediate statements have been fully implemented. The FFIEC Intermediate Declarative Statement reads "A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure and connectivity."

Neither Baseline nor Intermediate can be met by creating a network diagram alone. A network diagram focuses on the hardware assets, to varying levels of detail, and the path in which traffic flows between them. They do not address a business process, the actual data that flows between those processes, systems involved, or the applicable 3rd party entities. They do not address encryption of data through a process.

Part 5: Practical Implementation Guide

The following outlines a path to create a successful data flow diagram. Depending on the organizations current maturity, this can be a simple addition to the existing plethora of tools or a time intensive set of steps. Regardless, we recommend each topic be addressed, taking careful consideration of the size and complexity of the institution. The topics are discussed in their order of importance to help create a mature cybersecurity model.

Risk Assessments

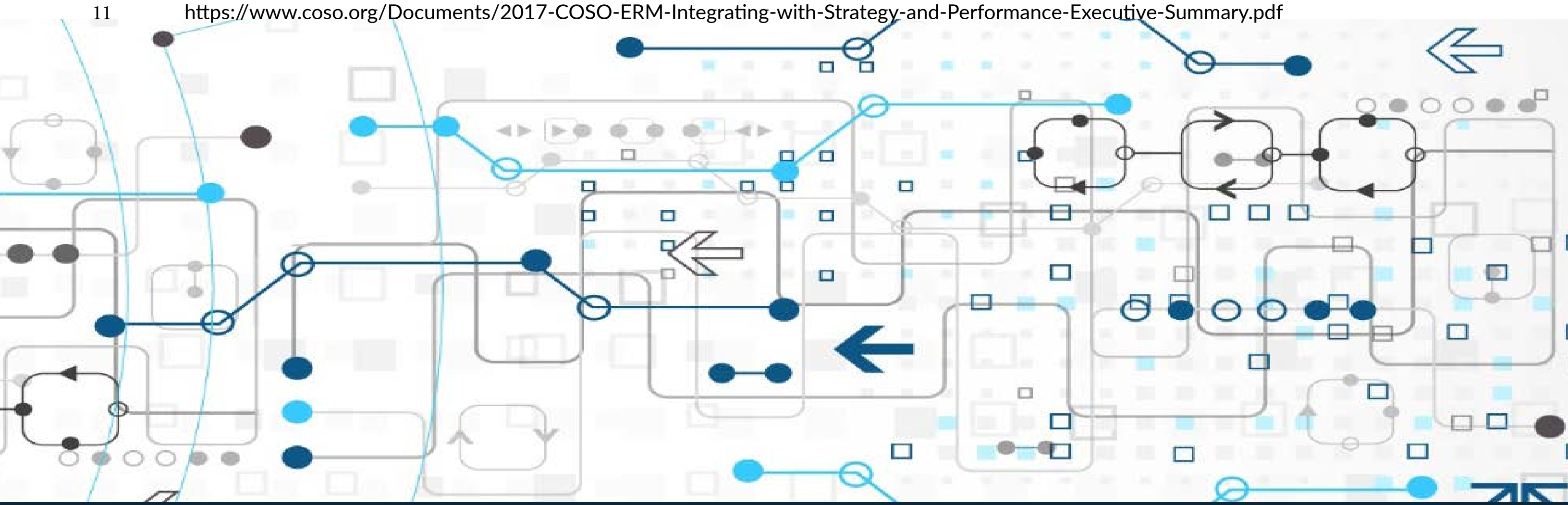
The most common concern we hear around the scope of a DFD, is how detailed does a data flow diagram need to be. A secondary concern might be around the number of data flow diagrams that need to be created. We cannot make this clear enough; the process is not one size fits all. Assuming the general organization is fully understood, the starting point should be a comprehensive risk assessment. A great source to peruse is the NIST Special Public 800-30 – Guide for Conducting Risk Assessments. The formal methodology of developing any of the following risk assessments goes beyond the scope of this paper.

Enterprise-wide Risk Management

Enterprise risk management (ERM) is defined by COSO as the "process of planning, organizing, leading, and controlling the activities of an organization in order to minimize the effects of risk on an organization's capital and earnings."[11] While this is ultimately the responsibility of management, true ERM must be driven from the top downward. A tone at the top, if you will. Because of the breadth of ERM, we will focus here on those aspects most importantly considered in the information and technology realm:

- The Board of Directors – In following with their charge of governance of the organization, the Board is responsible for proposing strategy, business objectives, and an overarching risk appetite. These should be established so that they meet the organizations stated mission, vision, and core values.

[11] https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf



- Management – Though the Board of Directors is responsible for the final determination of strategy and business objectives, it is the responsibility of management to provide them with the necessary information to make those decisions. And once the strategy and objectives have been established, ensuring their implementation and performance.
- Employees – As the front line of the organization, employees are the first to see and interact with customers. They drive heart of the business, and as a result, are responsible for carrying out the steps needed to complete business objectives.

All parties are responsible for information, communication, and reporting between each level. Without this step, the optimum goal of ERM, Enhanced Value, will never be reached.

Vendor Management

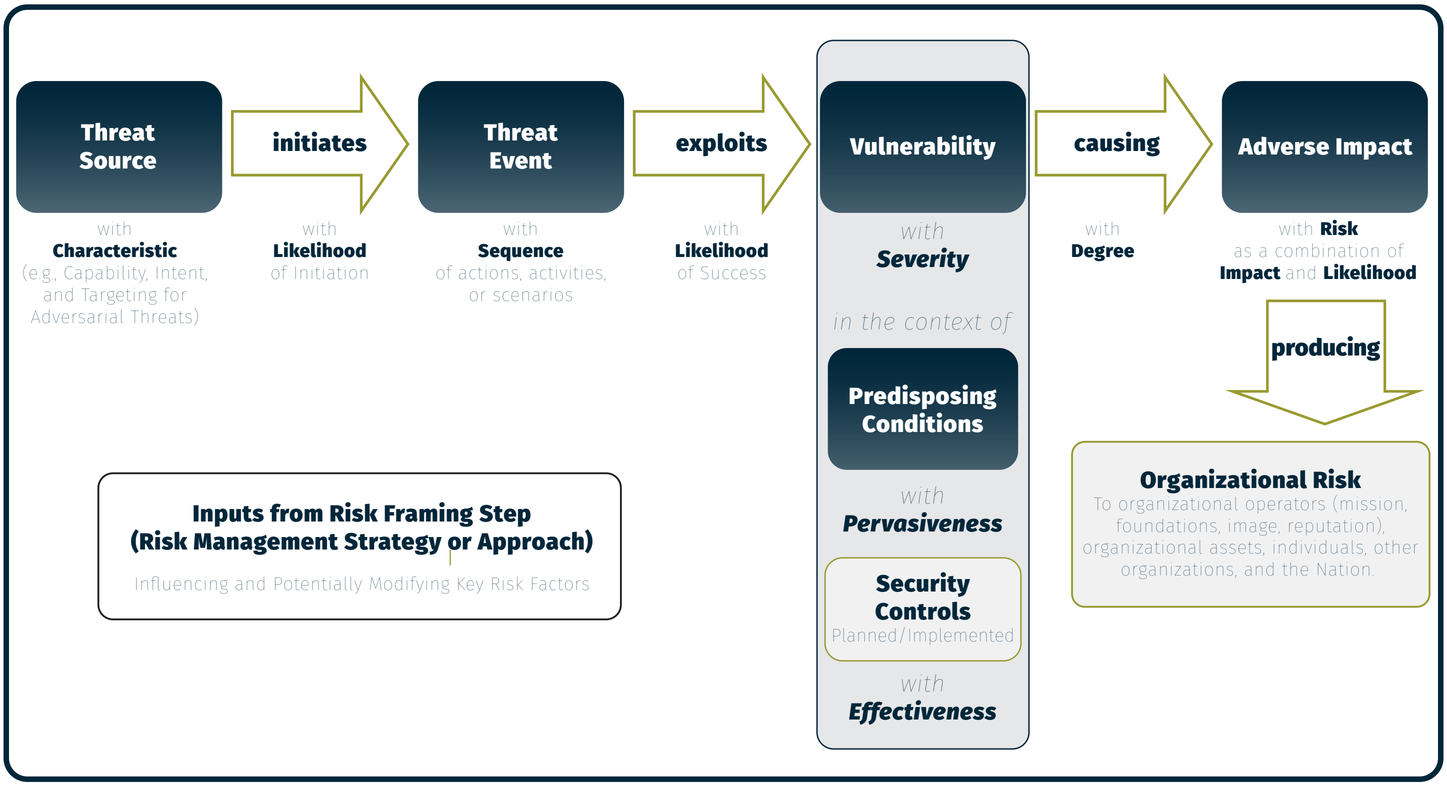
The FFIEC CAT clearly states “information flow to external parties” are of baseline maturity level. Therefore, in order to consider the flow to external parties, identifying those parties is very important.

- Catalog all vendors. While all vendors may not be financially significant or highly impactful to the business (i.e. landscaping services or cleaning service) the entities still pose some level of risk.
- Profile each vendor. This should include the company name, address, key contacts, service provided, contract renewal dates, total expenses, etc. Grouping types of services provided may help to identify and isolate the critical vendors.
- Define criticality of the vendor. A common set of evaluation points include: strategic, operational, financial, reputational and regulatory risk.
- Assign inherent risk. The profile of each vendor will assist in assigning an inherent risk to the vendor. That is to say the risk of the vendor prior to the application of controls.
- Identify internal controls related to each vendor. Note: formalized controls may not be in existence for all low-risk vendors.
- Assign residual risk. After determining the inherent risk and controls in place, a final residual risk can be assigned.

There are many white papers and vendors who can assist in establishing a quality vendor risk management program. Questionnaires are especially useful when determining what the residual risk for each vendor. Critical vendors should be evaluated on an annual basis. Non-critical vendors can be assessed on a rotating basis.

Cybersecurity

NIST defines five key functions within its Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. The first component, Identify, includes a number of subcategories, many of which are vital to ERM and Vendor Management. Just as important of a subcategory is the risk assessment process. The core focus of the cybersecurity risk assessment is to identify, mitigate and manage the risks around digital assets. As with all risk assessments, identifying the inherent amount of risk presented, the organizations corresponding controls, calculating the residual risk after implementing mitigating controls, and determining whether this remaining risk is acceptable are required.


Threat Source
with Characteristic (e.g., Capability, Intent, and Targeting for Adversarial Threats)
initiates
with Likelihood of Initiation
Threat Event
with Sequence of actions, activities, or scenarios
exploits
with Likelihood of Success
Vulnerability
with Severity
in the context of
Predisposing Conditions
with Pervasiveness
Security Controls Planned/Implemented
with Effectiveness
causing
with Degree
Adverse Impact
with Risk as a combination of Impact and Likelihood
producing
Organizational Risk
To organizational operators (mission, foundations, image, reputation), organizational assets, individuals, other organizations, and the Nation.
Inputs from Risk Framing Step (Risk Management Strategy or Approach)
Influencing and Potentially Modifying Key Risk Factors

NIST Special Publication 800-30 Revision 1 – Guide for Conducting Risk Assessments

Once each risk assessment has been addressed, the scope of data flow diagrams will begin to become evident. The intersection of corporate governance, vendor management, and cybersecurity risks is a great starting point. Hopefully this will outline the key business processes, vendors, and cybersecurity risk landscape within the organization.

The next few categories can be performed in any order. Serious consideration should be given to create each list. There are tools that will help in identifying a comprehensive list of each area. As a default, each asset list (hardware, software, and data) should have an assigned priority level or risk level.

Hardware Asset List

A hardware asset list should include all computers (workstations and servers), mobile devices, network equipment (routers, firewalls, etc.), electronic storage devices (external hard drives, USB drives, etc.), printers, scanners, and any other physical asset that may store or come in contact with the organization's data. A best practice with hardware is to give each piece of equipment an asset tag. If the hardware is on the network and has a static IP address, documenting the IP address will also be useful.

Asset management seems to be an area many organizations push to the back burner. All too often an asset has reached end-of-life and there is an intense push to obtain funding, acquiring new hardware, and prioritizing implementation. Include projected end-of-life and projected replacement dates for each piece of equipment.

Software Inventory

Each organization often has a set of approved applications. The scope typically includes financial applications, fixed contract applications, and licensed applications. Unless a workstation is wiped prior to being distributed, the vendors typically install baseline and sometimes-proprietary software applications. To further complicate the process of obtaining a comprehensive list of applications installed on company owned devices or devices connected to the network, some organizations choose to grant employees local administrative rights. This allows employees to install their preferred, as oppose to pre-approved, applications.

As noted above with the hardware, documenting the end-of-life for software is important. After a certain timeframe, a vendor will no longer provide support for a version of their software. This will introduce unwarranted risk when zero-day vulnerabilities are identified and the vendor will not provide a patch. Tracking the current patch level of applications installed on workstations will help assist in the patch management process.

Data Inventory

Business data will not necessarily reside on all hardware or within all applications documented on the prior two asset lists. However, those are great starting points for determining the scope of data inventory. Within the context of this white paper, a data inventory list can be kept relatively high-level.

The data inventory list includes the type of data, how it is stored (database, file server, etc.), and who the business owner is. Unless it is IT-related data, the IT department should not be the data owner. The IT department may manage the hardware or database it resides on, but they are not the daily users of the data.

Once each of these comprehensive asset lists are in place and risk assessments completed, the support functions (often the IT Department) will have a full picture of the organization. The scope of the data flow diagrams will begin to come into focus.

At this point, revisit the section on Data Flow Diagrams and begin to put into practice the concepts there-in with the assistance of the exhaustive set of risk assessments and asset lists. The level of detail on each DFD will depend on the complexity of the organization's business.

It is important to keep in mind that regardless of where applications and/or data resides (internally or hosted) it still belongs to the organization, especially in the customer's mind. Therefore, the organization should not draw a line at the point at which the data leaves the internal network and take no ownership once it is in the hands of a 3rd party.

Part 6: Data Flow Diagram Example

The following data flow diagram shows the high-level relationship between a Bank and two vendors during the Payroll process. The initial risk assessments were:

Environments:

1. Bank Internal Network protected by a Cisco Firewall with Secureworks IDS & Monitoring
2. ADP Payroll System – hosted by ADP
3. Citrix ShareFile – hosted by Citrix

Entity or Data Source

1. Human Resources Department
2. Accounting Department

Processes

1. Initiate Payroll Processing

   Human Resources collects employee data and uploads the data to ADP, the payroll processing vendor, to process payroll

2. Download Employee Data from ADP

   Human Resources downloads select employee data, from ADP, to their local Workstation

3. Save the Employee Data to the HR internal Network Share Drive

   Human Resources saves the downloaded information from their Workstation to the HR Network Drive

4. Send Employee Report, through ShareFile, to Accounting

   Human Resources sends select Employee data via ShareFile, encrypted email software. The encrypted file will reside on a server at Citrix and will be available for download by the Accounting department

5. Download Employee Report, from ShareFile, to Accounting workstations

   Accounting downloads the Employee data from ShareFile to their local Workstations

6. Save the Employee Report to the Accounting internal Network Share Drive

   Accounting copies the Employee data from their Workstation to the Accounting Network Drive

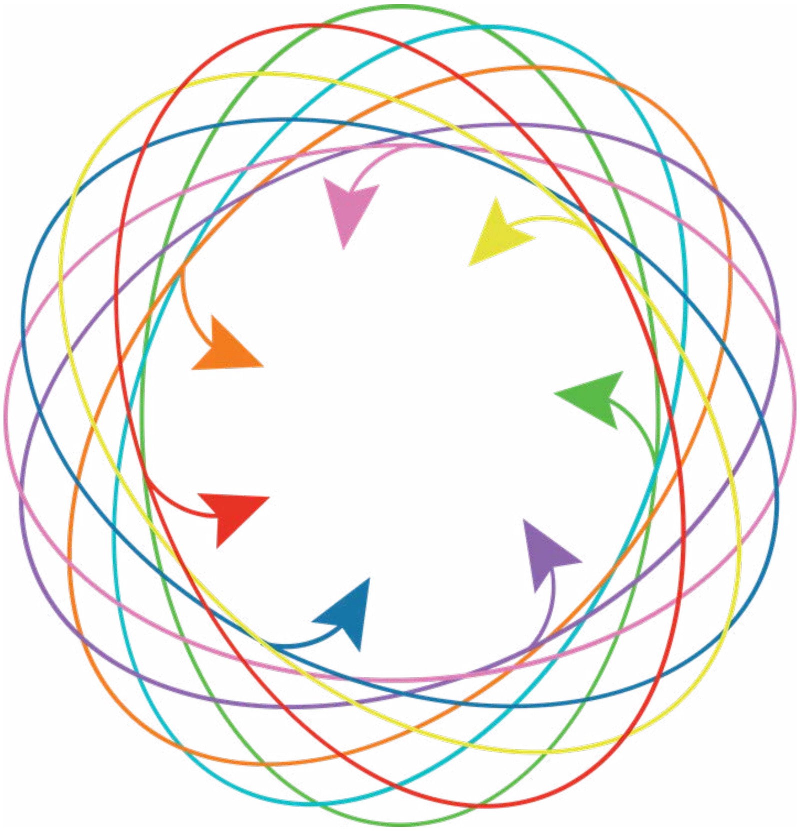
Data Store (Encrypted data-at-rest)

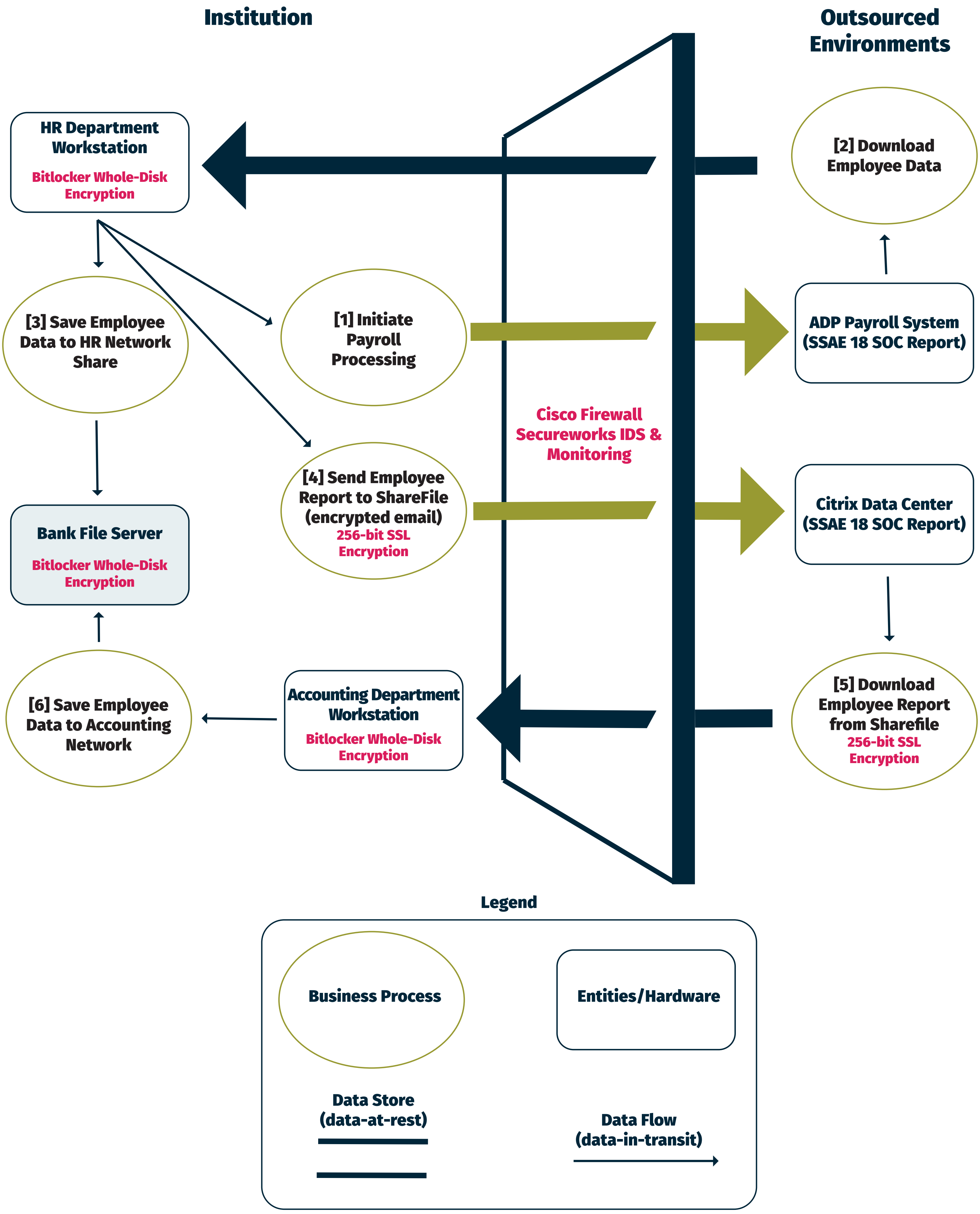
1. File Server with an HR network drive and Accounting network drive
2. ADP Payroll database
3. Citrix database

Data Flow (Encrypted data-in-transit)

The following data flows are an example of data that may flow through each process described above?

1. Employee name, Employee number, Hours worked, Pay rate
2. Employee name, Employee number, Employee address, Employee SSN, Employee manager, Pay rate
3. Employee name, Employee number, Employee address, Employee SSN, Employee manager, Pay rate
4. Employee Report with total pay, withholdings, and hours worked by category
5. Employee Report with total pay, withholdings, and hours worked by category
6. Employee Report with total pay, withholdings, and hours worked by category





Institution

Outsourced Environments

HR Department Workstation
Bitlocker Whole-Disk Encryption

[3] Save Employee Data to HR Network Share

[1] Initiate Payroll Processing

[4] Send Employee Report to ShareFile (encrypted email)
256-bit SSL Encryption

Bank File Server
Bitlocker Whole-Disk Encryption

[6] Save Employee Data to Accounting Network

Accounting Department Workstation
Bitlocker Whole-Disk Encryption

Cisco Firewall Secureworks IDS & Monitoring

[2] Download Employee Data

ADP Payroll System (SSAE 18 SOC Report)

Citrix Data Center (SSAE 18 SOC Report)

[5] Download Employee Report from Sharefile
256-bit SSL Encryption

Legend

Business Process

Entities/Hardware

Data Store (data-at-rest)

Data Flow (data-in-transit)

We found several important questions to explore while creating this diagram.

External Vendors

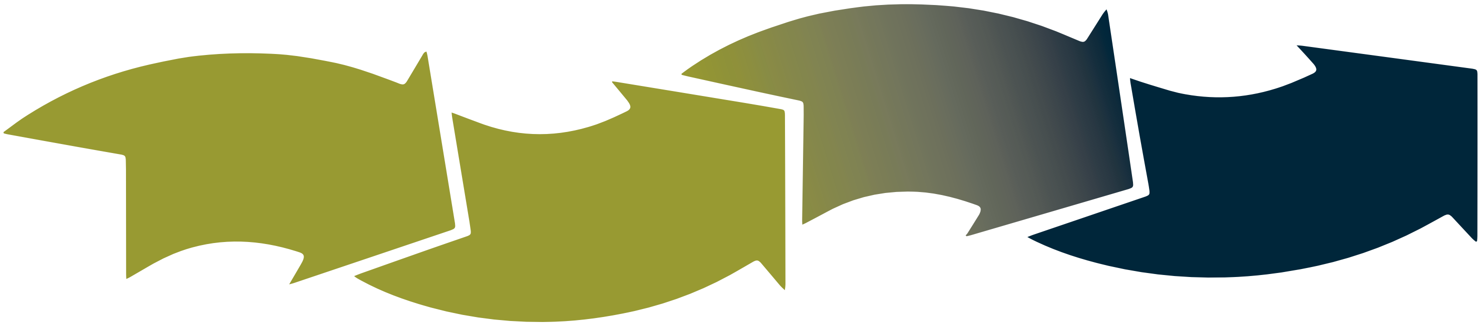
- Is there a SSAE 18 report available for review? What were the results?
- How is data stored by the 3rd party? Is the data properly encrypted?
- What other processes are supported by these vendors?
- What is the technical infrastructure of the vendor? What type of database is used?
- What are the specific applications used by the vendor for this process?

Internal

- Is data retained locally on the HR and Accounting workstations?
- Are the workstations properly patched?
- Is anti-virus installed on the workstations and is it up to date?
- Do the files exist outside of the HR and Accounting network shares?
- Is the file server encrypted? Are the workstations encrypted?

Data Flow

- How is the data encrypted while moving internally and externally?
- What confidential data is flowing through each process?
- What is the scope of data flowing through each process?



Part 7: Conclusion

Data flow diagrams have risen in visibility over the past few years. Organizations like the FFIEC and NIST, have brought awareness to how they can impact an institutions overall cybersecurity maturity. An organization's cybersecurity maturity is paramount in the protection of one of its greatest assets, customer data. Loss of or breach of customer data will ultimately result in a loss of consumer confidence, which hurts the organization's reputation and bottom line. Utilizing data flow diagrams has, consequently, become not just a recommendation, but in many cases a regulatory requirement. Their ability to depict the storage, flow, and protection of information provides a valuable tool in creating a safe and guarded data environment.

Acknowledgments

Risk Advisory Services

YHB's Risk Advisory Services team provides you the tools to make your information technology and internal controls work for you. Your IT controls should protect your data, and more importantly your clients' data in a way that it is secure, available, and accurate. Internal controls outside of IT should also protect your assets from fraud and errors. RAS can provide a thorough review of your controls by experienced professionals. We are CPAs that have devoted our career to Information Technology and internal controls.

Learn more at yhbcpa.com

Lead Author:
Stephen Weber, MBA, CISA | Manager
stephen.weber@YHBcpa.com | 804.553.1900

Stephen has extensive experience in IT Audit and Advisory Services. His background includes internal and external IT Audit services for state and federal agencies and Fortune 500 companies in retail, manufacturing and financial lending. His expertise spans financial statement audits, SOX, project management, legal and compliance and data analytics. To further his commitment to IT Security, Stephen has also completed the ISACA®'s Cybersecurity Audit Certificate Program.

Expert Contributors:
Brad Brosig, CISA | Manager
Bryan Newlin, CPA.CITP, CISA | Principal
Curtis Thompson, CPA.CITP, CISA | Principal