SBS CyberSecurity

\VENDOR MANAGEMENT/ \IN 2025/

HOW TO MAKE GOOD VENDOR MANAGEMENT DECISIONS

SBS CyberSecurity

CONTACT INFORMATION

JON WALDMAN

- President, Partner
- CISA, CRISC, CDPSE
- Master's of Information Assurance, Dakota State University
- Mission: help you make better cybersecurity decisions
- Phone: 605-380-8897
- jon@sbscyber.com
- www.sbscyber.com

WHAT WE'LL EXPLORE TODAY

1. VENDOR RISK ASSESSMENT
2. VENDOR LEVELS
3. ONGOING VENDOR MANAGEMENT
4. OTHER WAYS TO MANAGE VENDOR RISK
5. SELECTING BETTER VENDORS
6. SUPPLY CHAIN MANAGEMENT/ 4TH PARTY MANAGEMENT

DOWNLOADS & MORE!

- HEAD TO OUR LANDING PAGE AND DOWNLOAD SOME GOODIES!
- INCLUDING:
- CHANCE TO WIN A FREE SBS INSTITUTE WEBINAR OR MEMBERSHIP!
- THIS PRESENTATION'S SLIDE DECK!
- PRESENTATION SURVEY - WE LOVE FEEDBACK! TELL US HOW WE DID!
- FREE DOWNLOADS - 6 ISP/VM IDEAS AND TEMPLATES WE DISCUSSED TODAY!
- SIGN UP FOR IN THE WILD!

HTTPS://SBSCYBER.COM/RVASEC

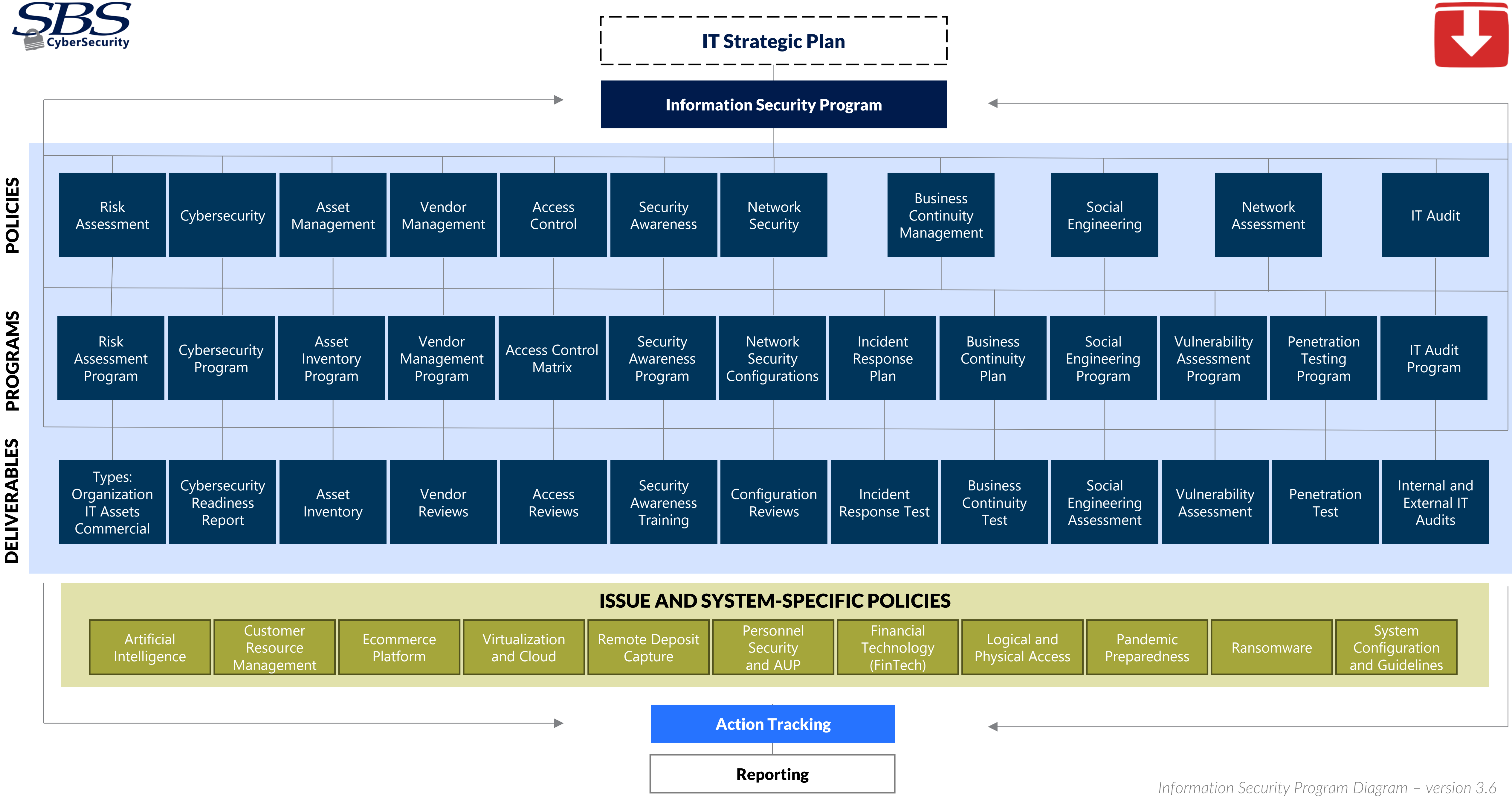
Building a Modern Vendor Management Program

SBS CyberSecurity

"CYBERSECURITY IS MORE THAN A TECHNOLOGY ISSUE. IT IS A BUSINESS ISSUE."

- GINNI ROMETTY, FORMER IBM CEO

SBS CyberSecurity



IT Strategic Plan

Information Security Program

POLICIES

- Risk Assessment
- Cybersecurity
- Asset Management
- Vendor Management
- Access Control
- Security Awareness
- Network Security
- Business Continuity Management
- Social Engineering
- Network Assessment
- IT Audit

PROGRAMS

- Risk Assessment Program
- Cybersecurity Program
- Asset Inventory Program
- Vendor Management Program
- Access Control Matrix
- Security Awareness Program
- Network Security Configurations
- Incident Response Plan
- Business Continuity Plan
- Social Engineering Program
- Vulnerability Assessment Program
- Penetration Testing Program
- IT Audit Program

DELIVERABLES

- Types: Organization IT Assets Commercial
- Cybersecurity Readiness Report
- Asset Inventory
- Vendor Reviews
- Access Reviews
- Security Awareness Training
- Configuration Reviews
- Incident Response Test
- Business Continuity Test
- Social Engineering Assessment
- Vulnerability Assessment
- Penetration Test
- Internal and External IT Audits

ISSUE AND SYSTEM-SPECIFIC POLICIES

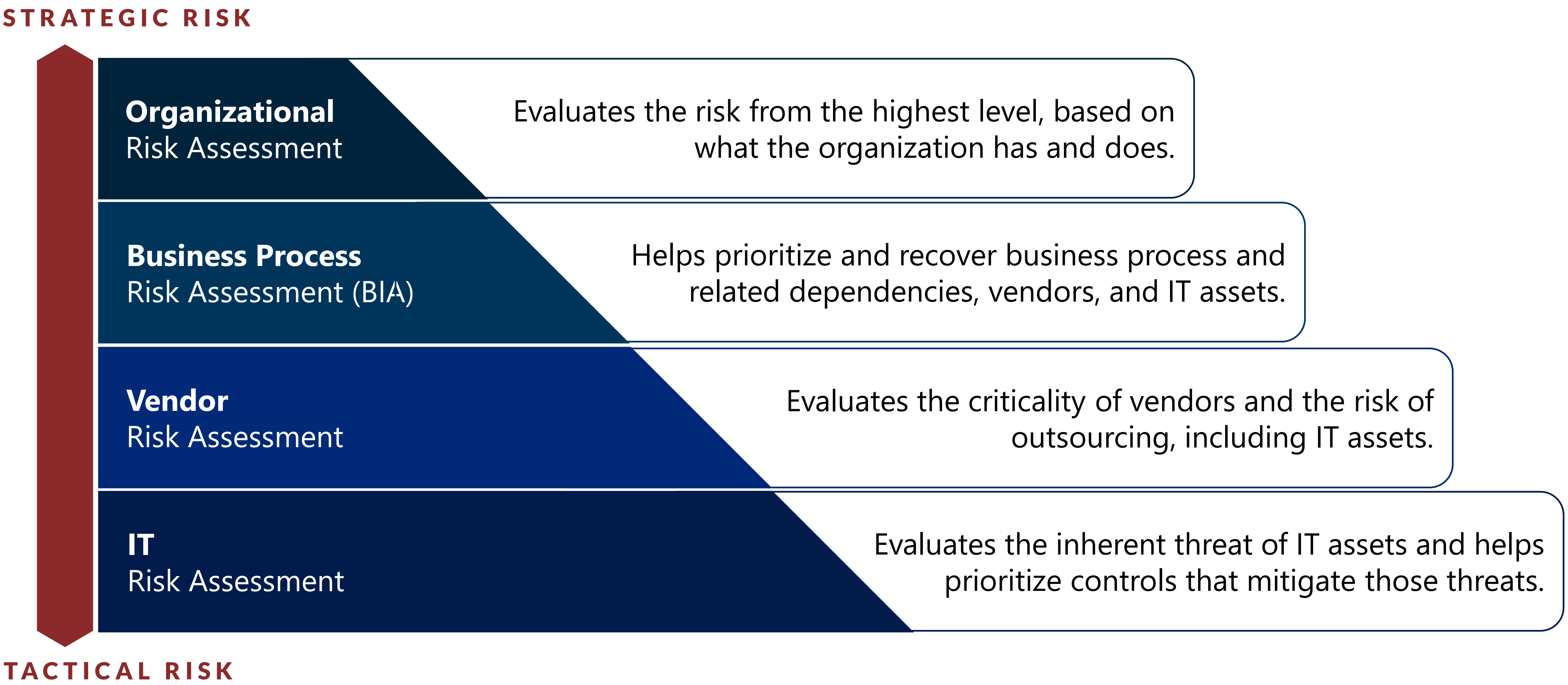
- Artificial Intelligence
- Customer Resource Management
- Ecommerce Platform
- Virtualization and Cloud
- Remote Deposit Capture
- Personnel Security and AUP
- Financial Technology (FinTech)
- Logical and Physical Access
- Pandemic Preparedness
- Ransomware
- System Configuration and Guidelines

Action Tracking

Reporting

Information Security Program Diagram – version 3.6

RISK MANAGEMENT HIERARCHY



STRATEGIC RISK

Organizational
Risk Assessment

Evaluates the risk from the highest level, based on what the organization has and does.

Business Process
Risk Assessment (BIA)

Helps prioritize and recover business process and related dependencies, vendors, and IT assets.

Vendor
Risk Assessment

Evaluates the criticality of vendors and the risk of outsourcing, including IT assets.

IT
Risk Assessment

Evaluates the inherent threat of IT assets and helps prioritize controls that mitigate those threats.

TACTICAL RISK

3 MAJOR COMPONENTS OF MODERN VENDOR MANAGEMENT

VENDOR RISK ASSESSMENT

- Your risk assessments MUST help you make better decisions
- Identify Vendor Risk
- Identify Vendor Levels

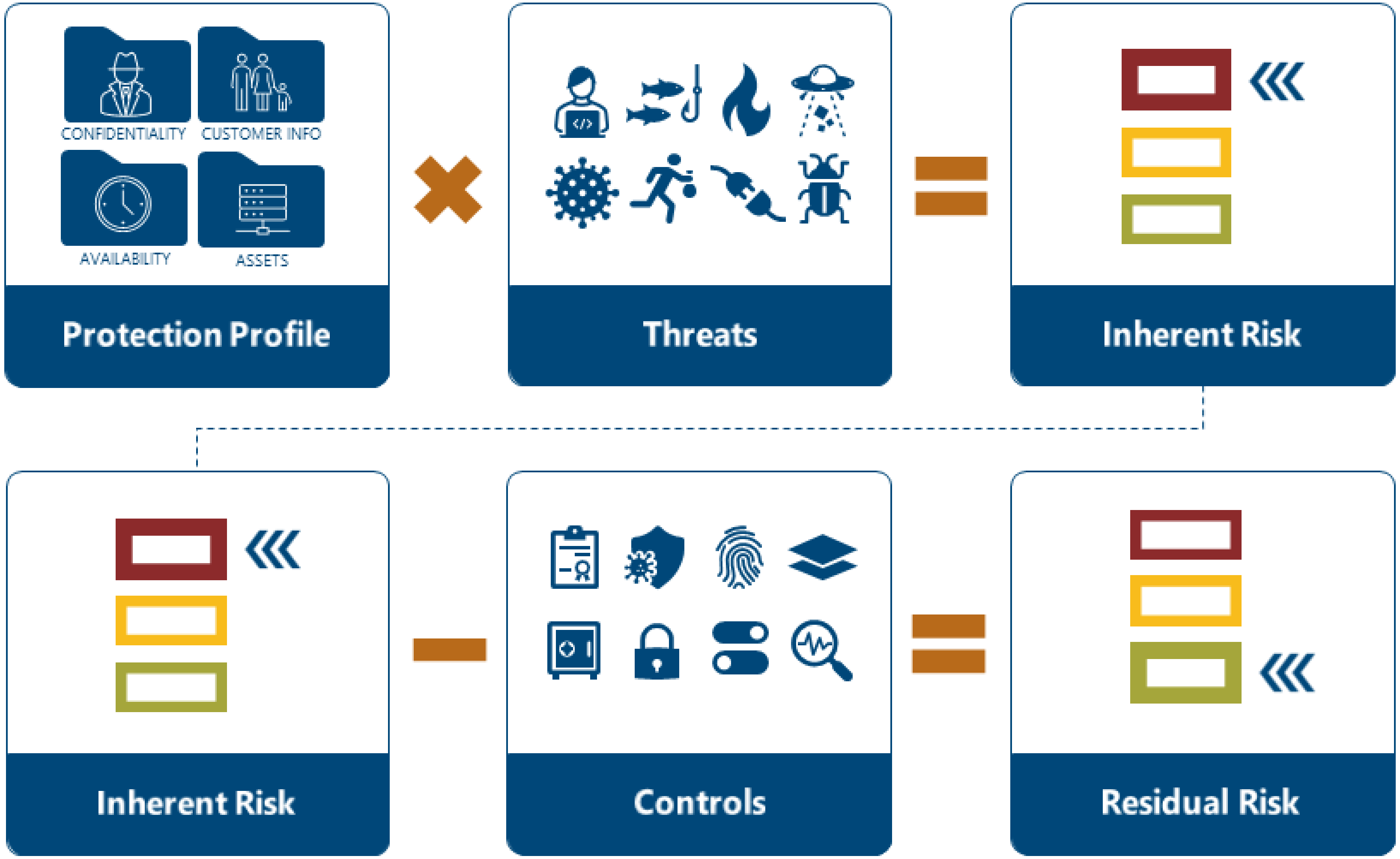
VENDOR SELECTION

- Based on Vendor Level
- Contract Review
- Due Diligence
- Metrics

ONGOING MANAGEMENT

- Based on Vendor Level
- Contract Review
- Due Diligence
- Metrics

RISK ASSESSMENT COMPONENTS



GOALS OF VENDOR RISK ASSESSMENT

1

CATEGORIZE YOUR VENDORS

Is there a difference between your critical vendors and the lawn care company? Not all vendors are created equal!

GOALS OF VENDOR RISK ASSESSMENT

1

2

SELECT YOUR VENDORS

Using the Vendor Risk Assessment, what decisions should you make?
Which vendors do we want to do business with?

GOALS OF VENDOR RISK ASSESSMENT

1

2

3

ONGOING MANAGEMENT

The biggest decision of Ongoing VM:
Do we want to keep doing business with this vendor?

WHAT DATA IS ACCESSIBLE TO YOUR VENDORS?

Or... where does your data live?

SBS CyberSecurity

CATS: ALL YOUR DATA ARE BELONG TO US!!

WHERE DOES THE IT ASSET LIVE?

ON YOUR NETWORK?

- Can the Vendor access info in or from the IT Asset?
- Does the Vendor have direct access to your network?

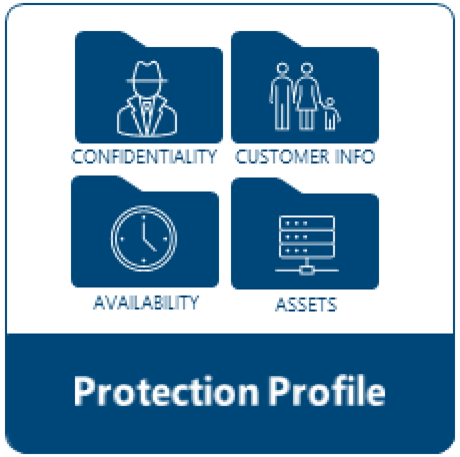
WITH THE VENDOR?

- Does the Vendor have read or write access to your info?

IN THE CLOUD?

- Does the Vendor have read or write access to your info?

START WITH THE PROTECTION PROFILE

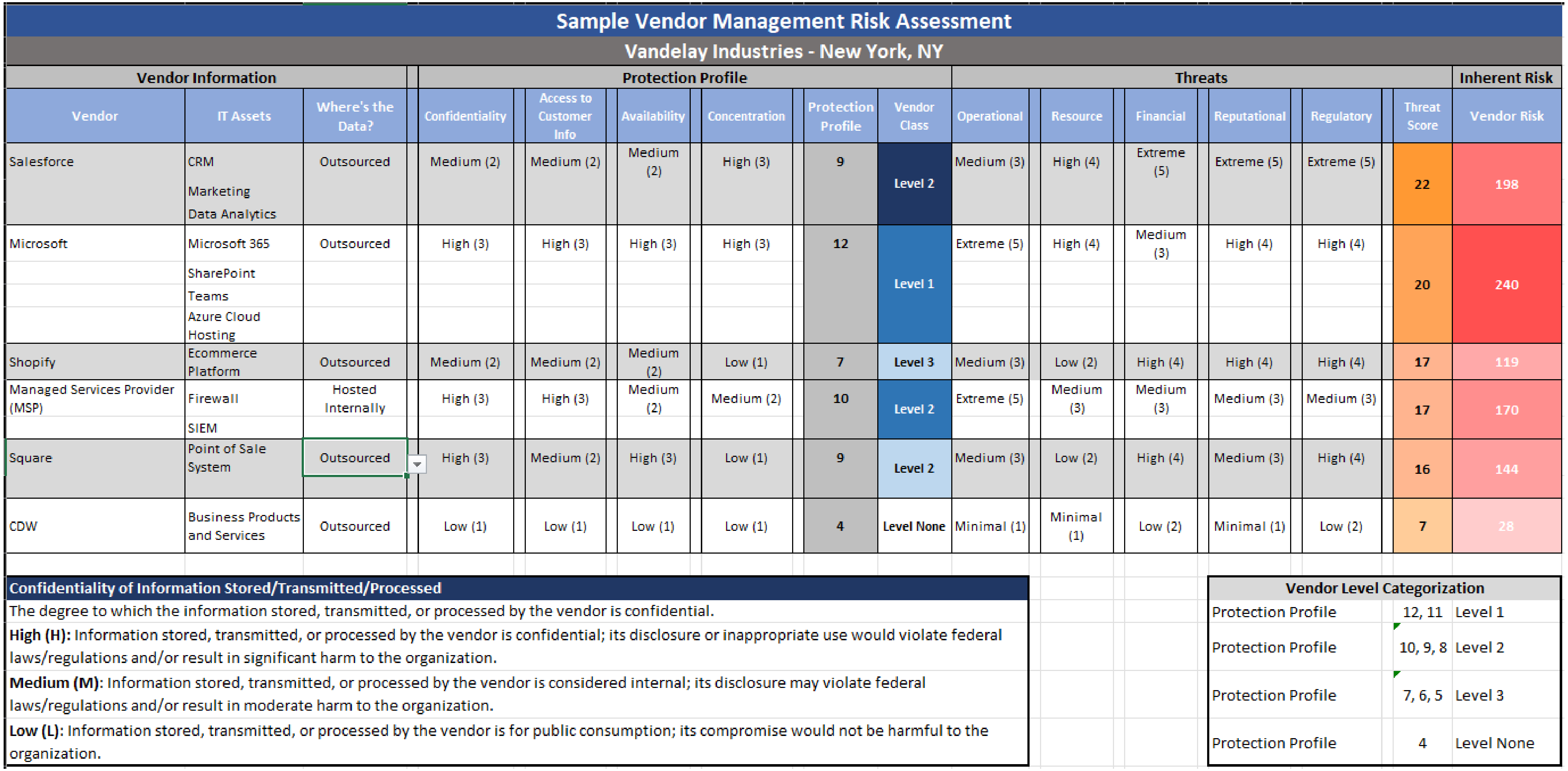


HOW IMPORTANT IS THIS VENDOR?

Areas of Measurement:

1. **Store, transmit, or process** confidential customer info?
2. **Access** to your customer info?
3. How critical is it that this vendor be **available** to us?
4. How many **IT assets** (or systems/apps) does the vendor provide us?

EXAMPLE VENDOR RISK ASSESSMENT



Sample Vendor Management Risk Assessment

Vandelay Industries - New York, NY

Vendor Information			Protection Profile						Threats						Inherent Risk
Vendor	IT Assets	Where's the Data?	Confidentiality	Access to Customer Info	Availability	Concentration	Protection Profile	Vendor Class	Operational	Resource	Financial	Reputational	Regulatory	Threat Score	Vendor Risk
Salesforce	CRM Marketing Data Analytics	Outsourced	Medium (2)	Medium (2)	Medium (2)	High (3)	9	Level 2	Medium (3)	High (4)	Extreme (5)	Extreme (5)	Extreme (5)	22	198
Microsoft	Microsoft 365 SharePoint Teams Azure Cloud Hosting	Outsourced	High (3)	High (3)	High (3)	High (3)	12	Level 1	Extreme (5)	High (4)	Medium (3)	High (4)	High (4)	20	240
Shopify	Ecommerce Platform	Outsourced	Medium (2)	Medium (2)	Medium (2)	Low (1)	7	Level 3	Medium (3)	Low (2)	High (4)	High (4)	High (4)	17	119
Managed Services Provider (MSP)	Firewall SIEM	Hosted Internally	High (3)	High (3)	Medium (2)	Medium (2)	10	Level 2	Extreme (5)	Medium (3)	Medium (3)	Medium (3)	Medium (3)	17	170
Square	Point of Sale System	Outsourced	High (3)	Medium (2)	High (3)	Low (1)	9	Level 2	Medium (3)	Low (2)	High (4)	Medium (3)	High (4)	16	144
CDW	Business Products and Services	Outsourced	Low (1)	Low (1)	Low (1)	Low (1)	4	Level None	Minimal (1)	Minimal (1)	Low (2)	Minimal (1)	Low (2)	7	28

Confidentiality of Information Stored/Transmitted/Processed

The degree to which the information stored, transmitted, or processed by the vendor is confidential.

High (H): Information stored, transmitted, or processed by the vendor is confidential; its disclosure or inappropriate use would violate federal laws/regulations and/or result in significant harm to the organization.

Medium (M): Information stored, transmitted, or processed by the vendor is considered internal; its disclosure may violate federal laws/regulations and/or result in moderate harm to the organization.

Low (L): Information stored, transmitted, or processed by the vendor is for public consumption; its compromise would not be harmful to the organization.

Vendor Level Categorization		
Protection Profile	12, 11	Level 1
Protection Profile	10, 9, 8	Level 2
Protection Profile	7, 6, 5	Level 3
Protection Profile	4	Level None

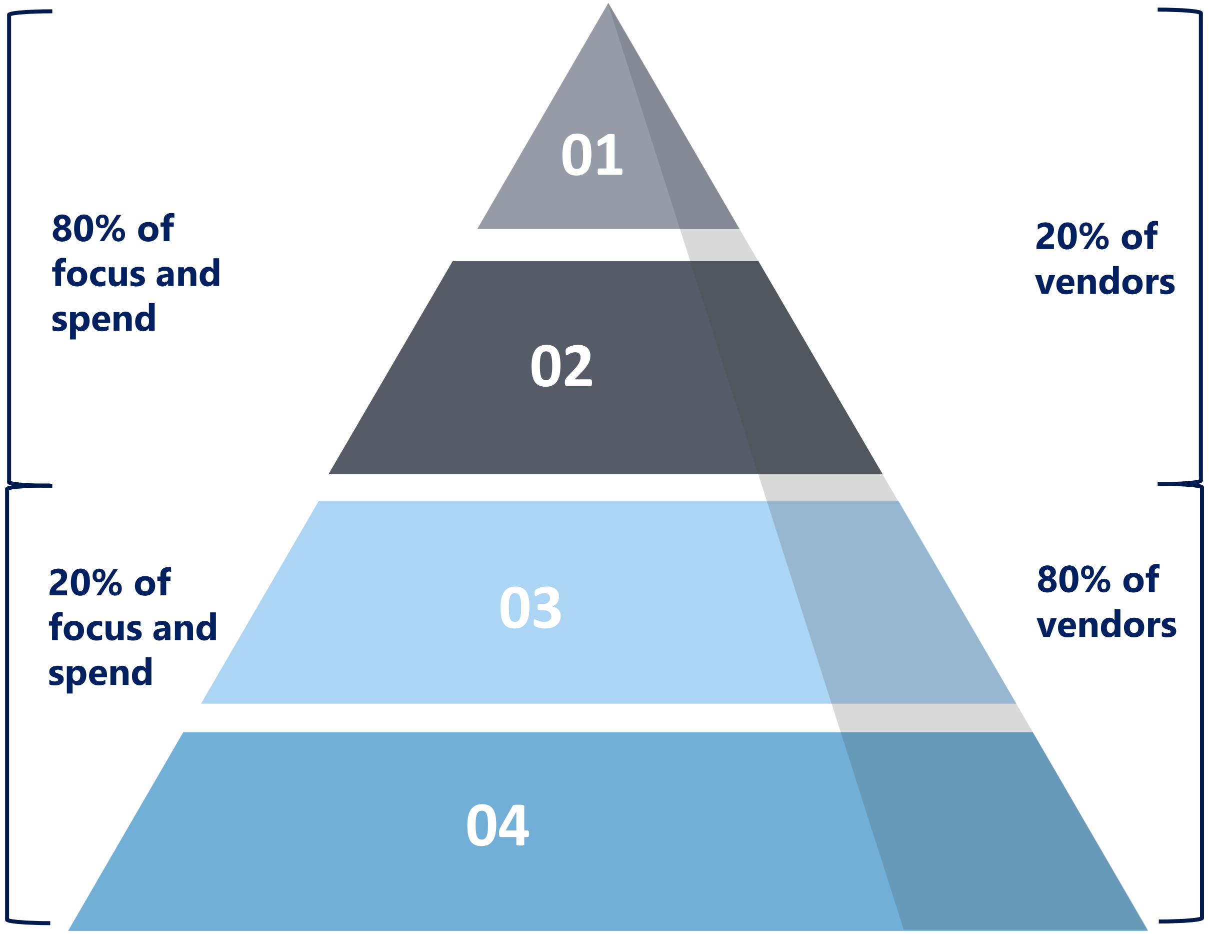
VENDOR MANAGEMENT LEVELS

01 ORGANIZATION-WIDE CRITICAL VENDORS

02 SIGNIFICANT VENDORS

03 NON-ESSENTIAL VENDORS

04 EXEMPT VENDORS



80% of focus and spend

20% of vendors

20% of focus and spend

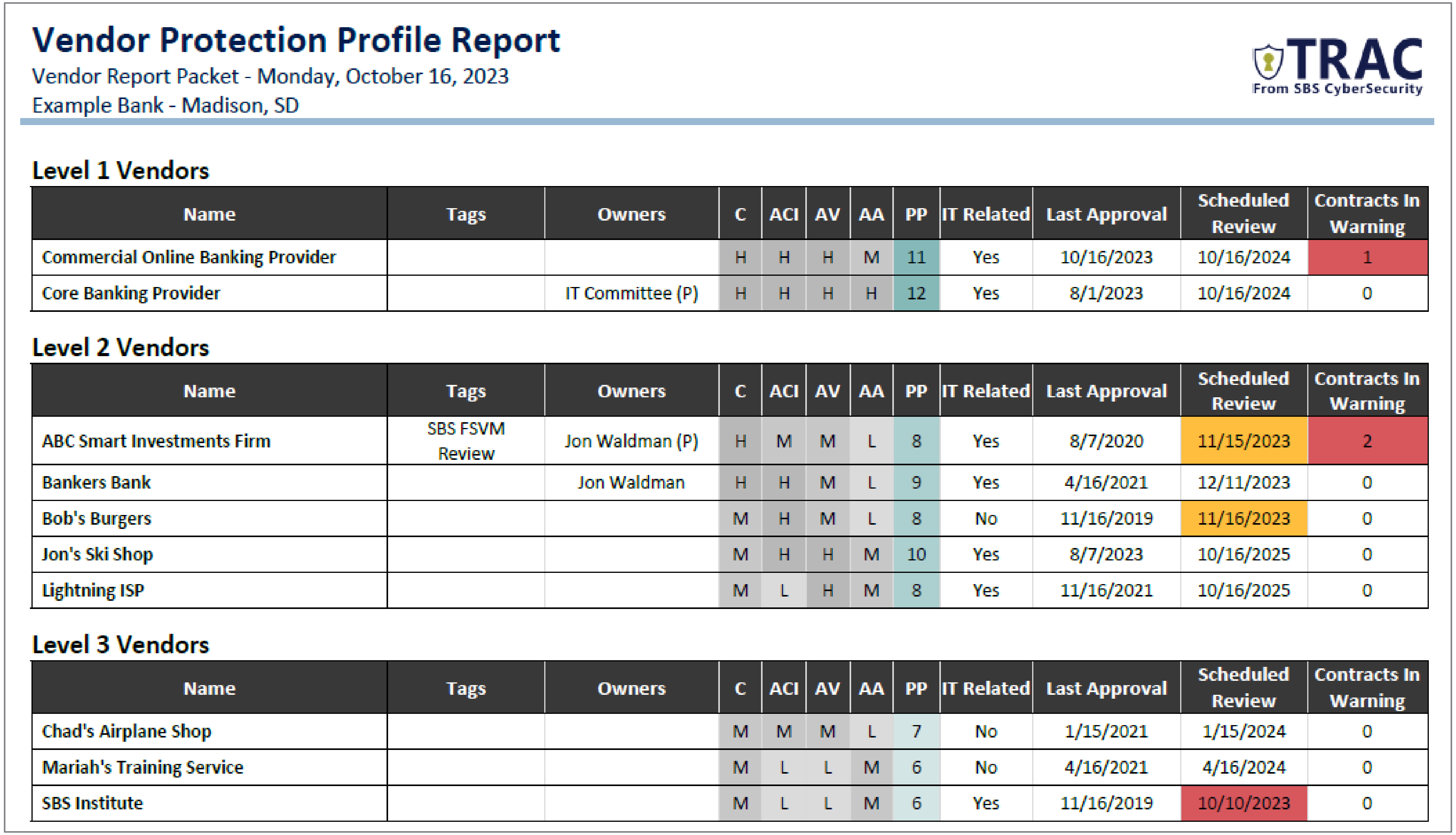
80% of vendors

SBS Blog

How Should I Categorize My Vendors?

https://sbscyber.com/blog/vendor-management-how-should-i-categorize-my-vendors

DETERMINING VENDOR LEVELS



Vendor Protection Profile Report

Vendor Report Packet - Monday, October 16, 2023
Example Bank - Madison, SD

TRAC
From SBS CyberSecurity

Level 1 Vendors

Name	Tags	Owners	C	ACI	AV	AA	PP	IT Related	Last Approval	Scheduled Review	Contracts In Warning
Commercial Online Banking Provider			H	H	H	M	11	Yes	10/16/2023	10/16/2024	1
Core Banking Provider		IT Committee (P)	H	H	H	H	12	Yes	8/1/2023	10/16/2024	0

Level 2 Vendors

Name	Tags	Owners	C	ACI	AV	AA	PP	IT Related	Last Approval	Scheduled Review	Contracts In Warning
ABC Smart Investments Firm	SBS FSVM Review	Jon Waldman (P)	H	M	M	L	8	Yes	8/7/2020	11/15/2023	2
Bankers Bank		Jon Waldman	H	H	M	L	9	Yes	4/16/2021	12/11/2023	0
Bob's Burgers			M	H	M	L	8	No	11/16/2019	11/16/2023	0
Jon's Ski Shop			M	H	H	M	10	Yes	8/7/2023	10/16/2025	0
Lightning ISP			M	L	H	M	8	Yes	11/16/2021	10/16/2025	0

Level 3 Vendors

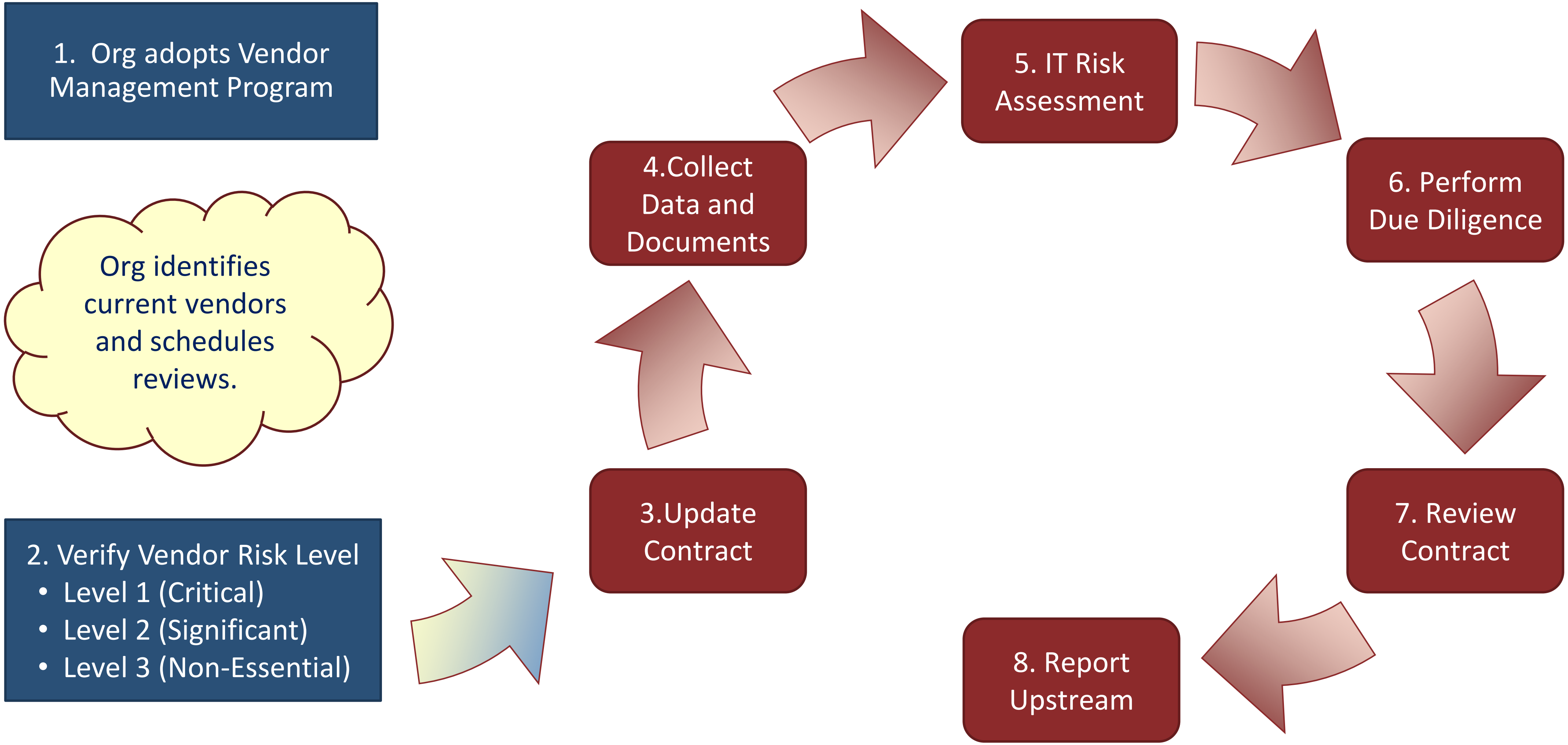
Name	Tags	Owners	C	ACI	AV	AA	PP	IT Related	Last Approval	Scheduled Review	Contracts In Warning
Chad's Airplane Shop			M	M	M	L	7	No	1/15/2021	1/15/2024	0
Mariah's Training Service			M	L	L	M	6	No	4/16/2021	4/16/2024	0
SBS Institute			M	L	L	M	6	Yes	11/16/2019	10/10/2023	0

ONGOING VENDOR MANAGEMENT

ARE YOU *REALLY* MANAGING EXISTING VENDOR RISK AND RELATIONSHIPS, OR ARE YOU JUST FLOATING ALONG?

SBS CyberSecurity

ONGOING VENDOR MANAGEMENT



1. Org adopts Vendor Management Program

Org identifies current vendors and schedules reviews.

2. Verify Vendor Risk Level

- Level 1 (Critical)
- Level 2 (Significant)
- Level 3 (Non-Essential)

3.Update Contract

4.Collect Data and Documents

5. IT Risk Assessment

6. Perform Due Diligence

7. Review Contract

8. Report Upstream

WHERE TO START WITH VENDOR MANAGEMENT?

…the **RISK ASSESSMENT**!

- Determine vendor classification
- The more important/risky the vendor, the more should be done to mitigate risk
- **MAKE THE #1 DECISION: DOES THE ORGANIZATION WANT TO KEEP DOING BUSINESS WITH THIS VENDOR?**
  - If yes – great! Move along.
  - If no – or if there's more risk than acceptable – then what?

REQUIRED DOCUMENTATION

- All depends on the Level of the Vendor
- The greater the Vendor Level (risk), the more documentation should be required
- And vice-versa!
- Don't forget to **analyze**; can't just **collect**
- What does the organization look for? RED FLAGS!

Critical Vendor Docs Checklist:

☑ **IT or IS Audit/Assessment**

1. **SOC Reports** are most common (**SOC 2 preferred for security standards**)
2. **External IT Audit** or similar as an alternative
3. **Other**

☑ **Information Security Program**

☑ **Business Continuity/Disaster Recovery Plan**

☑ **Incident Response Plan**

☑ **Insurance Coverage** (look for cyber insurance)

☑ **Audited Financials**

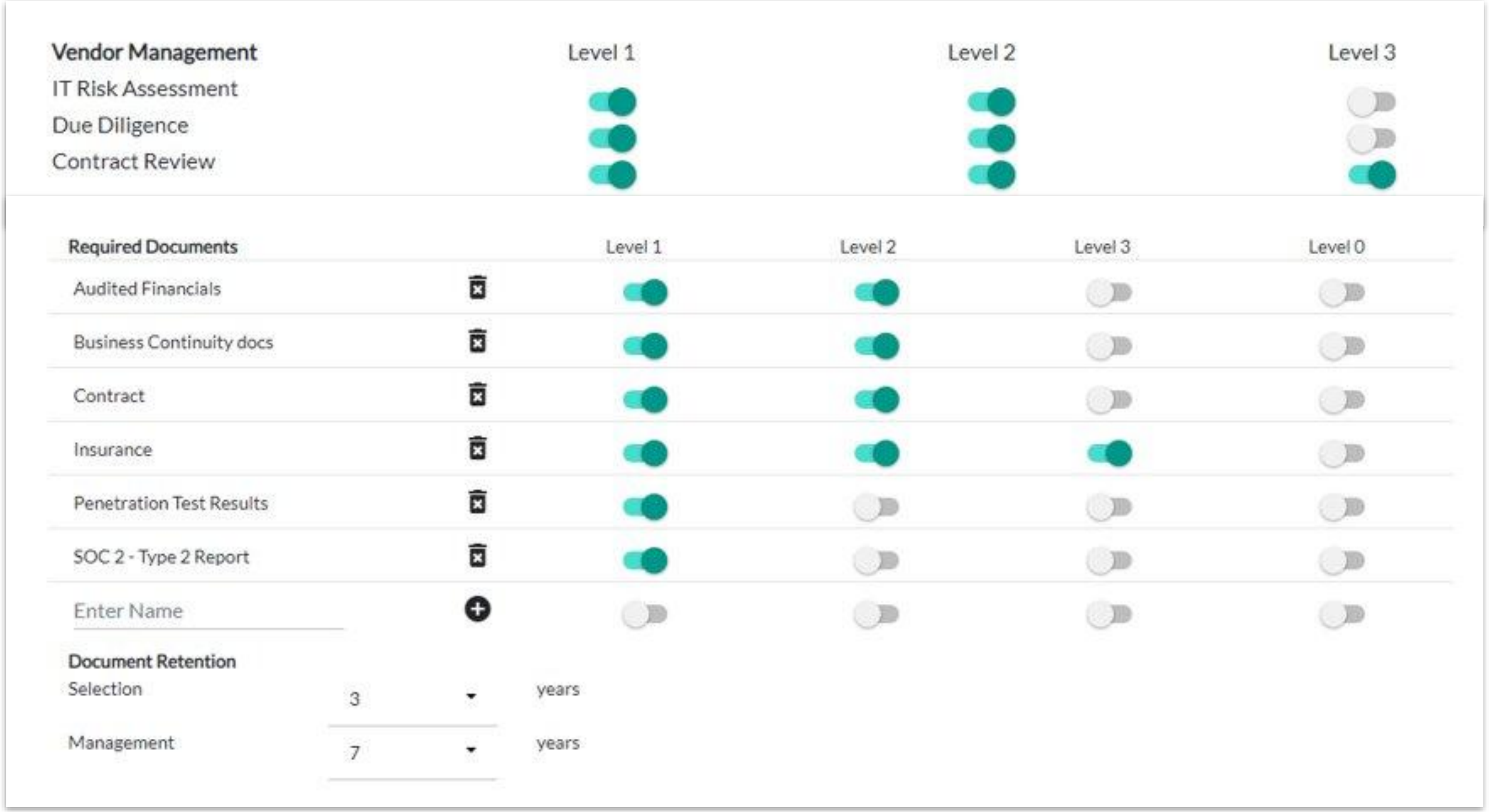
☑ **Contract**

☑ **Results of NetSec Testing** (PT, VA, SE, etc.)

☑ **Web Application Assessment** (if SaaS)

☑ **Results of BC/DR/IR Testing**

MANAGEMENT REQUIREMENTS



Vendor Management	Level 1	Level 2	Level 3
IT Risk Assessment	●	●	○
Due Diligence	●	●	○
Contract Review	●	●	●

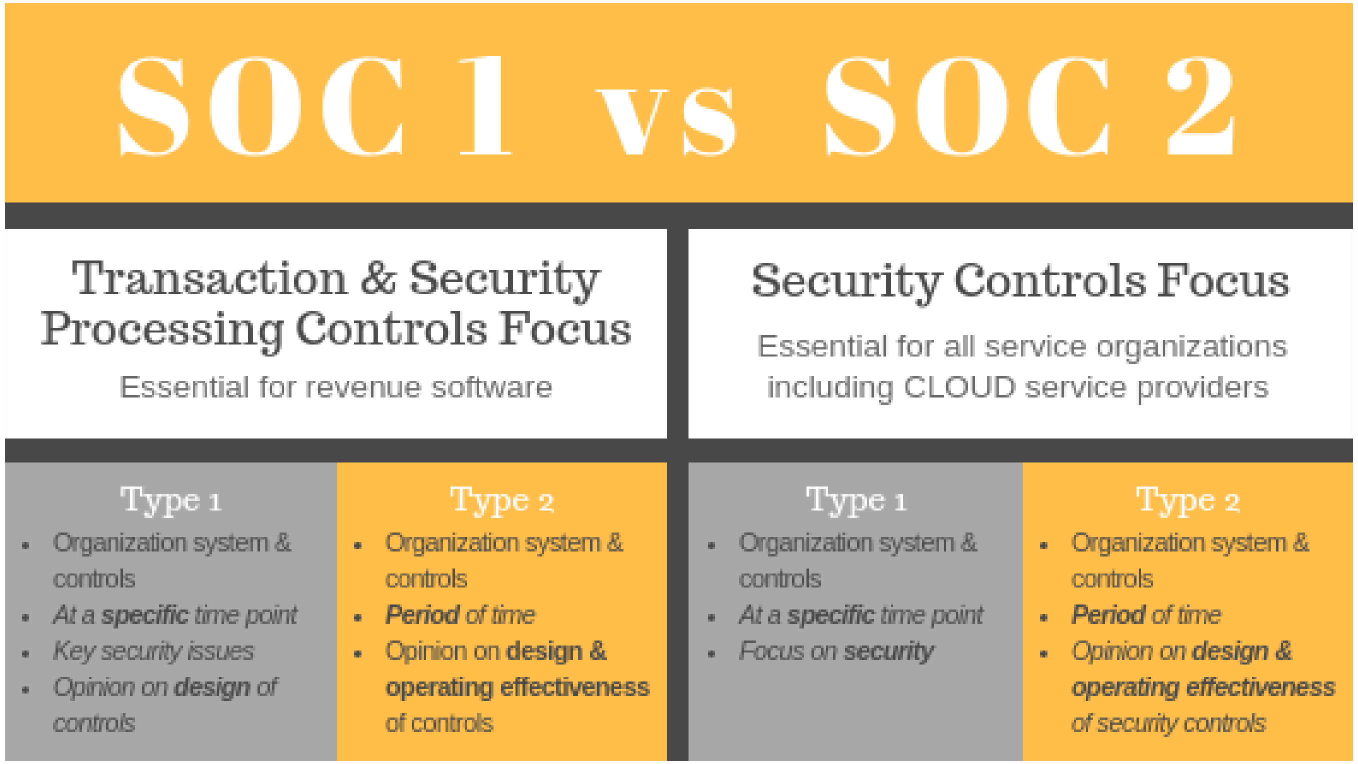
Required Documents		Level 1	Level 2	Level 3	Level 0
Audited Financials	🗑	●	●	○	○
Business Continuity docs	🗑	●	●	○	○
Contract	🗑	●	●	○	○
Insurance	🗑	●	●	●	○
Penetration Test Results	🗑	●	○	○	○
SOC 2 - Type 2 Report	🗑	●	○	○	○
Enter Name	⊕	○	○	○	○

Document Retention

Selection	3 ▾	years
Management	7 ▾	years

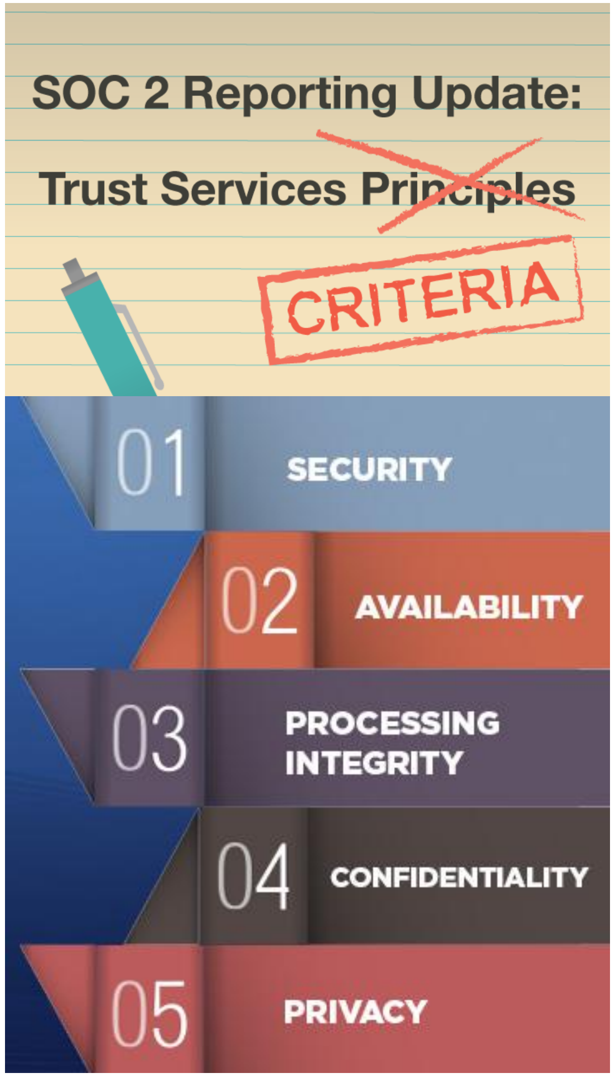
WHY DO WE WANT SOC 2 REPORTS?

SSAE-18 SOC 1 reports ***do not address*** logical security nor physical security topics; SSAE-18 SOC 1 reports only address “internal controls over financial reporting.”



SOC 1 vs SOC 2

Transaction & Security Processing Controls Focus Essential for revenue software		Security Controls Focus Essential for all service organizations including CLOUD service providers	
Type 1	Type 2	Type 1	Type 2
• Organization system & controls • *At a **specific** time point* • *Key security issues* • *Opinion on **design** of controls*	• Organization system & controls • ***Period** of time* • Opinion on **design & operating effectiveness** of controls	• Organization system & controls • *At a **specific** time point* • *Focus on **security***	• Organization system & controls • ***Period** of time* • *Opinion on **design & operating effectiveness** of security controls*



SOC 2 Reporting Update:

Trust Services ~~Principles~~

CRITERIA

THE BIG QUESTION

Who is **REQUIRED** to have a SSAE 18/SOC Assessment?

NO ONE!

Also note: there is **no such thing** as "SSAE 18 Compliant"

DUE DILIGENCE + CONTRACT REVIEW

- Set a baseline of questions to ask your vendors
- DUE DILIGENCE = What do you know about the company?
- CONTRACT REVIEW = does the contract protect only the vendor, or does it meet standard expectations for the duty of care today
  - Termination
  - Incident Notifications
  - Who owns the data?
  - More…
- Regulated Industries can show us the way (banking is the best example)
  - Joint Banking Guidance on Third Party Risk Management: https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html

DUE DILIGENCE + CONTRACT REVIEW

- Other question sets where appropriate:
  - **SOC Review Questions** – what is important to take away from a SOC review?
  - **Cloud Computing Questions**
  - **Foreign-Based Service Provider Questions**
  - **Artificial Intelligence**
- Just as different documentation requirements should be set for different levels of vendor, so should the amount and types of questions.

THE MORE CRITICAL THE VENDOR, THE DEEPER THE DIVE INTO CONTRACT REVIEW AND DUE DILIGENCE QUESTIONS

WHAT ARE YOU LOOKING FOR?

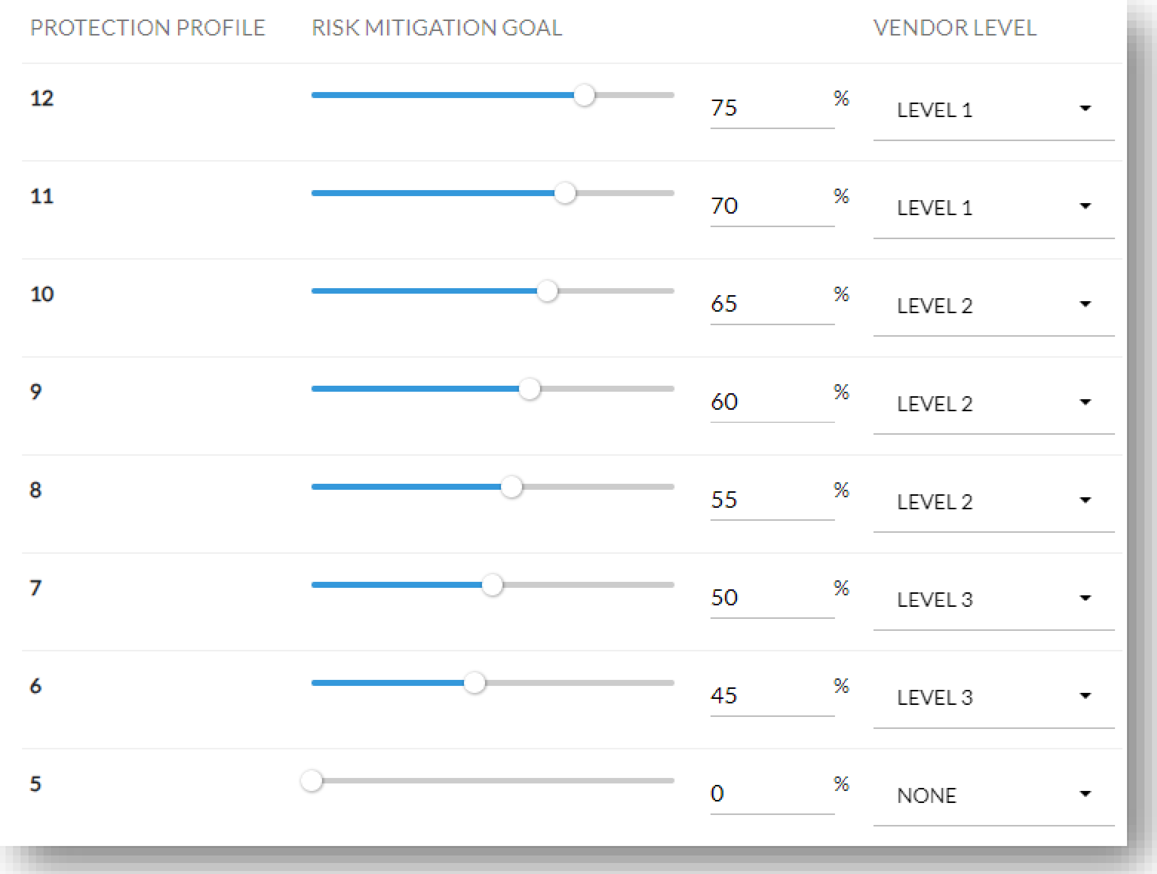
SBS CyberSecurity

ACCEPTABLE LEVELS OF RISK

- How do you measure risk?

  THERE NEEDS TO BE A GOAL!

- How does Residual Risk compare to risk goals?
  - ❑ Acceptable levels of Risk?
    - ✓ IT Risk Mitigation Strategy
  - ❑ IT Strategic Plan?
  - ❑ **Plan to meet acceptable levels of risk**
    - ✓ **Now or in the future…**

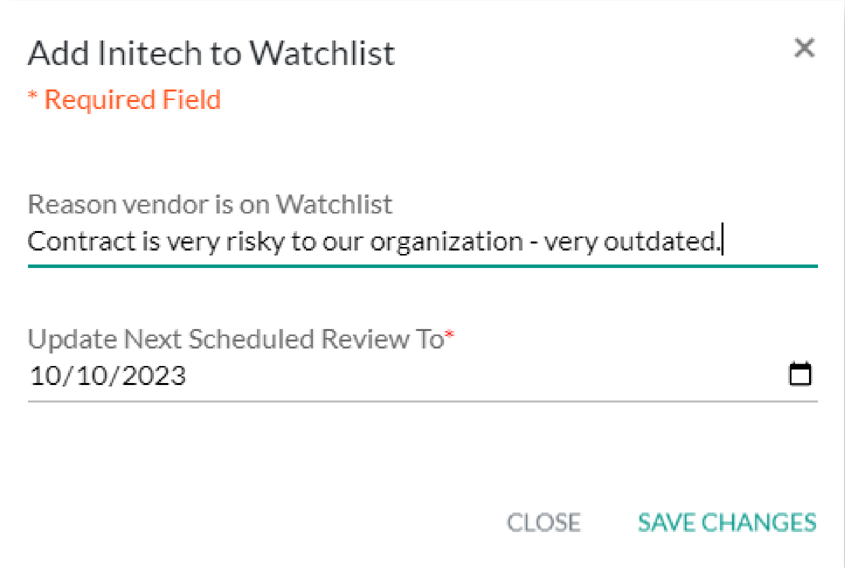


PROTECTION PROFILE	RISK MITIGATION GOAL		VENDOR LEVEL
12	75	%	LEVEL 1
11	70	%	LEVEL 1
10	65	%	LEVEL 2
9	60	%	LEVEL 2
8	55	%	LEVEL 2
7	50	%	LEVEL 3
6	45	%	LEVEL 3
5	0	%	NONE

THE WATCH LIST

- The Watch List has four (4) outcomes:

1. ACCEPT THE RISK
2. RESOLVE THE RISK
   - ❑ Work with the vendor to address any issues until resolved, then remove the vendor from the Watch List
3. CHANGE THE RISK
   - ❑ Find a new vendor
   - ❑ Bring the product in-house (if outsourced) for more control
   - ❑ Discontinue the product or service
4. ~~TRANSFER THE RISK~~

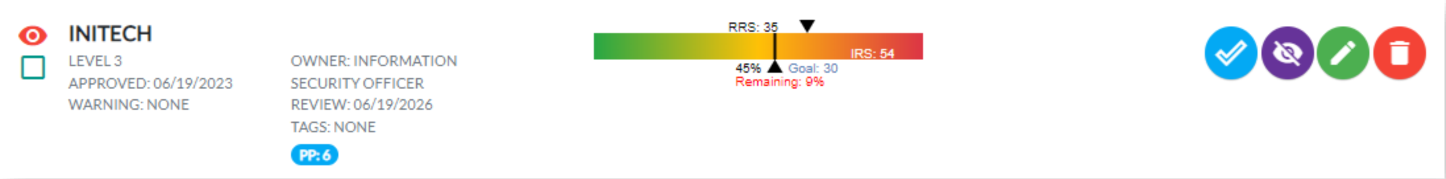


Add Initech to Watchlist

* Required Field

Reason vendor is on Watchlist
Contract is very risky to our organization - very outdated.

Update Next Scheduled Review To*
10/10/2023



INITECH
LEVEL 3
APPROVED: 06/19/2023
WARNING: NONE

OWNER: INFORMATION SECURITY OFFICER
REVIEW: 06/19/2026
TAGS: NONE

OTHER WAYS TO MANAGE VENDOR RISK

SBS CyberSecurity

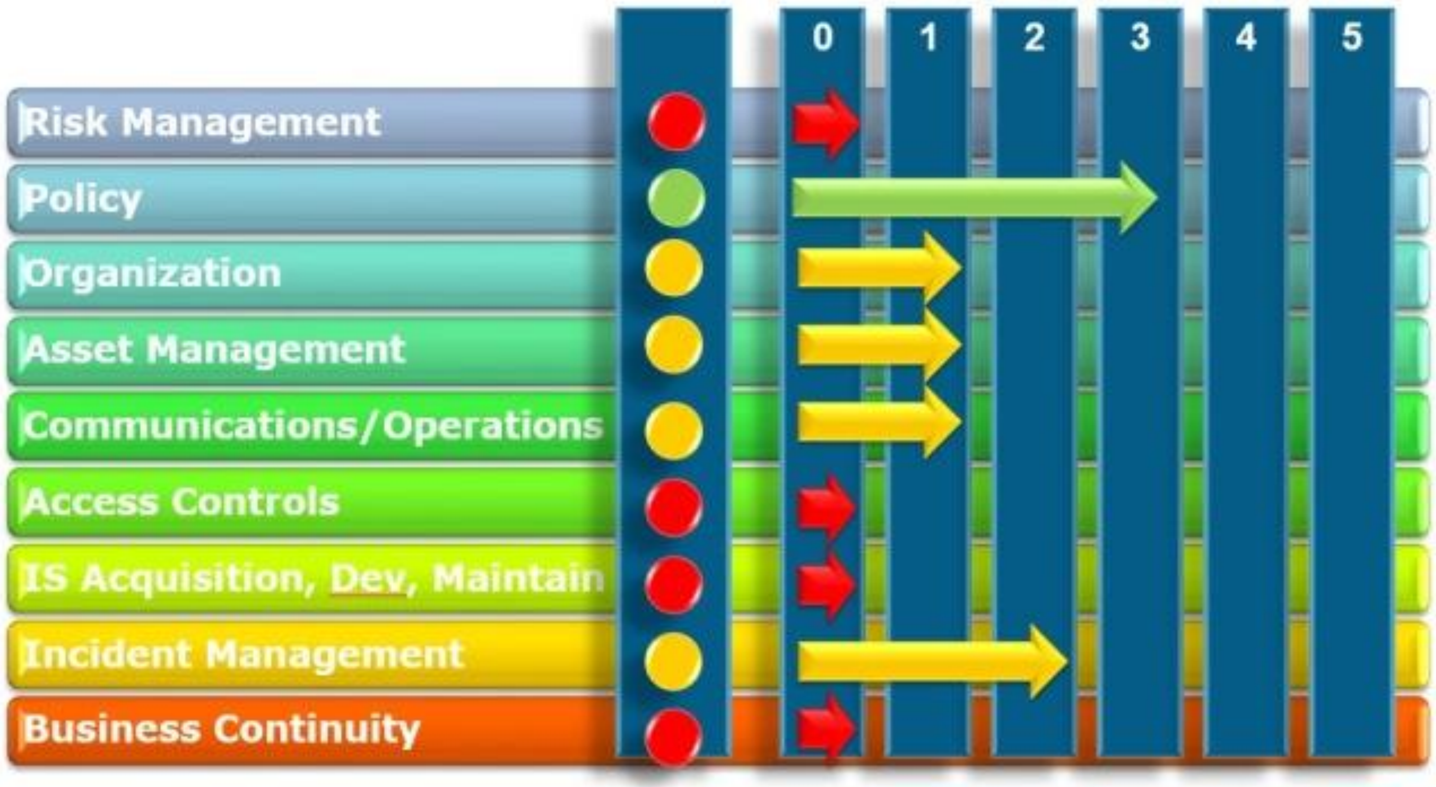
SHARED ASSESSMENTS

- Shared Assessments is a global membership organization dedicated to developing the best practices, education, and products to drive third-party risk assurance.
- Two most common assessments: SIG and VRMMM
- Not a certification! A self-assessment
- SIG = Standardized Information Gathering (maps to many frameworks)
  - ❑ SIG is a third-party self-assessment that covers 19 risk domains
- VRMMM = Vendor Risk Management Maturity Model
  - ❑ Free to download – framework for assessing Vendors
- **SBS is seeing a more SIG and VRMMM reports**
  - ❑ https://sharedassessments.org/products/

SFG SHARED ASSESSMENTS

ISO 27002 GAP ASSESSMENT

ISO 27002 Controls Maturity Scorecard



0 – Non-Existent, 1 – Initial, 2 – Repeatable, 3 – Defined, 4 – Managed, 5 - Optimized

TOP VM RISK ASSESSMENT PRODUCTS

Archer	https://www.archerirm.com/content/vendor-risk-management	Massachusetts
CoNetrix	https://tandem.app/vendor-management-software	Texas
Venminder	https://www.venminder.com/	Kentucky
Ncontracts	https://ncontracts.com/	Tennessee
Quantivate	https://quantivate.com/vendor-management-software-2/	Washington
WolfPAC	https://www.wolfpacsolutions.com/	Boston
TRAC Vendor	https://sbscyber.com/solutions/trac	South Dakota

WHAT ABOUT CODE REVIEWS?

- HAS THE VENDOR HAD A CODE REVIEW PERFORMED FOR THE SYSTEM/APPLICATION THE ORGANIZATION IS USING?
- OWASP - OPEN WEB APPLICATION SECURITY PROJECT
  - ❑ HTTPS://WWW.OWASP.ORG/INDEX.PHP/MAIN_PAGE
  - ❑ THE STANDARD FOR ONLINE WEB APPLICATION SECURITY
- IN OUR EXPERIENCE, MOST VENDORS DO NOT HAVE THEIR WEB APPS TESTED AGAINST OWASP STANDARDS

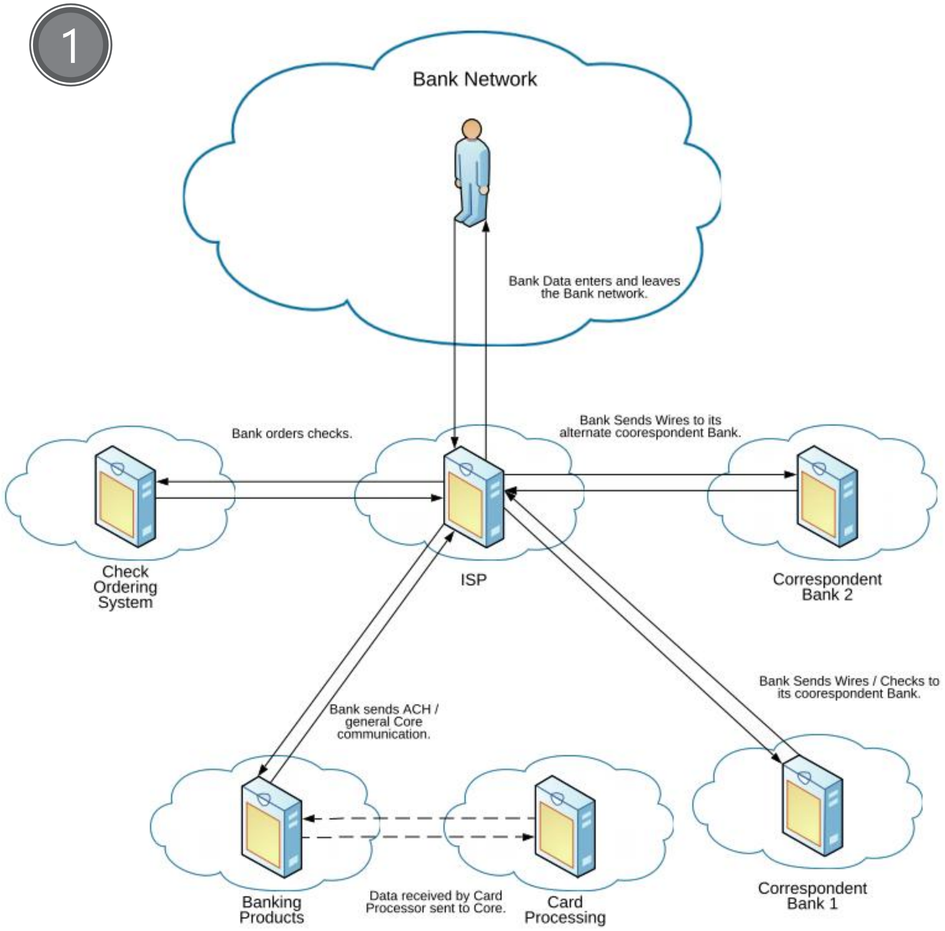
CONTINUOUS VENDOR MONITORING

- **UPGUARD**
  - https://www.upguard.com/product/vendorrisk
- **SECURITYSCORECARD**
  - https://securityscorecard.com
- **BITSIGHT**
  - https://www.bitsight.com/
- **DUNN & BRADSTREET CYBER RISK SCORE (FORMERLY FICO)**
  - https://www.dnb.com/resources/cyber-risk-rating.html

CAVEAT: THESE ARE NEWER TECHNOLOGIES, AND THERE ARE ASSUMPTIONS MADE IN MANY OF THESE SCORES. DON'T TREAT THEM AS GOSPEL, BUT THEY ARE A GOOD RESOURCE

DATA FLOW DIAGRAMS

1


Bank Network
Bank Data enters and leaves the Bank network.
Bank orders checks.
Bank Sends Wires to its alternate cooorespondent Bank.
Check Ordering System
ISP
Correspondent Bank 2
Bank Sends Wires / Checks to its cooorespondent Bank.
Bank sends ACH / general Core communication.
Banking Products
Data received by Card Processor sent to Core.
Card Processing
Correspondent Bank 1

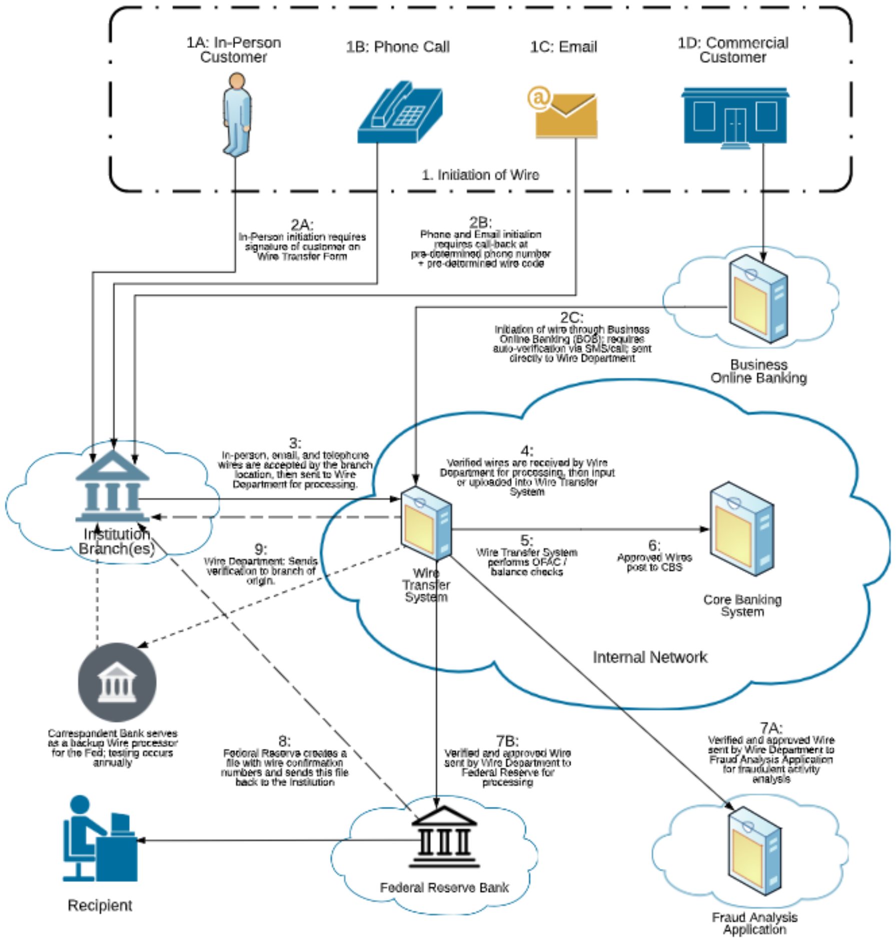
SBS BLOG

Data Flow Diagrams

https://sbscyber.com/blog/data-flow-diagrams-101

2

Example Financial Institution
Data Flow Diagram
Wire Transfers


1A: In-Person Customer
1B: Phone Call
1C: Email
1D: Commercial Customer
1. Initiation of Wire
2A:
In-Person initiation requires signature of customer on Wire Transfer Form
2B:
Phone and Email initiation requires call-back at pre-determined phone number + pre-determined wire code
2C:
Initiation of wire through Business Online Banking (BOB); requires auto-verification via SMS/call; sent directly to Wire Department
Business Online Banking
3:
In-person, email, and telephone wires are accepted by the branch location, then sent to Wire Department for processing.
4:
Verified wires are received by Wire Department for processing, then input or uploaded into Wire Transfer System
Institution Branch(es)
9:
Wire Department: Sends verification to branch of origin.
Wire Transfer System
5:
Wire Transfer System performs OFAC / balance checks
6:
Approved Wires post to CBS
Core Banking System
Internal Network
Correspondent Bank serves as a backup Wire processor for the Fed; testing occurs annually
8:
Federal Reserve creates a file with wire confirmation numbers and sends this file back to the Institution
7B:
Verified and approved Wire sent by Wire Department to Federal Reserve for processing
7A:
Verified and approved Wire sent by Wire Department to Fraud Analysis Application for fraudulent activity analysis
Recipient
Federal Reserve Bank
Fraud Analysis Application

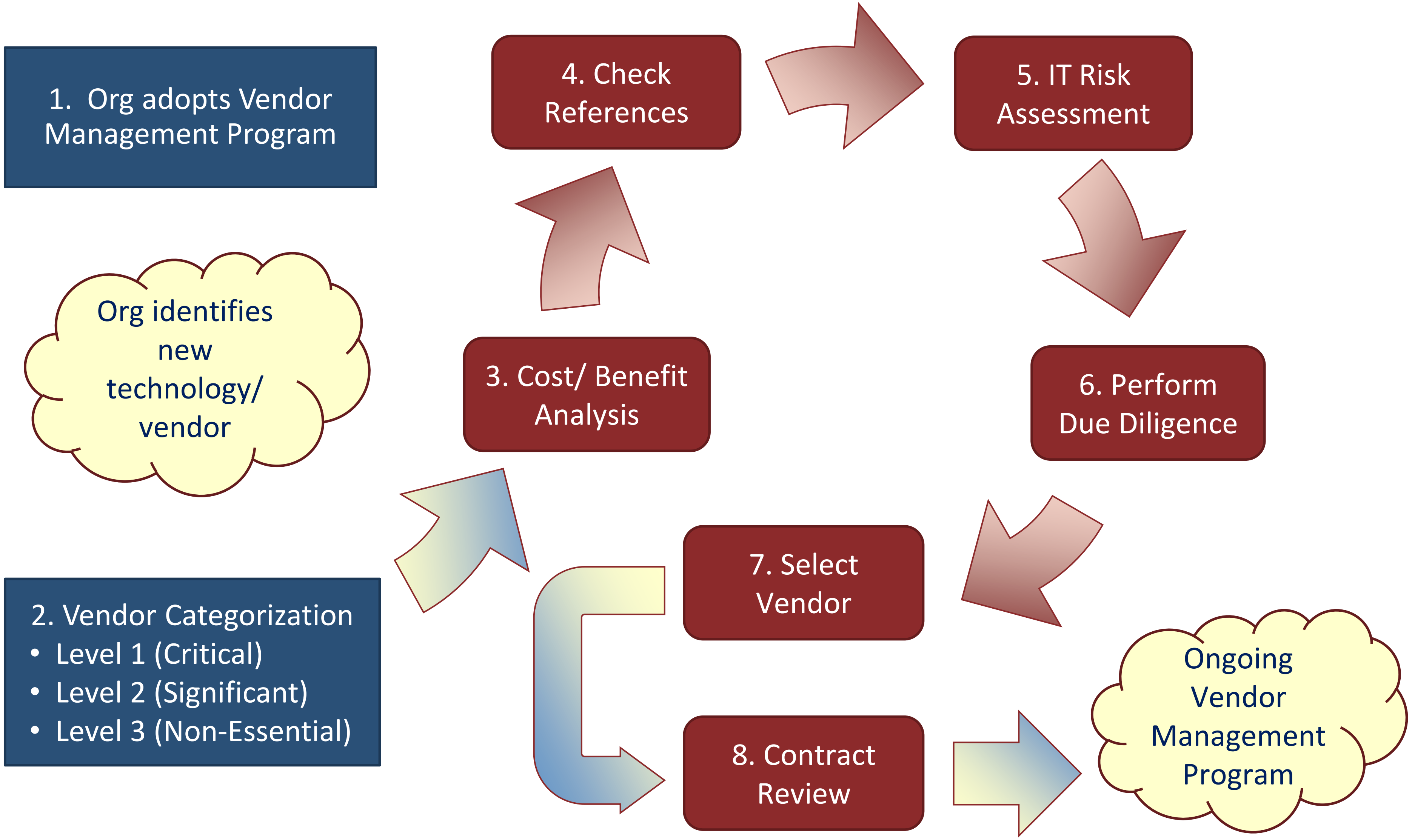
SELECTING BETTER VENDORS

FIRST QUESTION:

DO YOU ASSESS RISK *BEFORE* TALKING TO NEW VENDORS, OR ONLY *AFTER* THE CONTRACT IS SIGNED?

SBS CyberSecurity

VENDOR SELECTION FLOW



1. Org adopts Vendor Management Program

Org identifies new technology/ vendor

2. Vendor Categorization
- Level 1 (Critical)
- Level 2 (Significant)
- Level 3 (Non-Essential)

3. Cost/ Benefit Analysis

4. Check References

5. IT Risk Assessment

6. Perform Due Diligence

7. Select Vendor

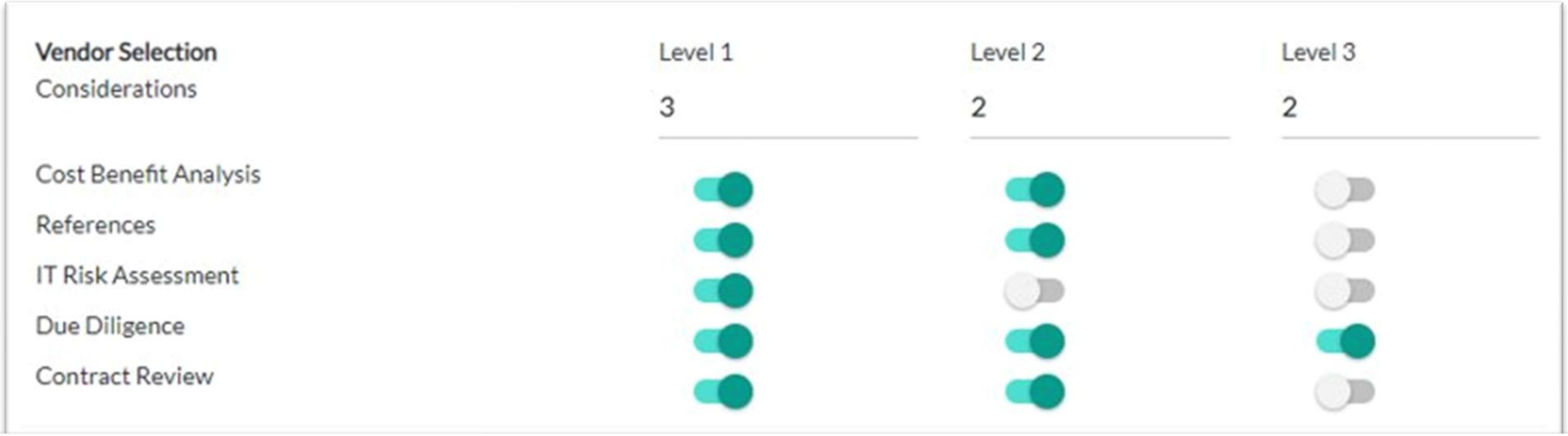
8. Contract Review

Ongoing Vendor Management Program

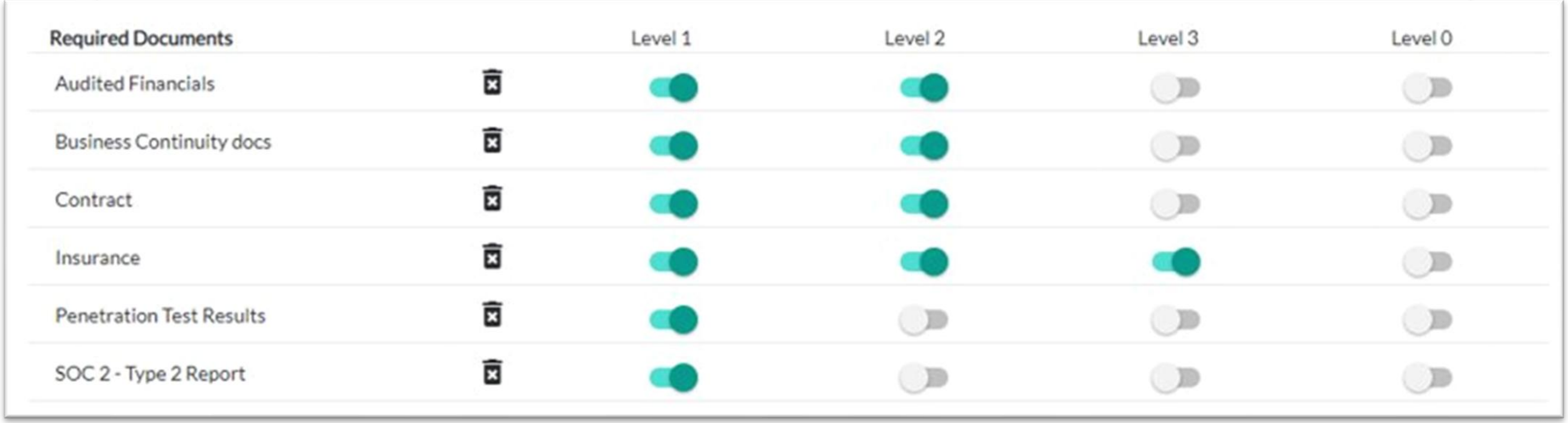
MUCH OF THE SAME AS MANAGEMENT

- Always start with the **RISK ASSESSMENT!**
- What is the risk associated with the vendors and/or IT systems or assets being selected?
- Determine the type of Vendor the organization is looking at during the selection process
  - ❑ What kind of information are they storing, transmitting, and processing?
  - ❑ How critical will this vendor be to the organization going forward?
- Different selection requirements for different levels of vendors

SELECTION REQUIREMENTS



Vendor Selection Considerations	Level 1	Level 2	Level 3
	3	2	2
Cost Benefit Analysis	●	●	○
References	●	●	○
IT Risk Assessment	●	○	○
Due Diligence	●	●	●
Contract Review	●	●	○



Required Documents	Level 1	Level 2	Level 3	Level 0
Audited Financials	●	●	○	○
Business Continuity docs	●	●	○	○
Contract	●	●	○	○
Insurance	●	●	●	○
Penetration Test Results	●	○	○	○
SOC 2 - Type 2 Report	●	○	○	○

HOW MANY VENDORS TO REVIEW?

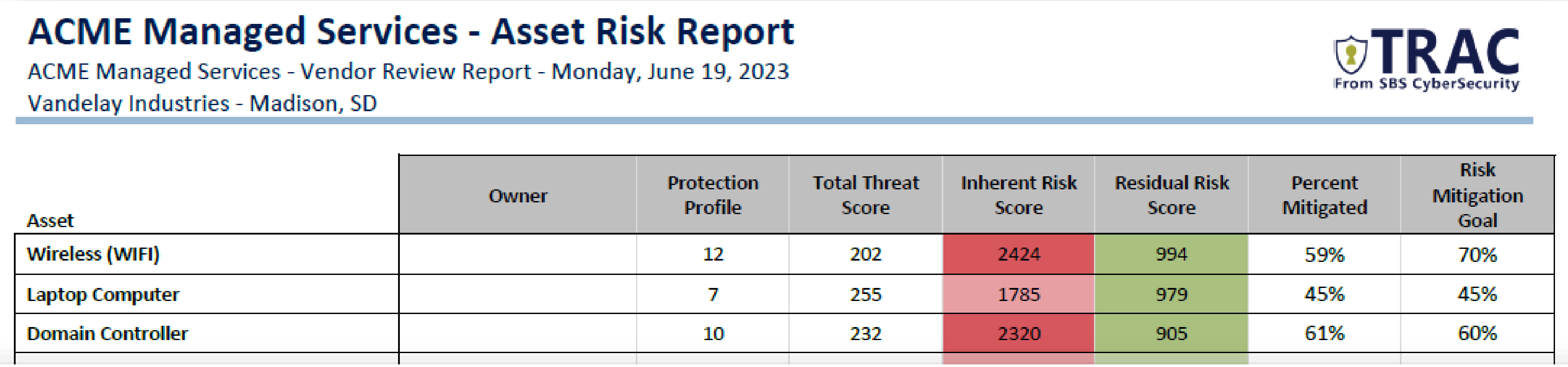
- **DEPENDS ON THE LEVEL OR IMPORTANCE!**
  - Level 1 Vendor (High) – minimum of 3 vendors
  - Level 2 Vendor (Medium) – minimum of 2 vendors
  - Level 3 Vendor (Low) – minimum of 1 vendor
- **MORE IS ALWAYS BETTER, BUT WHY?**
  - Security controls
  - Additional functionality
  - PRICE!

MAKING THE SELECTION DECISION

- **USE METRICS** (BUT DON'T FORGET VALUE)
- Rank the Vendors being selected
  - Importance
  - Threats
  - Cost/Benefit Analysis
  - IT Risk Assessment
  - Due Diligence
- Most importantly, the organization's opinion
- **The #1 question: which Vendor do we want to do business with?**

VENDOR SELECTION RESULTS

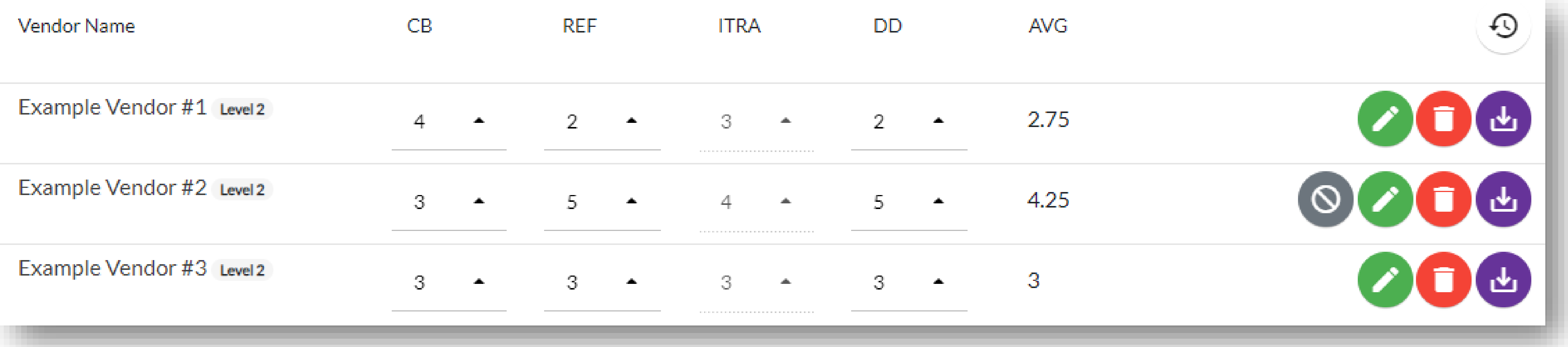
- Notice that vendor 3 has done the most to reduce the risk of information security threats.
- However, considerations must be given for other areas.



ACME Managed Services - Asset Risk Report

ACME Managed Services - Vendor Review Report - Monday, June 19, 2023
Vandelay Industries - Madison, SD

Asset	Owner	Protection Profile	Total Threat Score	Inherent Risk Score	Residual Risk Score	Percent Mitigated	Risk Mitigation Goal
Wireless (WIFI)		12	202	2424	994	59%	70%
Laptop Computer		7	255	1785	979	45%	45%
Domain Controller		10	232	2320	905	61%	60%



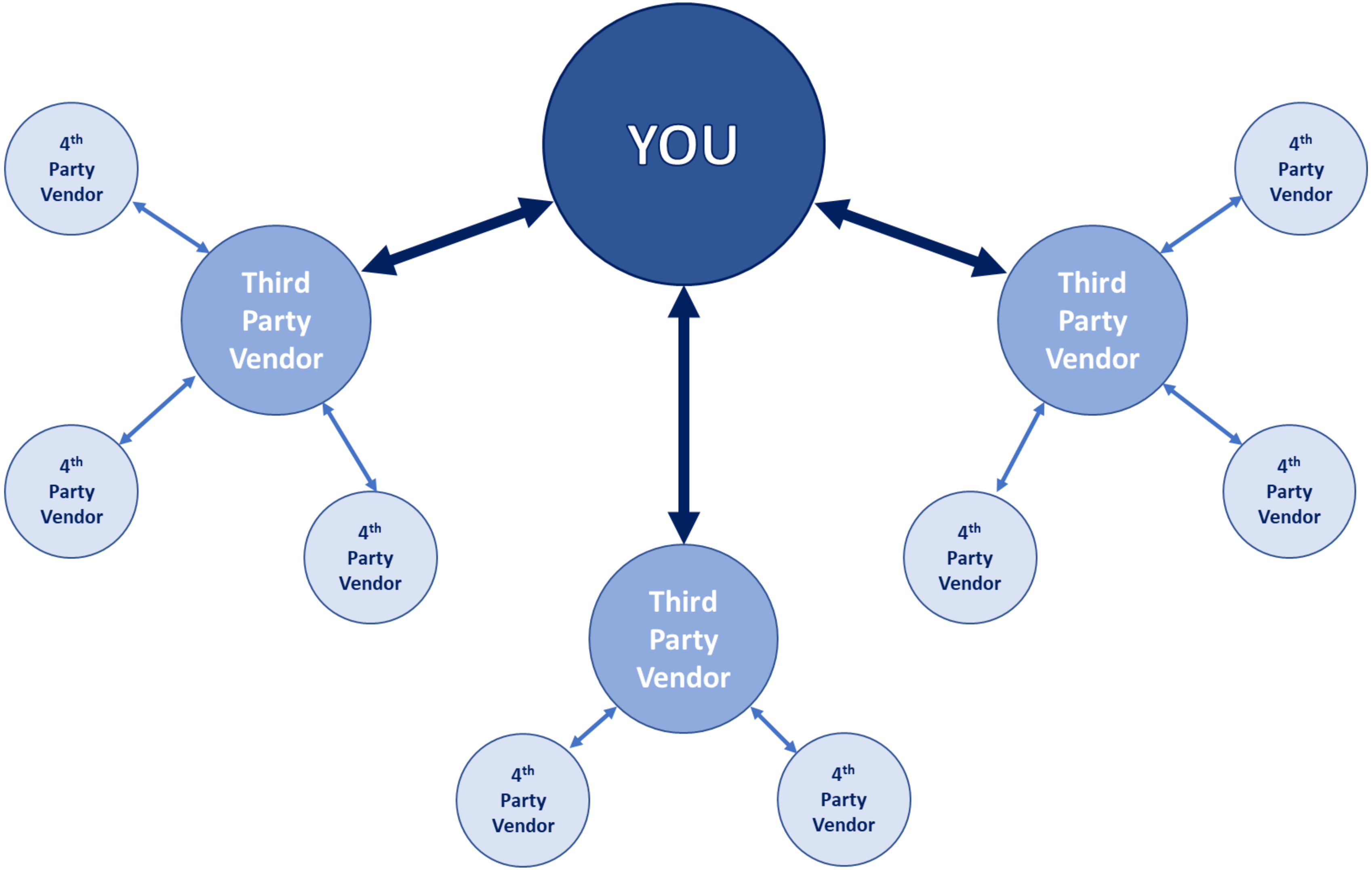
Vendor Name	CB	REF	ITRA	DD	AVG
Example Vendor #1 Level 2	4	2	3	2	2.75
Example Vendor #2 Level 2	3	5	4	5	4.25
Example Vendor #3 Level 2	3	3	3	3	3

THIRD VS FOURTH PARTY MANAGEMENT

WHAT'S THE DIFFERENCE? WHY SHOULD YOU CARE?
WHAT DO YOU NEED TO DO?

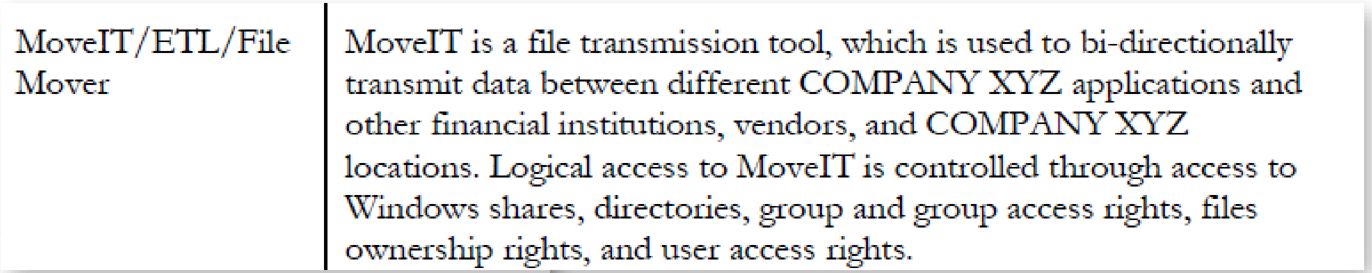
SBS CyberSecurity

THIRD VS. FOURTH PARTY RISK

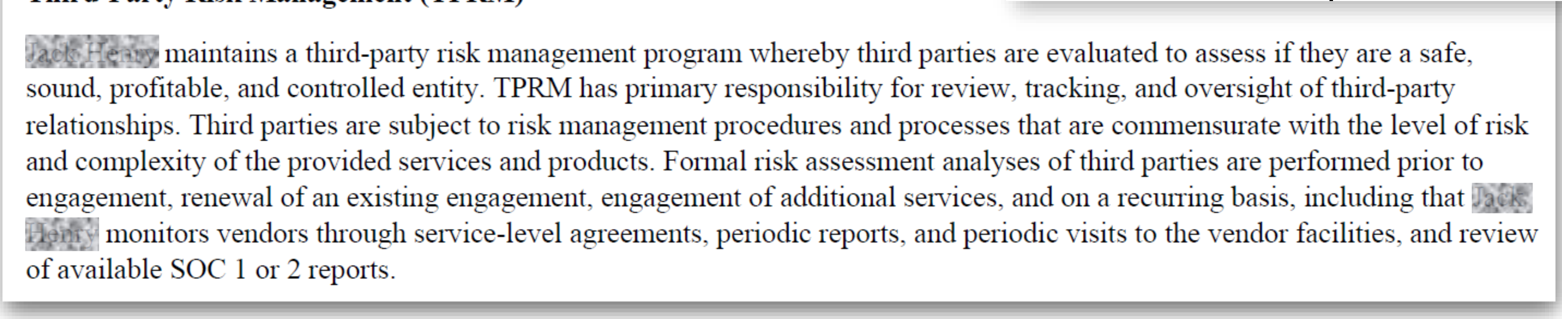


SOC REPORT 4TH PARTY EXAMPLE

- Vendor (or Third-Party) Risk Management documentation may be found in a few areas in a SOC Report:
  - ❑ Company's Description of Systems and Controls
    - ✓ Internal Controls > Vendor/Third Party Risk Management
  - ❑ Common Criteria (Security)
    - ✓ Monitoring
    - ✓ Risk Assessment
    - ✓ Risk Mitigation



MoveIT/ETL/File Mover	MoveIT is a file transmission tool, which is used to bi-directionally transmit data between different COMPANY XYZ applications and other financial institutions, vendors, and COMPANY XYZ locations. Logical access to MoveIT is controlled through access to Windows shares, directories, group and group access rights, files ownership rights, and user access rights.



Third-Party Risk Management (TPRM)

[redacted] maintains a third-party risk management program whereby third parties are evaluated to assess if they are a safe, sound, profitable, and controlled entity. TPRM has primary responsibility for review, tracking, and oversight of third-party relationships. Third parties are subject to risk management procedures and processes that are commensurate with the level of risk and complexity of the provided services and products. Formal risk assessment analyses of third parties are performed prior to engagement, renewal of an existing engagement, engagement of additional services, and on a recurring basis, including that [redacted] monitors vendors through service-level agreements, periodic reports, and periodic visits to the vendor facilities, and review of available SOC 1 or 2 reports.

BEST PRACTICES FOR 4TH PARTY MANAGEMENT

- **STEP 1:** Know who your Critical Vendors' critical vendors are – inventory them
- **STEP 2:** Determine if your Critical Vendors are performing any Vendor Management of their own
  - Should be listed out in their SOC 2 report
    - If so, ask see their process and results
    - If not, you've got some risk
- **STEP 3:** Work with your Vendor to improve their vendor management processes or gather documentation to perform your own due diligence
- **STEP 4:** Review your findings with your Vendor
- **STEP 5:** Work to mitigate the risk as best you can

BIG TAKEAWAYS

- MOST OF YOUR DATA TODAY DOES NOT RESIDE ON YOUR NETWORK
- VENDORS ARE CRITICAL TO BUSINESS OPERATIONS
- VENDOR RISK = BUSINESS RISK
- YOUR DATA = YOUR RESPONSIBILITY - NO MATTER WHERE THE DATA LIVES
- KNOW HOW TO MAKE GOOD VENDOR DECISIONS BASED ON RISK
- ALIGN VENDORS WITH YOUR CYBERSECURITY GOALS AND STANDARDS

GAME OVER

10

CONTINUE?

>YES NO

DOWNLOADS & MORE!

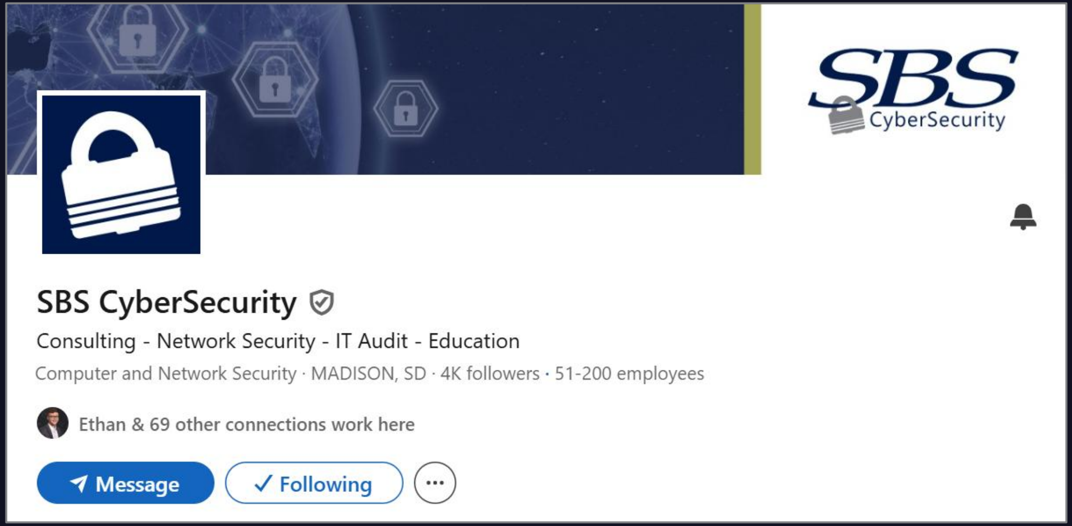
SBS CyberSecurity

- HEAD TO OUR LANDING PAGE AND DOWNLOAD SOME GOODIES!
- INCLUDING:
- CHANCE TO WIN A FREE SBS INSTITUTE WEBINAR OR MEMBERSHIP!
- THIS PRESENTATION'S SLIDE DECK!
- PRESENTATION SURVEY - WE LOVE FEEDBACK! TELL US HOW WE DID!
- FREE DOWNLOADS - 6 ISP/VM IDEAS AND TEMPLATES WE DISCUSSED TODAY!
- SIGN UP FOR IN THE WILD!

SBS INSTITUTE

HTTPS://SBSCYBER.COM/RVASEC

FOLLOW SBS ON LINKEDIN!



SBS CyberSecurity

SBS CyberSecurity

Consulting - Network Security - IT Audit - Education

Computer and Network Security · MADISON, SD · 4K followers · 51-200 employees

Ethan & 69 other connections work here

HTTPS://WWW.LINKEDIN.COM/COMPANY/SBS-CYBERSECURITY

SBS INSTITUTE - WE'VE GOT YOUR CONTENT

CE

WE

Month
conversatio
and techn
between our
exp

$
C

TRUSTED PARTNERS

SDBANKERS ASSOCIATION Educate. Advocate. Grow.
NORTH DAKOTA BANKERS ASSOCIATION
OBL Ohio Bankers League
Wisconsin Bankers Association
mba Michigan Bankers Association
LBA LouisianaBankers Association
IOWA BANKERS ASSOCIATION
ARKANSAS BANKERS ASSOCIATION
PROUD TO BE WYOMING BANKERS ASSOCIATION A WYOMING BANKER
MBA Minnesota Bankers Association The Champion for Minnesota Banks
VACB Virginia Association of Community Banks Our Mission, Community Banks!
MONTANA BANKERS ASSOCIATION
PACB Pennsylvania Association of Community Bankers
KANSAS BANKERS ASSOCIATION
NBA Nebraska Bankers Association
MBA MISSOURI BANKERS ASSOCIATION
UTAH BANKERS ASSOCIATION
NH Bankers ASSOCIATION

HTTPS://LEARNING.SBSCYBER.COM/

SBS - TOP RATED CYBER GRC COMPANY

CY

Cybe

W
strate
you
maint

ISP DEL

IT

A

Why
au
tailor
matc
cust
result

CYBER

Open-S
Intelligenc

During this fir
gather intellig
target orga
through reco
without direct

PT, VA,

TRAC: CYBER RISK MANAGEMENT SOFTWARE

TRAC
From SBS CyberSecurity

Frustration-Free Risk Management

Software Advice. ★★★★★ 4.8

GetApp USER REVIEWS ★★★★★

Capterra ★★★★★ 4.8

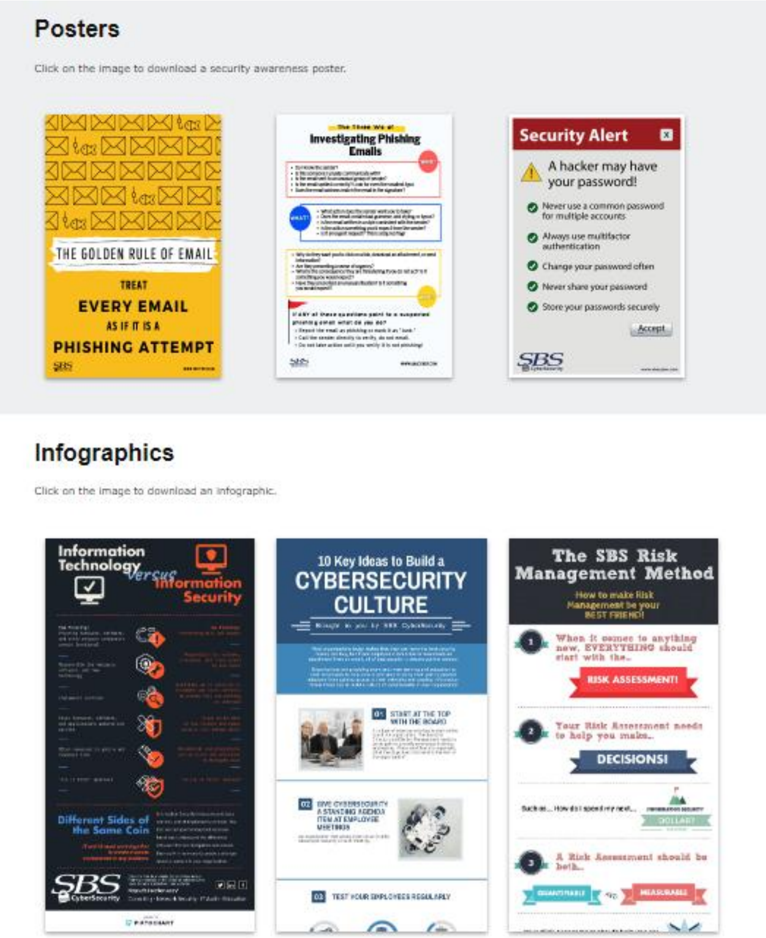
Vendor	IT	Business Continuity Management (BCM)
Action Tracking	Audit	Bank Secrecy Act (BSA)
Commercial Account Tracking (CATRAC)	Compliance	Enterprise Risk Management (ERM)
Information Security Program (ISP)	NIST CSF	

SPRING 2025 High Performer

HTTPS://SBSCYBER.COM/

Clients Love Us

COMPLIMENTARY RESOURCES



Posters

Click on the image to download a security awareness poster.

THE GOLDEN RULE OF EMAIL
TREAT EVERY EMAIL AS IF IT IS A PHISHING ATTEMPT
The Three Ws of Investigating Phishing Emails
Security Alert
A hacker may have your password!
Never use a common password for multiple accounts
Always use multifactor authentication
Change your password often
Never share your password
Store your passwords securely
Accept
SBS CyberSecurity

Infographics

Click on the image to download an infographic.

Information Technology versus Information Security
Different Sides of the Same Coin
10 Key Ideas to Build a CYBERSECURITY CULTURE
The SBS Risk Management Method
How to make Risk Management be your BEST FRIEND!
RISK ASSESSMENT!
DECISIONS!
SBS CyberSecurity

Toolkits

Cybersecurity tips, tricks, and best practice guides to help support the cybersecurity culture at your organization. Click the image to download your toolkit.

5 KEY QUESTIONS to Consider When Researching a vCISO Solution
ESSENTIAL CYBERSECURITY BEST PRACTICES
Cybersecurity Tips
Graphics to share and make aware
SECURITY AWARENESS TOOLKIT
EDUCATE YOUR EMPLOYEES, BOARD, AND CUSTOMERS
Eight Emergency Preparedness Testing Scenarios
50+ Incident Response Preparedness Checklist Items
34 Unique Ideas to Create a Culture of Cybersecurity
You Are a Technology Company
Three Steps to Changing Your Perspective on Technology and Business
SBS Institute
SBS CyberSecurity

Tipsheets

Cybersecurity tips, tricks, and best practice guides to help support the cybersecurity culture at your organization. Click the image to download your toolkit.

SBS SECURING REMOTE WORK CHECKLIST
SBS MICROSOFT OFFICE 365 SECURITY SUGGESTIONS
SBS MICROSOFT 365 SECURITY SUGGESTIONS
SBS INVESTIGATING PHISHING EMAILS
SBS STRONGER PASSWORDS, STRONGER SECURITY

SBS INSTITUTE

HTTPS://LEARNING.SBSCYBER.COM/RESOURCELIBRARY

IN THE WILD

Email Jon to receive our weekly top-secret cybersecurity newsletter… or click here:

SIGN UP TODAY

CONTACT INFORMATION

JON WALDMAN

- President, Partner
- CISA, CRISC, CDPSE
- Master's of Information Assurance, Dakota State University
- Mission: help you make better cybersecurity decisions
- Phone: 605-380-8897
- jon@sbscyber.com
- www.sbscyber.com