

# Third-Party Vendor Risk Management

Enhancing Information Security and Compliance

Information Security and Privacy Office (ISPO)




ITS   
SEMINOLE  
SHOWCASE

# Learning Outcomes



Today we will discuss the Third-Party Vendor Risk Management Process

- We will discuss how we created this process
  - Why it's important to the university
  - Why it is important to an FSU employee
- 

# Background



Addressing May 2021 Audit Findings

## **Context of the Audit:**

1. In May 2021, a comprehensive audit identified crucial areas for improvement in our vendor management processes.
2. The audit highlighted the need for enhanced scrutiny of third-party vendors providing essential business functions.

## **Key Findings:**

1. The audit revealed gaps in information security protocols concerning third-party vendors.
2. There was a noted lack of consistent independent security audits across our vendor network.

# Action Items

Compile a list a list of business essential services based on Business Impact Analysis (BIA) results



Established a review process for web/cloud services providing essential business functions



Required vendors to include provisions for independent information security audits, accessible for university review



Required vendors to submit SOC II reports or complete self risk assessments

# Controls Development



## Written Processes and Procedures

Developed comprehensive written processes and procedures that align with our organizational policies.

These documents guide the systematic implementation of security measures across all vendor engagements.

## Third-Party Risk Self-Assessment Survey

Created a self-assessment survey tool for vendors lacking a current SOC II report.

This survey helps in evaluating the risk level and security posture of these vendors, ensuring we have a consistent understanding of their compliance status.

## Integration with ISPO Standard

Ensured that the new processes and the self-assessment survey are integrated with the ISPO Standard Terms & Conditions.

Aligned these controls with the requirements of SOC II audits to maintain consistency and comprehensiveness in our security assessments.

# ISPO Standard T&C Updates

<b>Inclusion of SOC II Audits:</b>	<b>Third-Party Risk Self-Assessment Requirement</b>	<b>Integration with Business Impact Analysis and Disaster Recovery</b>
ISPO standard terms and conditions now mandatorily include annual SOC II audits for Business Essential vendors.	In cases where a vendor hasn't completed a SOC II audit, we now require them to complete a third-party risk self-assessment.	This alignment strengthens our overall approach to risk management and business continuity
This ensures consistent adherence to recognized cybersecurity standards among our vendors.	This assessment, developed by FSU, allows us to evaluate the vendor's risk profile and security measures.	The updated terms and conditions have been integrated with Business Impact Analysis and Disaster Recovery processes.

# Deliverables



## Annual Reviews of Policies, Standards, and Procedures:

Successfully conducted annual reviews to ensure that our policies, standards, and procedures remain current and effective.

These reviews are crucial in identifying areas for improvement and updating our practices to reflect the latest security trends and requirements.

## Alignment with Seminole Secure Cycle:



Aligned third-party vendor risk assessments with the tri-annual Seminole Secure cycle.

This alignment facilitates the continuous functioning of essential university business functions and services, tailored to meet the evolving needs of the FSU community.




# Contract Status Confirmation:



## Contract Confirmation and Updating:

- ✓ Conducted a comprehensive review of all existing vendor contracts to confirm their current status with FSU.
- ✓ Updated contract details in our records to reflect the latest information, ensuring accuracy in our vendor management system.

## Preparation for Contract Renewals:

- ✓ Initiated the process of drafting and proposing modifications for upcoming contract renewals.
  - ✓ Focus on integrating enhanced security requirements and compliance clauses in line with our updated ISPO standards and policies.
- 





# Contract Inventory Initiation



## Initiation of Manual Contract Inventory:

- ✓ Began a detailed manual inventory process for all existing vendor contracts.
- ✓ This initiative is crucial for obtaining a clear, current view of our contractual relationships and obligations.

## Evaluating SOC/ISO Requirements:



- ✓ A key focus of the inventory is to evaluate how each contract addresses SOC and ISO compliance requirements.
- ✓ Assessing for SOC/ISO clauses to ensure vendors meet the rigorous security and quality standards FSU adheres to.



# COSO to NIST Crosswalk

## COSO FRAMEWORK

- Focus: COSO (Committee of Sponsoring Organizations) primarily addresses internal control over financial reporting and broader organizational objectives. The majority of SOC II reports follow the COSO framework.
- Purpose: It aims to provide "reasonable assurance" regarding the achievement of objectives in operations, financial reporting, and compliance.

## NIST Framework (NIST 800-53)

- Focus: NIST (National Institute of Standards and Technology) primarily focuses on cybersecurity and information security.
- Purpose: It provides a flexible and risk-based approach to managing and securing information systems.

## Similarities between COSO and NIST

- Effective Internal Controls: Each framework aims to establish and maintain effective internal controls within organizations.

# Vendor Risk Scores



## Explanation of Risk Recon Score

ISPO enhanced vendor security assessments by integrating Risk Recon scoring.

This approach provides an additional layer of visibility into each vendor's security posture, allowing for a more nuanced ranking of vulnerabilities.

## Scoring Methodology

Utilized NIST 800-53 baselines to establish control risk levels, ranging from low to high.

Risk levels are numerically assigned: 1 for low risk, 2 for medium, and 3 for high risk. Scores are assigned based on risk severity to the university after reviewing SOC II and self-risk assessment exceptions.

# Analysis Insights

## Implications of the Analysis:

The amalgamation of SOC II reports, self-risk assessments, and Risk Recon scores offered a holistic view of each vendor's security posture.

This approach enabled us to identify specific areas where vendors excel in security practices and areas needing improvement.

These insights are pivotal for informed decision-making regarding ongoing and future vendor relationships.

# Ongoing efforts

## Implications of the Analysis:

- Phase 1 achievements and alignment with Seminole Secure
- Future assessments for high or moderate-risk data vendors
- Collaboration with Procurement for contractual language alignment
- Continuous monitoring of vendor security posture.
- Further assessments planned for vendors handling high or moderate-risk data.

# By The Numbers

**Unique vendors identified**

**122**

# Self Risk Assessment

File Home Insert Draw Page Layout Formulas Data Review View Automate Help Acrobat

Clipboard Font Alignment Number Styles Cells Editing Sensitivity Add-ins Analyze Data Adobe Acrobat

Comments Share

Formula Bar

**Third-Party Risk Summary**

Third-party Risk Assessment Areas	Risk Exposure Score
Company Controls & Overview	1.00
Business Continuity & Management Processes	1.33
Security Systems Engineering	1.00
Security Monitoring Systems	1.00
Data & Data Center Management	1.00
Lower number is better	
<b>Overall Risk Exposure Score</b>	<b>Low To Moderate</b>

**Interpreting Third-Party Risk Exposure Based on Self-Assessment Scores**

**Third-Party Risk Evaluation Scale**

Description	Acceptable Risk Exposure Score Range	Moderate to High Risk Score 2-3	Low To Moderate Risk Score 1-2	Nominal to Low Risk Score 0-1
Company Controls & Overview	<=2.4	Accept if Not Applicable or With Compensating Controls	Acceptable Risk with/without Compensating Controls	Acceptable Risk
Business Continuity & Management Processes	<=2.4	Accept with Compensating Controls	Acceptable Risk with/without Compensating Controls	Acceptable Risk
Security Systems Engineering	<=2.4	Accept with Compensating Controls	Acceptable Risk with/without Compensating Controls	Acceptable Risk
Security Monitoring Systems	<=2.4	Unacceptable due to Very High Risk	Acceptable Risk with/without Compensating Controls	Acceptable Risk
Data & Data Center Management	<=2.4	Accept with Compensating Controls	Acceptable Risk with/without Compensating Controls	Acceptable Risk

**Compensating Control: A management, operational, and/or technical safeguard or approach employed to provide comparable levels of protection.**

Third-Party Risk Exposure Company Controls & Overview Business Continuity & Managemen Security Systems Engineering Security Monitoring Systems Data & Data Center

Accessibility: Investigate 70%

# Vendor Risk Analysis

File Home Insert Draw Page Layout Formulas Data Review View Automate Help Acrobat Table Design

Comments Share

Paste Font Alignment Number Styles Cells Editing Sensitivity Add-ins Analyze Data Adobe Acrobat

K6 : X ✓ fx 1

A B C D E F G H I J K L

1 **VENDOR RISK SUMMARY**

2

VENDOR	RISK RECON SCORE	RISK SCORE	VENDOR ANALYSIS	SOC II/RISK ASSESSMENT	DATE REVIEW	STATUS	COMMENTS
Ac...	8	1.7	<a href="#">Yes</a>	<a href="#">Yes</a>	1/12/2024		
Ad....	7.2	1.0	<a href="#">Yes</a>	<a href="#">Yes</a>	12/6/2023		
Atla...	8.2	1.0	<a href="#">Yes</a>	<a href="#">Yes</a>	12/6/2023		
A...	7	1.0	<a href="#">Yes</a>	<a href="#">Yes</a>	1/12/2024		
Bla....	7.8	1.5	<a href="#">Yes</a>	<a href="#">Yes</a>	1/12/2024		
Ca.....	8.7	1.2	<a href="#">Yes</a>	<a href="#">Yes</a>	1/12/2024		
Ci....	8.4	2.7	<a href="#">Yes</a>	<a href="#">Yes</a>	1/16/2024		
Co...	8.6	2.3	<a href="#">Yes</a>	<a href="#">Yes</a>	1/11/2024		
Clo...	6.5	1.0	<a href="#">Yes</a>	<a href="#">Yes</a>	1/11/2024		
Ja...	9.4	1.0	<a href="#">Yes</a>	<a href="#">Yes</a>	1/11/2024		
Li...		1.7	<a href="#">Yes</a>	<a href="#">Yes</a>	1/16/2024		
Ma....	5	1.0	<a href="#">Yes</a>	<a href="#">Yes</a>	1/11/2024		
Mi....	9.3	3.0	<a href="#">Yes</a>	<a href="#">Yes</a>	1/11/2024		

RATING_NO	RISK LEVEL
1	LOW RISK
2	MEDIUM RISK
3	HIGH RISK

Ready Accessibility: Investigate 90%



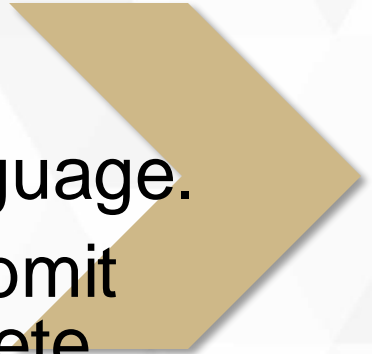
# Why is This Important?



- Identify our essential applications for the university.
- Ensure that we do reviews of our vendors and products.
- Meet legal and compliance requirements.
- Strengthen our security posture.
- Have visibility into the security of vendors that have our data.
- The ability to audit third party vendor security controls.
- To help reduce the likelihood of a breach.



# Recap



- This process originated from an audit finding.
- Compiled a list of business essential services
- Established a review process for those services
- Created policies and procedures
- Required provisions be included in contract language.
- Required vendors to submit SOC II reports or complete self risk assessments.
- Created a scoring system to rank vendors
- Review vendors on an ongoing basis

# CONTACT INFORMATION



- Keith Bennett (IT Security Specialist)

- Email:  
keith.bennett@fsu.edu

- Jeremy Anderson( IT Security Specialist)

- Email:  
jjanderson@fsu.edu

# Questions?



Please Provide Feedback!

