



A Standards-Based Approach to Assessing Your Organization's Cybersecurity Maturity

BSides Austin 2019

About Us

Josh Sokol (@joshsokol)

- Information Security Program Owner @ National Instruments
- Creator & CEO of SimpleRisk
- Former OWASP Board member

Alex Polimeni

- IT Compliance Manager @ National Instruments
- Animal Enthusiast
- First time speaker
- Once got stuck in a cave

Security

Define the technical controls for the organization.

Enforcement of the organizational controls.

Compliance

Helps to define policies, guidelines, standards and procedures.

Validates compliance with defined requirements.

Background

We were asked to
assess our
organization's
cybersecurity maturity
and create a roadmap
for the National
Instruments
Information Security
Program

Gartner is great, but
provides very high level
advice and is far from a
roadmap.

What is Organizational Cybersecurity Maturity?


This speaks to how effective the people, processes and technology are at mitigating cybersecurity risk.

An immature control would be people/process/technology that management can/should place little confidence in regarding their overall cybersecurity risk mitigation plan.

A mature control would be people/process/technology that management can/should place more confidence in regarding their overall cybersecurity risk mitigation plan.

Example: Endpoint with only basic password protection

Example: Endpoint with full-disk encryption, complex password requirements, multi-factor authentication, etc.




So how do you
create a
roadmap?

Start with where you
are.

End with where you're
going.

Everything in-between
is your roadmap.



How do you
assess where
you are?

We need to find a control framework
that embodies whatever it is that we
are looking to assess.

Frameworks Considered

NIST 800-53

NIST 800-171

NIST Cybersecurity Framework

ISO 27001



NIST Cybersecurity Framework (CSF)

- Free
- Best practices
- Relatively complete

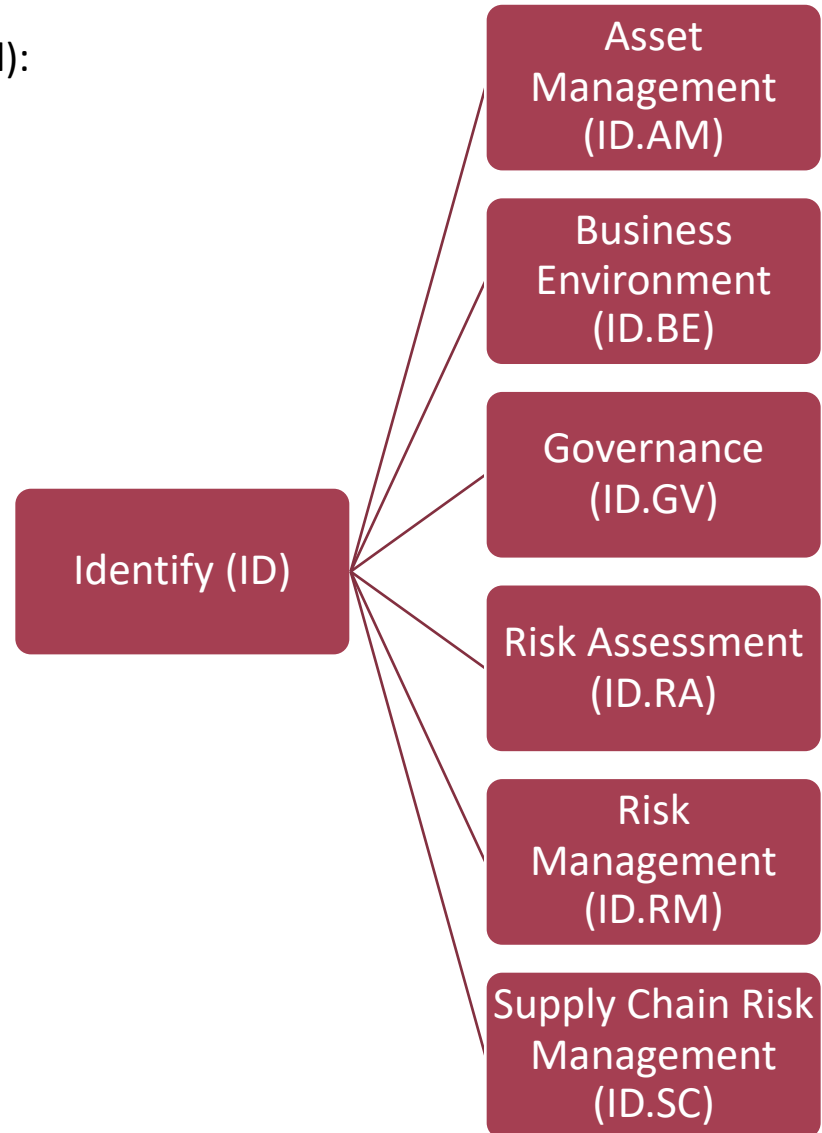
NIST Cybersecurity Framework

- 5 Functions:



NIST Cybersecurity Framework

Each function has several categories (23 total):



NIST Cybersecurity Framework

Each category has one or more sub-categories/controls (108 total):

<u>Category</u>	<u>Subcategory</u>
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-1: Physical devices and systems within the organization are inventoried
	ID.AM-2: Software platforms and applications within the organization are inventoried
	ID.AM-3: Organizational communication and data flows are mapped
	ID.AM-4: External information systems are catalogued
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

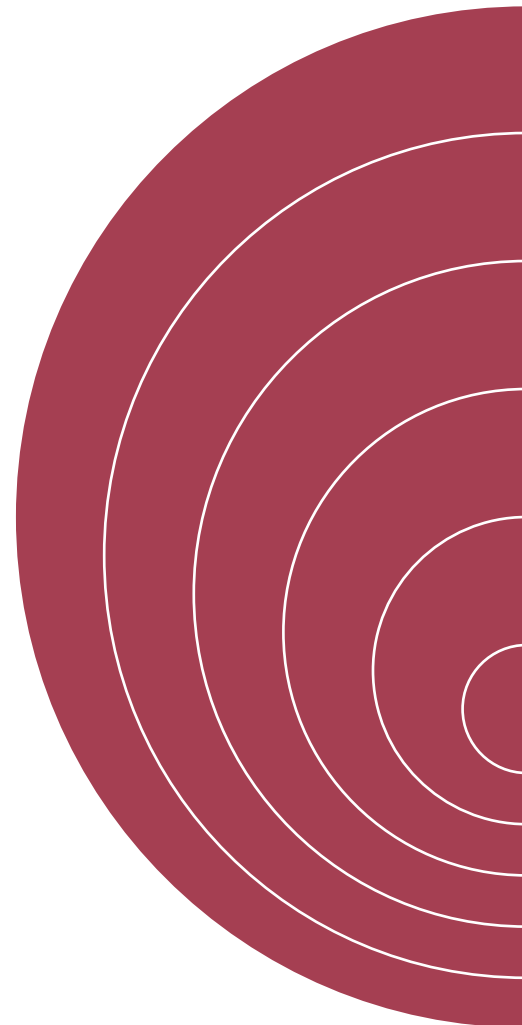


Assessing Your Current Maturity

(Or at least how we did it)

Establish Criteria for Assessing Yourself

We defined our criteria by reviewing the NIST CSF and COBIT. We eventually landed on the following values:



Optimized Process	<ul style="list-style-type: none">Automated process with a closed feedback loop – we know it works and there is little left to improve upon
Predictable Process	<ul style="list-style-type: none">Established + it is either audited by management or third parties with consistent results
Established Process	<ul style="list-style-type: none">An owner is identified and held accountable for the area; Formalized policies and procedures exist
Managed Process	<ul style="list-style-type: none">An owner has been identified, some documentation exists but there is a lack of formal documentation
Performed Process	<ul style="list-style-type: none">Individuals do it, but it is defined mainly on tribal knowledge and answers will vary between teammates
Not implemented / Not Applicable	

Assess Your Current Maturity

Category	Subcategory	Current Capability
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-1: Physical devices and systems within the organization are inventoried	Optimizing Process
	ID.AM-2: Software platforms and applications within the organization are inventoried	Predictable Process
	ID.AM-3: Organizational communication and data flows are mapped	Established Process
	ID.AM-4: External information systems are catalogued	Managed Process
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Performed Process
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third party stakeholders (e.g., suppliers, customers, partners) are established	Not Implemented


Advice: Be Honest with Yourself

- While your understanding of the environment is a gut-check at times, you should be able to provide reasonable examples to support your grade or refute others.
- Err on the side of caution – being too optimistic can cause trouble from a compliance perspective.



Advice: Consider your environment as a whole – not just individual users or teams

- How standard is the process performed? If you went to two different/relevant managers, would you get the expected response?



Advice: Be prepared to “defend” your responses

- Keep notes, this will both help with regards to how you judge your future state and also keep your thoughts consistent throughout the process.
- This likely will go to upper levels of IT management. Inaccuracies will lead reviewers to question the entire gap assessment.



Assess Your Desired Maturity

Need to Understand Current Risks / Regulatory Compliance Requirements / Management's Appetite

The regulatory requirements should shape your minimum requirements. How do we comply with all mandatory regulations in the most efficient means possible.

Risk appetite should play a major part and this will require you to calibrate with management. Your overall goal is to set your desired state to the value that gives management comfort over the risk.

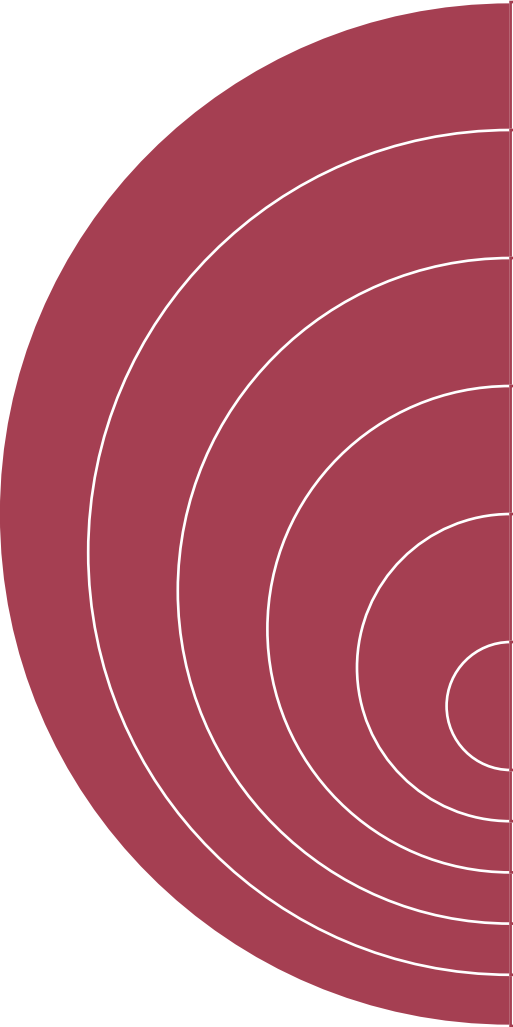


Remind Yourself to Be Reasonable – Not All Risks Require Optimized Solutions

- This is especially hard for folks routinely audited. Do not let perfection become the enemy of good.

Use the Same Assessment Criteria for Current and Desired State

We defined our criteria by reviewing the NIST CSF and COBIT. We eventually landed on the following values:



Optimized Process	<ul style="list-style-type: none">Automated process with a closed feedback loop – we know it works and there is little left to improve upon
Predictable Process	<ul style="list-style-type: none">Established + it is either audited by management or third parties with consistent results
Established Process	<ul style="list-style-type: none">An owner is identified and held accountable for the area; Formalized policies and procedures exist
Managed Process	<ul style="list-style-type: none">An owner has been identified, some documentation exists but there is a lack of formal documentation
Performed Process	<ul style="list-style-type: none">Individuals do it, but it is defined mainly on tribal knowledge and answers will vary between teammates
Not implemented / Not Applicable	

Assess Your Desired Maturity

Category	Subcategory	Current Capability	Desired Capability
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-1: Physical devices and systems within the organization are inventoried	Optimizing Process	Optimizing Process
	ID.AM-2: Software platforms and applications within the organization are inventoried	Predictable Process	Predictable Process
	ID.AM-3: Organizational communication and data flows are mapped	Established Process	Established Process
	ID.AM-4: External information systems are catalogued	Managed Process	Established Process
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Performed Process	Established Process
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third party stakeholders (e.g., suppliers, customers, partners) are established	Not Implemented	Predictable Process

Remember to to be reasonable – not all risks require optimized solutions

Add Notes and Assign Ownership

Category	Subcategory	Current Capability	Desired Capability	Capability Comments	Owners
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-1: Physical devices and systems within the organization are inventoried	Optimizing Process	Optimizing Process	Is this the real life?	IT Pre-purchase - Procurement
	ID.AM-2: Software platforms and applications within the organization are inventoried	Predictable Process	Predictable Process	Is this just fantasy?	IT Pre-purchase - Procurement
	ID.AM-3: Organizational communication and data flows are mapped	Established Process	Established Process	Caught in a landslide.	Dataflow Database/ETL/IM Communication
	ID.AM-4: External information systems are catalogued	Managed Process	Established Process	No escape from reality.	IT Pre-purchase - Procurement
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Performed Process	Established Process	Open your eyes	IT
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third party stakeholders (e.g., suppliers, customers, partners) are established	Not Implemented	Predictable Process	Look up to the sky and see.	Freddie Mercury

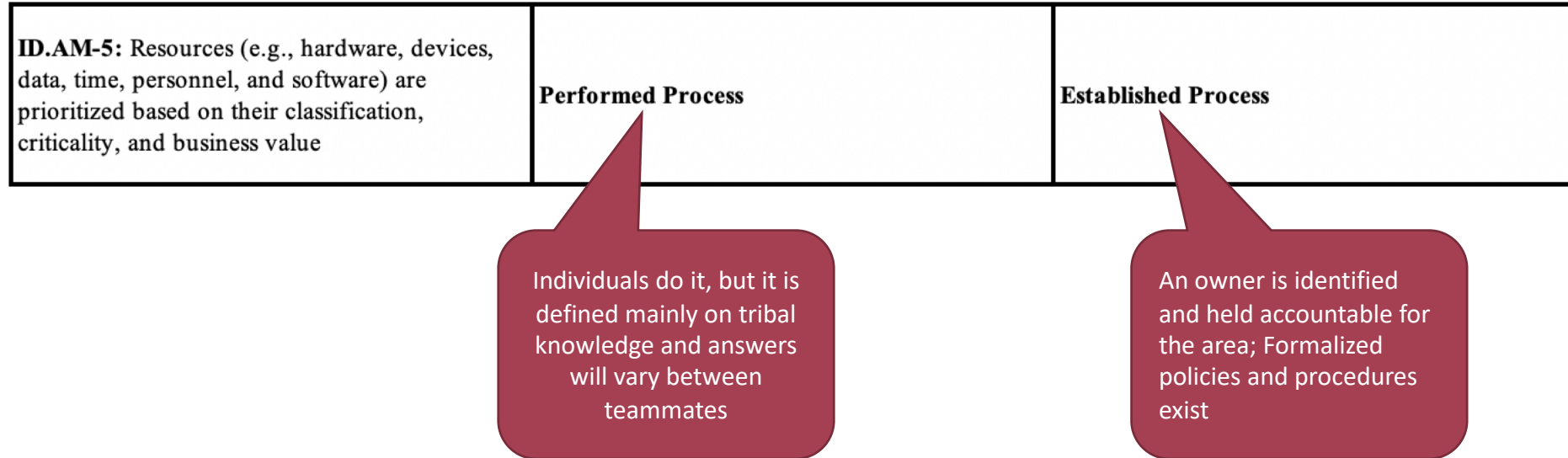


Defining Risks

Where There's a Gap, There's a Risk

Category	Subcategory	Current Capability	Desired Capability
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 organization objectives and the organization's risk strategy	ID.AM-1: Physical devices and systems within the organization are inventoried	Optimizing Process	Optimizing Process
	ID.AM-2: Software platforms and applications within the organization are inventoried	Predictable Process	Predictable Process
	ID.AM-3: Organizational communication and data flows are mapped	Established Process	Established Process
	ID.AM-4: External information systems are catalogued	Managed Process	Established Process
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Performed Process	Established Process
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third party stakeholders (e.g., suppliers, customers, partners) are established	Not Implemented	Predictable Process


Risk Example



Risk

No defined processes or ownership for the prioritization of resources based on classification, criticality, and business

Using a GRC Tool to Capture Risks

 SimpleRisk

GovernanceRisk ManagementComplianceAsset ManagementAssessmentsReportingConfigure

Admin

+New Risk...

1 Submit Risk

2 Plan Mitigation

3 Perform Reviews

4 Plan Projects

5 Review Regularly

Subject: No defined process or ownership for the prioritization of resources based on classification, criticality, and business

Category: --

Site/Location: --

External Reference ID:

Control Regulation: --

Control Number:

Affected Assets:

Technology: None selected

Team: None selected

Additional Stakeholders: None selected

Owner: --

Owner's Manager: --

Risk Source: --

Risk Scoring Method: Classic

Current Likelihood: --

Current Impact: --

Risk Assessment:

Additional Notes:

Supporting Documentation

Choose File0 File Added

Max 5 Mb

Complete the form above to document a risk for consideration in Risk Management Process

Clear FormSubmit Risk

Determining a Risk Score

We assigned a risk value based upon:

- The degree of a difference there was between current and desired state
- The potential operational and financial impact given a complete failure of the process
- The likelihood of a complete failure of the process.

Current Likelihood: --

Current Impact: --

Risk Assessment:

- Remote
- Unlikely
- Credible
- Likely
- Almost Certain

Current Impact: --

Risk Assessment: --

Additional Notes:

- Insignificant
- Minor
- Moderate
- Major
- Extreme/Catastrophic

Populate Locations, Teams, Owners, etc

Subject:	No defined process or ownership for the prioritization of resources based on classification, criticality, and business		
Category:	Policy and Procedure	Risk Source:	Process
Site/Location:	All Sites	Risk Scoring Method:	Classic
External Reference ID:		Current Likelihood:	Almost Certain
Control Regulation:	NIST Cybersecurity Framework (CSF)	Current Impact:	Moderate
Control Number:	ID.AM-5	Risk Assessment:	We currently do not have any defined process or ownership for the prioritization of resources based on classification, criticality, and business.
Affected Assets:			
Technology:	All	Additional Notes:	
Team:	IT Systems Management	Supporting Documentation	Choose File 0 File Added Max 5 Mb
Additional Stakeholders:	None selected		
Owner:	Josh Sokol		
Owner's Manager:	Josh's Boss		

Risk Score is Automatically Calculated

ID	Status	Subject	Inherent Risk	Days Open	Next Review Date
1001	New	No defined process or ownership for the prioritization of resources based on classification, criticality, and business	6 	0	UNREVIEWED

Plan Your Mitigations

This is where you document the desired maturity and how to get there:

Details	Mitigation	Review
Mitigation	03/28/2019	Current Solution:
Submission Date:		Currently being performed by individuals on an ad-hoc basis.
Planned Mitigation		
Date:		
Planning Strategy:	Mitigate	Security Requirements:
Mitigation Effort:	Considerable	We need to document the process for prioritization of resources based on classification, criticality, and business
Mitigation Cost:	\$0 to \$100,000	Security Recommendations:
Mitigation Owner:	Josh Sokol	
Mitigation Team:	IT Systems Management	
Mitigation Percent:	0%	Supporting Documentation:
		None



The Roadmap

Prioritizing What to Do First

- ✓ **Burning Fires:** These are high-priority items. This is predominately risks that were scored by high impact and high likelihood. These are items that could cause serious business interruption or financial loss to the company.
 - Use the “High Risk Report” in SimpleRisk to identify these

Total Open Risks: 239

Total Very High Risks: 7

Very High Risk Percentage: 2.93%

Total High Risks: 17

High Risk Percentage: 7.11%



ID#	Status	Subject	Inherent Risk	Submitted	Mitigation Planned	Management Review
1278	Mgmt Reviewed	RISK SUBJECT DATA HAS BEEN CENSORED	10	11/20/2017 1:00 AM CST	NO	PAST DUE
1285	Mgmt Reviewed		10	03/01/2018 1:00 AM CST	YES	PAST DUE
1294	Mgmt Reviewed		10	05/15/2018 7:11 PM CDT	NO	PAST DUE
1296	Mgmt Reviewed		10	07/24/2018 11:12 AM CDT	NO	PAST DUE
1330	New		10	02/04/2019 1:00 AM CST	NO	NO
1341	New		10	02/04/2019 3:11 PM CST	NO	NO
1290	Mgmt Reviewed		9	04/24/2018 12:00 AM CDT	NO	PAST DUE
1314	New		8	02/04/2019 1:00 AM CST	NO	NO
1316	New		8	02/04/2019 11:22 AM CST	NO	NO
1317	New		8	02/04/2019 11:27 AM CST	NO	NO

Prioritizing What to Do First

- ✓ **Burning Fires:** These are high-priority items. This is predominately risks that were scored by high impact and high likelihood. These are items that could cause serious business interruption or financial loss to the company.
 - Use the “High Risk Report” in SimpleRisk to identify these
- ✓ **Quick Wins:** Is there any low-hanging fruit. These are things you can accomplish without much assistance from other teams or that require little financial or personnel investment.
 - Use the “Risk Advice” report in SimpleRisk to identify these

Risk Advice

Your risk level distribution is as follows:

- Very High: 7
- High: 17
- Medium: 72
- Low: 143

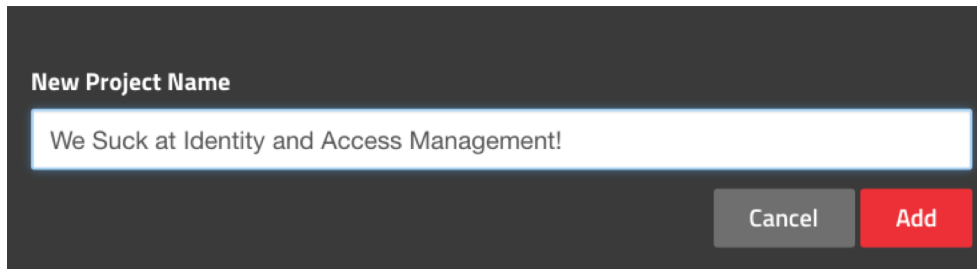
Recommendation(s):

- Mitigating these risks would provide the highest risk reduction for the lowest level of effort:

1)	RISK SUBJECT DATA HAS BEEN CENSORED	Trivial	3.6
2)		Trivial	3.6
3)		Trivial	3.6
4)		Trivial	2.4
5)		Trivial	2.4
6)		Trivial	1.8
7)		Trivial	1.6
8)		Trivial	1.6
9)		Trivial	1.2
10)		Trivial	0.8

Prioritizing What to Do First

- ✓ **Burning Fires:** These are high-priority items. This is predominately risks that were scored by high impact and high likelihood. These are items that could cause serious business interruption or financial loss to the company.
 - Use the “High Risk Report” in SimpleRisk to identify these
- ✓ **Quick Wins:** Is there any low-hanging fruit. These are things you can accomplish without much assistance from other teams or that require little financial or personnel investment.
 - Use the “Risk Advice” report in SimpleRisk to identify these
- ✓ **Long-Term Work:** Is this a thematic issue (example: your company lacks formal documentation). Maybe you should consider a policy revamp project.
 - Define a project in SimpleRisk to group these risks together

A screenshot of a software dialog box titled "New Project Name". It features a text input field containing the text "We Suck at Identity and Access Management!". Below the input field are two buttons: a grey "Cancel" button and a red "Add" button.

New Project Name

We Suck at Identity and Access Management!

Cancel Add

Prioritizing What to Do First

- ✓ **Burning Fires:** These are high-priority items. This is predominately risks that were scored by high impact and high likelihood. These are items that could cause serious business interruption or financial loss to the company.
 - Use the “High Risk Report” in SimpleRisk to identify these
- ✓ **Quick Wins:** Is there any low-hanging fruit. These are things you can accomplish without much assistance from other teams or that require little financial or personnel investment.
 - Use the “Risk Advice” report in SimpleRisk to identify these
- ✓ **Long-Term Work:** Is this a thematic issue (example: your company lacks formal documentation). Maybe you should consider a policy revamp project.
 - Define a project in SimpleRisk to group these risks together
- ✓ **Management Goals & Objectives:** Does your company or department currently have any ongoing goals or initiatives that these projects can support.
 - **Example:** If your company is trying to reduce office space; prioritizing a remote access policy may be a quick win that supports leadership initiatives.
 - **Example:** If your company is currently trying to make a push toward increasing automation, providing guidance regarding processes needed “Optimized” controls may be appropriate. This will help them build out their pipeline while accomplishing Security & Compliance goals.

Ownership



Management owns the control environment and any necessary remediation. They are responsible for defining the course of action and direct any projects.



Management consults Security and Compliance. Compliance and Security are Centers of Excellence. We provide valuable consultative services, but we do not engineer or implement changes.



Security and Compliance validate Management has effectively mitigated the identified risks and communicates overall status to IT Leadership



Conclusions

Conclusions

1

This technique can be used for assessing the maturity of just about anything as long as you have a standard to base it off of

2

Leveraging NIST CSF is great for assessing an overall Information Security program

3

It's all about determining where you are and where you need to get to

4

Risk management is an integral part of the process, but SimpleRisk is FREE!

THANK YOU



JOSH SOKOL
@joshsokol



ALEX POLIMENI
Instagram: tailsofdoggowaggins