FROM CONTROLS TO CLARITY: SIMPLIFYING FAIR USING THE NIST CSF

October 22, 2024

protiviti®
Global Business Consulting

Ostrich Cyber-Risk

Our Speakers

Daniel Stone

Director,
Technology Risk & Resilience,
Protiviti

Jack Nelson

Senior Manager,
Technology Risk & Resilience,
Protiviti

Adam Lamantia

Director,
Enterprise Sales,
Ostrich

Ostrich Cyber-Risk protiviti®

Introduction

1. Risk vs. Controls Assessments
2. Why Integrate?
3. Example Outputs
4. Panel Discussion

Ostrich Cyber-Risk protiviti

Risk Vs. Control Assessments

protiviti®

Ostrich Cyber-Risk

The Cybersecurity Framework

Three Primary Components:

Core

✓Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

Profiles

✓Alignment of an organization's requirements and objectives, risk appetite and resources ***using*** the desired outcomes of the Framework Core

Implementation Tiers

✓A qualitative measure of organizational cybersecurity risk management practices

Ostrich Cyber-Risk protiviti

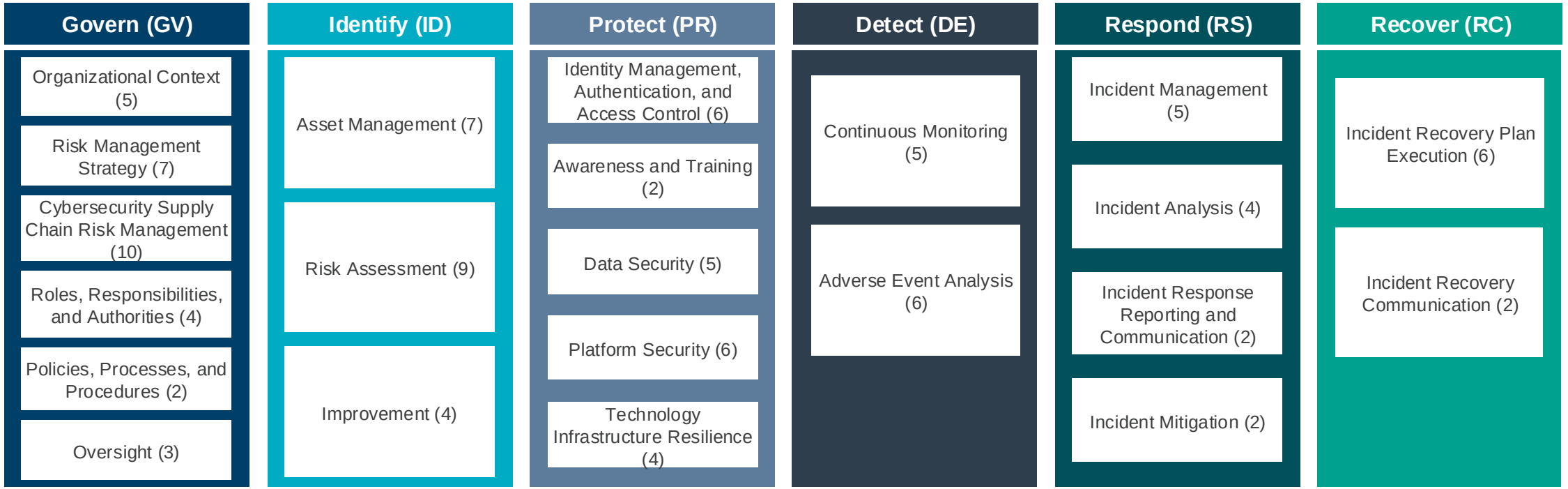
NIST Cybersecurity Framework

The National Institute of Standards in Technology (NIST)'s Cybersecurity Framework (CSF) was created to evaluate and guide cybersecurity programs and has become a de facto standard across the US and is often looked to by regulators as a means to implement and evaluate tools, practices, and standards. Our approach leverages the NIST CSF, other related framework (e.g., COBIT, ISO, ITIL), and our experience helping other similar companies.

NIST 2.0 Framework Overview

6 functions › 22 categories › 106 subcategories

Informative references based on industry best practices (NIST SP 800-53 and CMMI)



Control Assessment Overview

Objectives

Assess Control Maturity

Leverage a common framework (such as the NIST CSF or ISO 27000x) to assess the maturity of key cybersecurity controls across the environment.

Identify Gaps

Identify areas where control maturity can be improved and deliver detailed recommendations to address gaps between current and target state.

Develop Roadmap

Leverage understanding of environment gained during control assessment to plan future remediation actions aimed at addressing gaps.

Evaluate Against Peers

Benchmark control maturity relative to peers to understand where the organization sits relative to peers of a similar size or in the same industry.

Risk Assessment Overview

Objectives

Understand Threat Landscape

Conduct threat intelligence to understand the attack vectors most likely to be attempted against organizational assets.

Identify Top Risks

Translate threat intelligence to discrete, actionable, and organization-specific risk events that are most likely to occur in the current-state environment.

Analyze Control Risk

Identify controls most likely to influence top risks, expressing the expected impact of control gaps against the organization's risk landscape.

Define Return on Investment

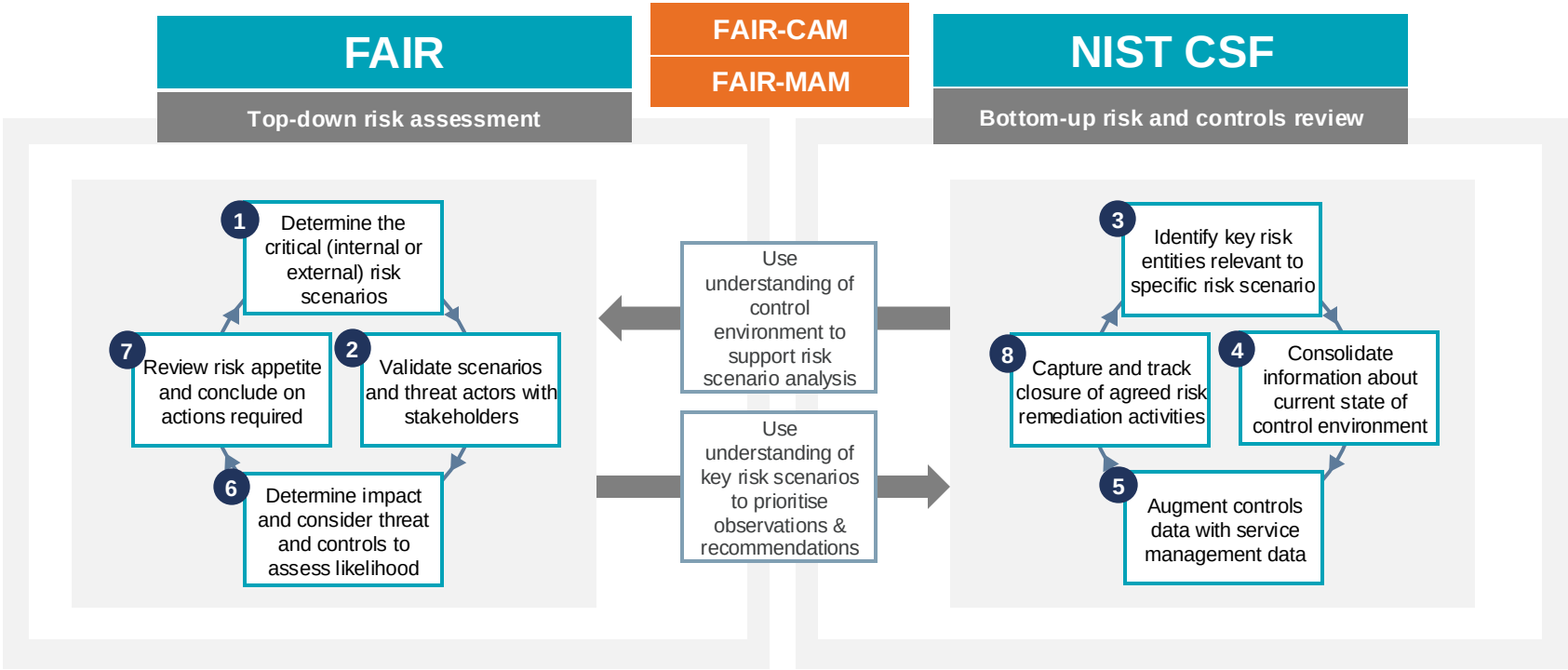
Prioritize control changes based on their expected, dollar-value impact on the organization's risk posture.

Ostrich Cyber-Risk protiviti

Risk Assessment vs. Controls Assessment

Integrating a bottom-up approach with a top-down approach that is focused on risk is a critical step that is missed in many risk assessment activities. It is much easier to get executive management engaged and to have meaningful discussions about business impact and risk appetite when risks are presented in this way.

A bottom up approach is more valuable when informed by a top-down approach. A top-down approach is not intended to achieve the same level of technical review and recommendation that a more detailed review may uncover, such as through a bottom-up controls assessment.



Ostrich Cyber-Risk protiviti

Control & Risk Synergy

Control Assessment Objectives

Assess Control Maturity

Leverage a common framework (such as the NIST CSF or ISO 27000x) to assess the maturity of key cybersecurity controls across the environment.

Identify Gaps

Identify areas where control maturity can be improved and deliver detailed recommendations to address gaps between current and target state.

Develop Roadmap

Leverage understanding of environment gained during control assessment to plan future remediation actions aimed at addressing gaps.

Evaluate Against Peers

Benchmark control maturity relative to peers to understand where the organization sits relative to peers of a similar size or in the same industry.

Control Maturity Informs Top Risks

Vulnerability (or susceptibility) to threats, and lack of controls to address Loss Magnitude, should **inform risk assessments**.

- Low maturity in PR.AA controls increases vulnerability to Ransomware, Hacking, Privilege Misuse, Misdelivery, and many other risk scenarios.
- Low maturity in RS.RP controls increases Loss Magnitude across a wide variety of scenarios.
- Each NIST CSF Category may have many threat scenarios or risks they project against.

Risk Assessment Objectives

Understand Threat Landscape

Conduct threat intelligence to understand the attack vectors most likely to be attempted against organizational assets.

Identify Top Risks

Translate threat intelligence to discrete, actionable, and organization-specific risk events that are most likely to occur in the current-state environment.

Analyze Control Risk

Identify controls most likely to influence top risks, expressing the expected impact of control gaps against the organization's risk landscape.

Define Return on Investment

Prioritize control changes based on their expected, dollar-value impact on the organization's risk posture.

Control Assessment Overview

Objectives

Assess Control Maturity

Leverage a common framework (such as the NIST CSF or ISO 27000x) to assess the maturity of key cybersecurity controls across the environment.

Identify Gaps

Identify areas where control maturity can be improved and deliver detailed recommendations to address gaps between current and target state.

Develop Roadmap

Leverage understanding of environment gained during control assessment to plan future remediation actions aimed at addressing gaps.

Evaluate Against Peers

Benchmark control maturity relative to peers to understand where the organization sits relative to peers of a similar size or in the same industry.

Sample Deliverables

Executive Summary | Observations | Roadmap

Observation 1.1

Efforts to improve integration of HR systems and identity management tools have not progressed in line with business requirements. The primary root cause of

Observation 1.2

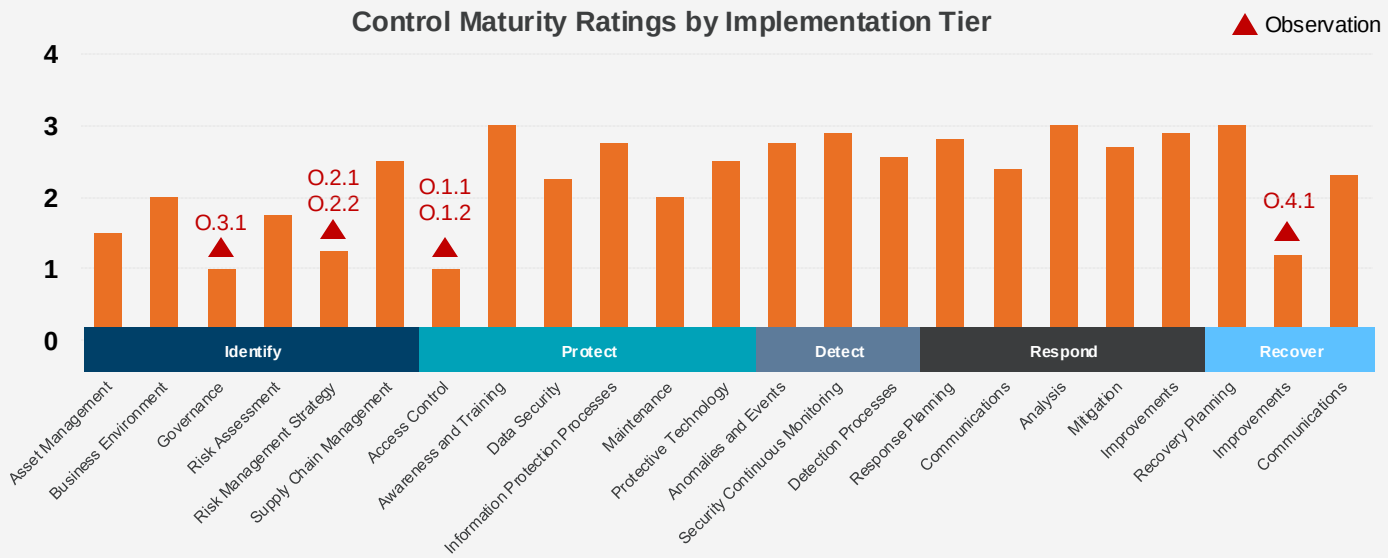
Privileged access management via legacy privileged access management tools has not extended to additional privileged or generic IDs, and is not widely

Observation 2.1

Efforts to improve integration of HR systems and identity management tools have not progressed in line with business requirements. The primary root cause of

Observation 2.2

Privileged access management via legacy privileged access management tools has not extended to additional privileged or generic IDs, and is not widely



Ostrich Cyber-Risk protiviti

Control & Risk Synergy

Control Assessment Objectives

Assess Control Maturity

Leverage a common framework (such as the NIST CSF or ISO 27000x) to assess the maturity of key cybersecurity controls across the environment.

Identify Gaps

Identify areas where control maturity can be improved and deliver detailed recommendations to address gaps between current and target state.

Develop Roadmap

Leverage understanding of environment gained during control assessment to plan future remediation actions aimed at addressing gaps.

Evaluate Against Peers

Benchmark control maturity relative to peers to understand where the organization sits relative to peers of a similar size or in the same industry.

Top Risks Prioritize Key Efforts

Top risks identified should **direct investments to those risks** where additional control maturity can further reduce risk.

- If Ransomware is a top risk, and maturity of PR.AT, PR.IR, PR.PS controls are low, this could show **higher rate of risk reduction return** than investing in DLP capabilities.

Risk Assessment Objectives

Understand Threat Landscape

Conduct threat intelligence to understand the attack vectors most likely to be attempted against organizational assets.

Identify Top Risks

Translate threat intelligence to discrete, actionable, and organization-specific risk events that are most likely to occur in the current-state environment.

Analyze Control Risk

Identify controls most likely to influence top risks, expressing the expected impact of control gaps against the organization's risk landscape.

Define Return on Investment

Prioritize control changes based on their expected, dollar-value impact on the organization's risk posture.

Control & Risk Synergy

Control Assessment Objectives

Assess Control Maturity

Leverage a common framework (such as the NIST CSF or ISO 27000x) to assess the maturity of key cybersecurity controls across the environment.

Identify Gaps

Identify areas where control maturity can be improved and deliver detailed recommendations to address gaps between current and target state.

Develop Roadmap

Leverage understanding of environment gained during control assessment to plan future remediation actions aimed at addressing gaps.

Evaluate Against Peers

Benchmark control maturity relative to peers to understand where the organization sits relative to peers of a similar size or in the same industry.

Establish Targets

Many organizations struggle with defining target NIST maturity scores. Quantifying benefits of a higher vs. lower score in each area can help.

Risk Assessment Objectives

Understand Threat Landscape

Conduct threat intelligence to understand the attack vectors most likely to be attempted against organizational assets.

Identify Top Risks

Translate threat intelligence to discrete, actionable, and organization-specific risk events that are most likely to occur in the current-state environment.

Analyze Control Risk

Identify controls most likely to influence top risks, expressing the expected impact of control gaps against the organization's risk landscape.

Define Return on Investment

Prioritize control changes based on their expected, dollar-value impact on the organization's risk posture.

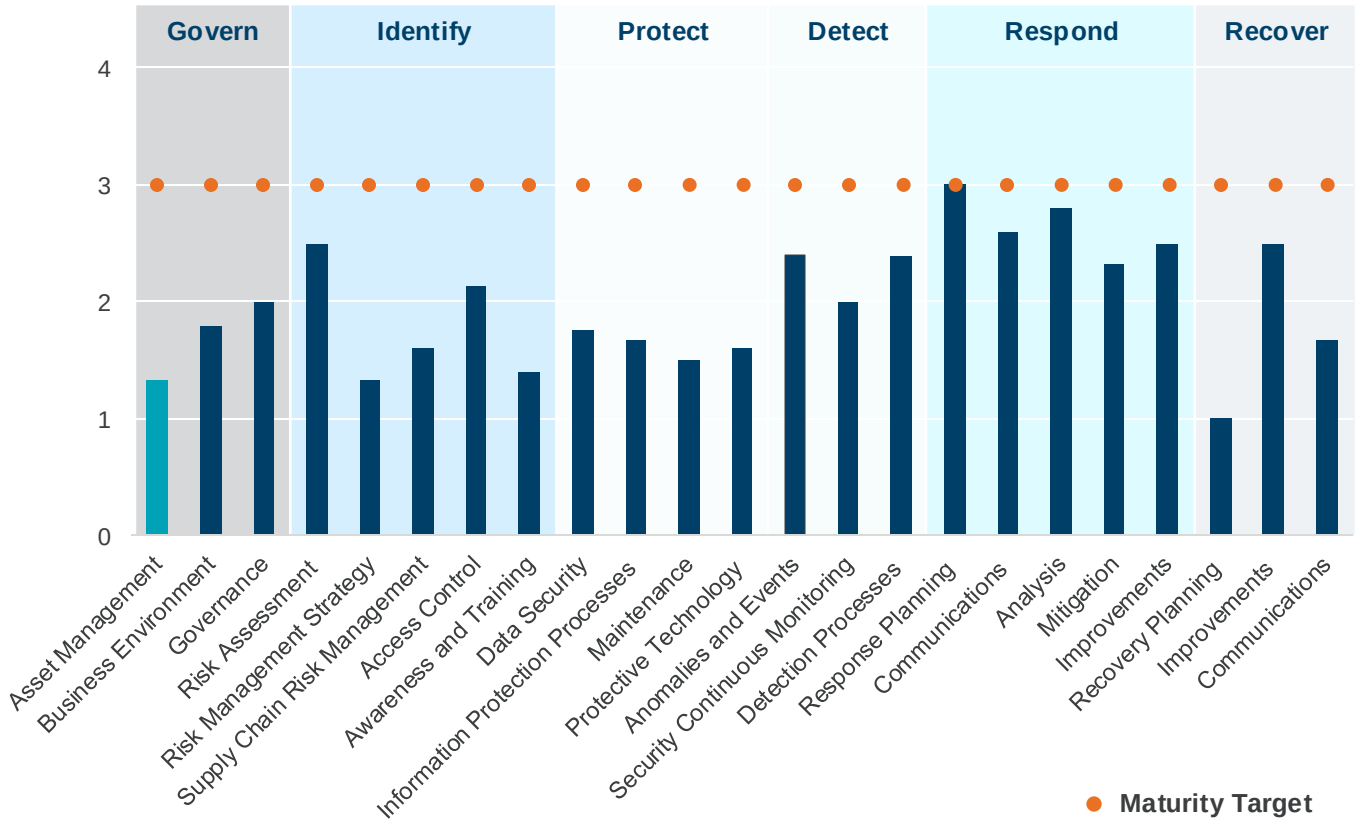
Translating CSF to FAIR

When using framework assessments like NIST CSF, organizations often aim to reach a defined target maturity. However, the importance of specific controls can vary based on the threats the organization faces. **By linking controls to specific risk scenarios, organizations can prioritize key initiatives and gain a clearer understanding of their overall risk landscape.**

Top Risks

Risk Scenario	Key Controls		
Phishing & Social Engineering	**PR.AT-2:** Privileged users understand their roles and responsibilities.	**PR.PT-3:** Email and web filters are implemented to detect and block malicious content.	**DE.CM-4:** Malicious code is detected.
Vulnerability Exploit	**PR.IP-12:** A vulnerability management plan is developed and implemented.	**DE.CM-8:** Vulnerabilities are identified and reported.	**ID.RA-3:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
Ransomware	**PR.DS-5:** Incidents are contained.	**RS.MI-1:** Incidents are contained.	**PR.IP-9:** Response and recovery plans are tested.

Controls Relative to Target



Ostrich Cyber-Risk protiviti

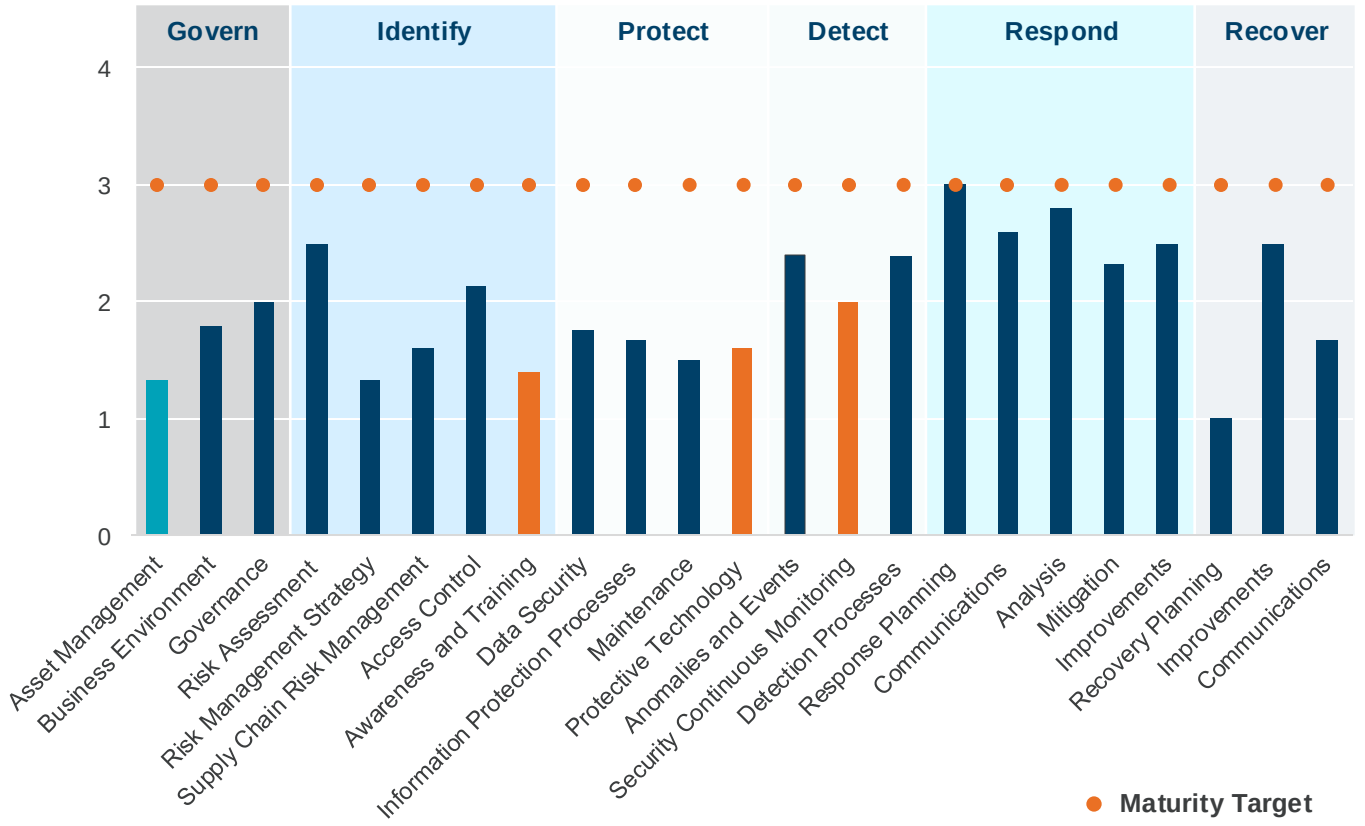
Translating CSF to FAIR

When using framework assessments like NIST CSF, organizations often aim to reach a defined target maturity. However, the importance of specific controls can vary based on the threats the organization faces. **By linking controls to specific risk scenarios, organizations can prioritize key initiatives and gain a clearer understanding of their overall risk landscape.**

Top Risks

Risk Scenario	Key Controls		
Phishing & Social Engineering	**PR.AT-2:** Privileged users understand their roles and responsibilities.	**PR.PT-3:** Email and web filters are implemented to detect and block malicious content.	**DE.CM-4:** Malicious code is detected.
Vulnerability Exploit	**PR.IP-12:** A vulnerability management plan is developed and implemented.	**DE.CM-8:** Vulnerabilities are identified and reported.	**ID.RA-3:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
Ransomware	**PR.DS-5:** Incidents are contained.	**RS.MI-1:** Incidents are contained.	**PR.IP-9:** Response and recovery plans are tested.

Controls Relative to Target



Ostrich Cyber-Risk protiviti

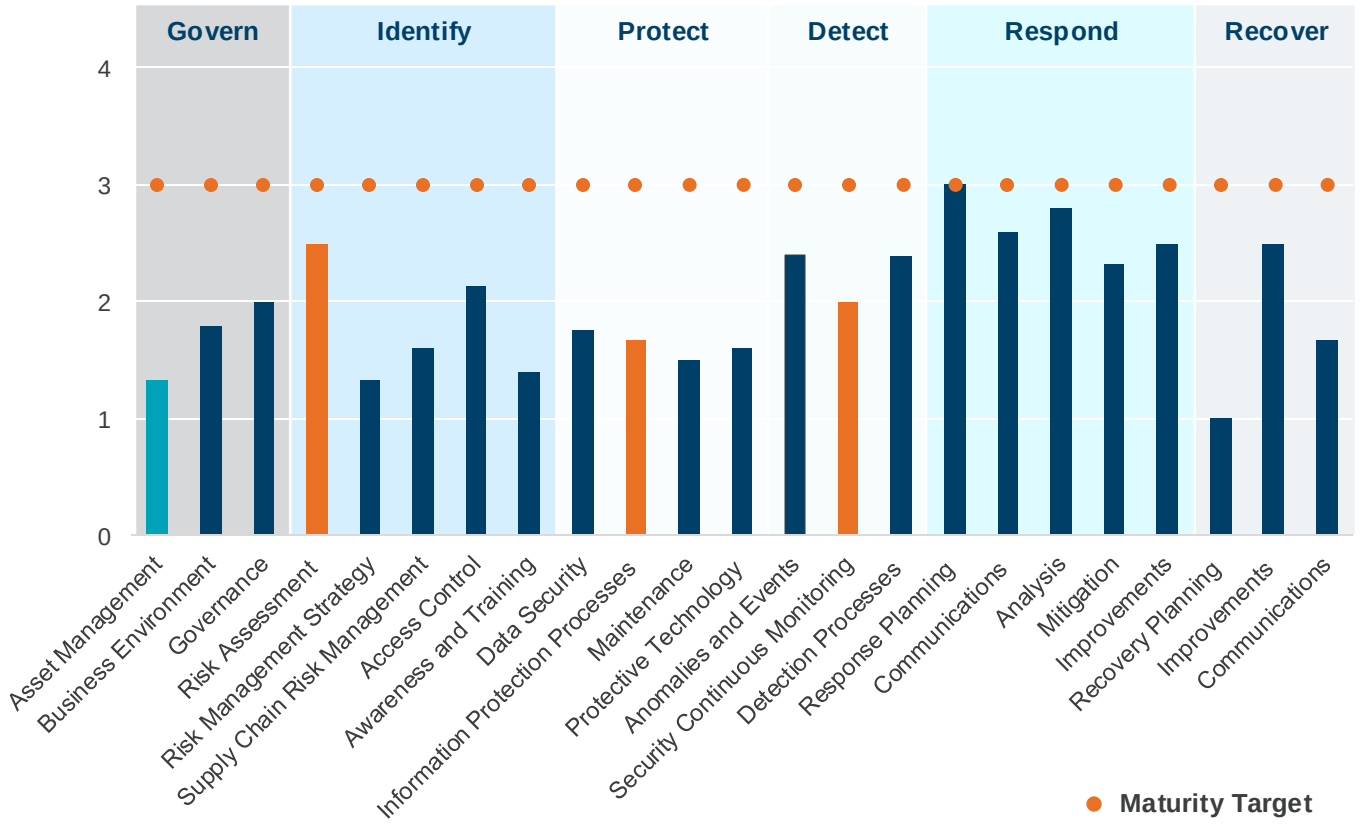
Translating CSF to FAIR

When using framework assessments like NIST CSF, organizations often aim to reach a defined target maturity. However, the importance of specific controls can vary based on the threats the organization faces. **By linking controls to specific risk scenarios, organizations can prioritize key initiatives and gain a clearer understanding of their overall risk landscape.**

Top Risks

Risk Scenario	Key Controls		
Phishing & Social Engineering	**PR.AT-2:** Privileged users understand their roles and responsibilities.	**PR.PT-3:** Email and web filters are implemented to detect and block malicious content.	**DE.CM-4:** Malicious code is detected.
Vulnerability Exploit	**PR.IP-12:** A vulnerability management plan is developed and implemented.	**DE.CM-8:** Vulnerabilities are identified and reported.	**ID.RA-3:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
Ransomware	**PR.DS-5:** Incidents are contained.	**RS.MI-1:** Incidents are contained.	**PR.IP-9:** Response and recovery plans are tested.

Controls Relative to Target



Ostrich Cyber-Risk protiviti

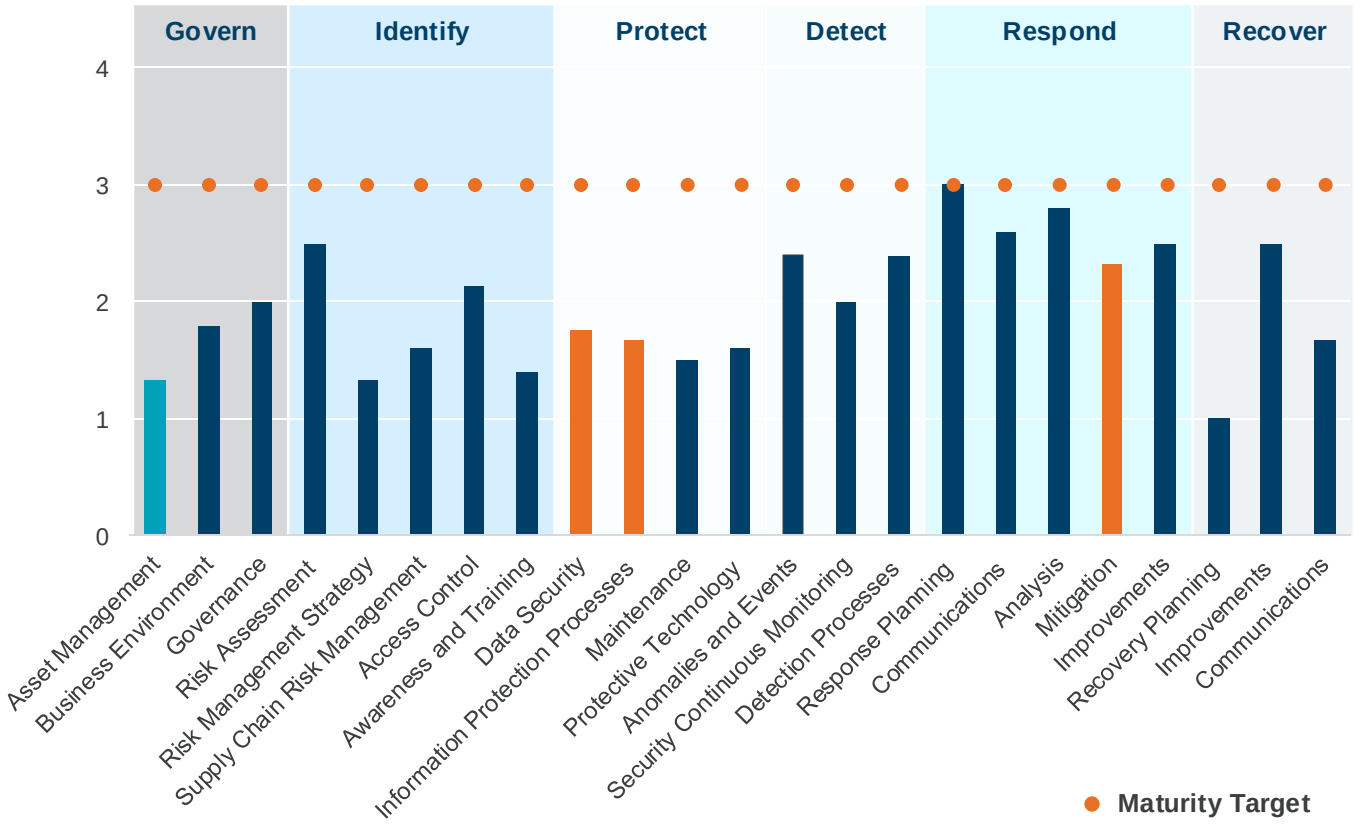
Translating CSF to FAIR

When using framework assessments like NIST CSF, organizations often aim to reach a defined target maturity. However, the importance of specific controls can vary based on the threats the organization faces. **By linking controls to specific risk scenarios, organizations can prioritize key initiatives and gain a clearer understanding of their overall risk landscape.**

Top Risks

Risk Scenario	Key Controls		
Phishing & Social Engineering	**PR.AT-2:** Privileged users understand their roles and responsibilities.	**PR.PT-3:** Email and web filters are implemented to detect and block malicious content.	**DE.CM-4:** Malicious code is detected.
Vulnerability Exploit	**PR.IP-12:** A vulnerability management plan is developed and implemented.	**DE.CM-8:** Vulnerabilities are identified and reported.	**ID.RA-3:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
Ransomware	**PR.DS-5:** Incidents are contained.	**RS.MI-1:** Incidents are contained.	**PR.IP-9:** Response and recovery plans are tested.

Controls Relative to Target



Ostrich Cyber-Risk protiviti

Current vs. Target Profiles

By weighting the relative impact of each control on the organization's top risks, a clearer and more comprehensive picture of potential risk reduction from maturity improvements can be quantitatively expressed.

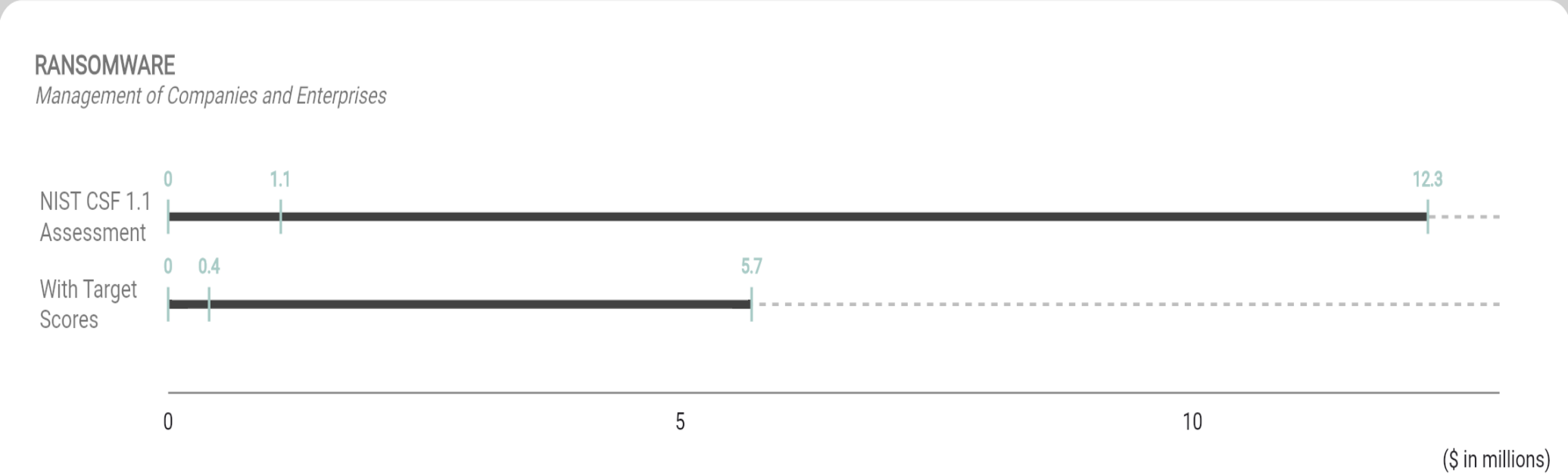
Top Risks

Risk Scenario	Key Controls			Risk-Weighted Current Rating	Risk-Weighted Target Rating	Maximum Potential Risk Reduction
Phishing & Social Engineering	**PR.AT-2:** Privileged users understand their roles and responsibilities.	**PR.PT-3:** Email and web filters are implemented to detect and block malicious content.	**DE.CM-4:** Malicious code is detected.	**1.83**	**2**	**$800K**
Vulnerability Exploit	**PR.IP-12:** A vulnerability management plan is developed and implemented.	**DE.CM-8:** Vulnerabilities are identified and reported.	**ID.RA-3:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	***1.93***	***2***	**$1.2M**
Ransomware	**PR.DS-5:** Incidents are contained.	**RS.MI-1:** Incidents are contained.	**PR.IP-9:** Response and recovery plans are tested.	***1.21***	***2***	**$5.5M**
					Aggregate Risk Reduction	**$7.5M**

Ostrich Cyber-Risk protiviti

Controls in FAIR

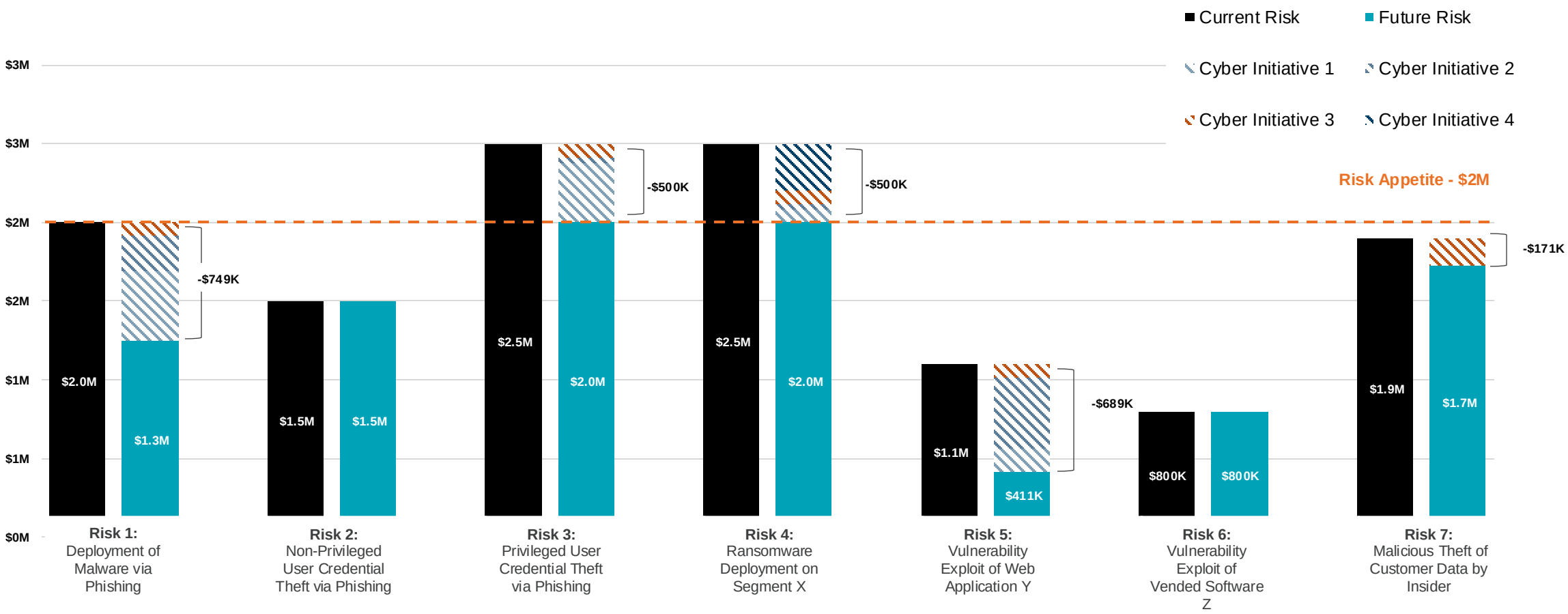
Using cyber risk quantification tools, you can automate the process of evaluating Current vs. Target state NIST CSF Profiles and the relative risk reduction of changes or investments in each control category.



Ostrich Cyber-Risk protiviti

Risk Landscape AND Recommendation Prioritization

Control changes and their expected maturity improvements can also be assigned to discrete initiatives, **enabling more detailed analysis of the expected return on investment from cybersecurity spending.**



Ostrich Cyber-Risk protiviti

Why Integrate FAIR + NIST CSF

Data Already Exists!

Many organizations are already doing a NIST CSF, NIST 800-53, ISO 27001, or other bottom-up controls based assessment. The data is there!

Bridging the Gap

What many organizations aren't doing is contextualizing the risk. You need top-down to do a more effective bottom-up, and vice versa.

Widespread Use

Both frameworks, but particular the NIST CSF, are known and understood by Board members. Regardless of opinion, NIST CSF maturity ratings are well-understood and resonate.

Prioritize

Your organization is going to get an audit and assessment report from someone, someday. This provides the framework to prioritize the outputs better.

Q&A

Our Speakers

Daniel Stone

Director,

Technology Risk & Resilience
Protiviti

Daniel.Stone@protiviti.com

Connect on LinkedIn

Jack Nelson

Senior Manager,

Technology Risk & Resilience
Protiviti

Jack.Nelson@protiviti.com

Connect on LinkedIn

Adam Lamantia

Director,

Enterprise Sales
Ostrich Cyber-Risk

Adam.lamantia@ostrichcyber-risk.com

Connect on LinkedIn

https://calendly.com/adam-lamantia

Ostrich Cyber-Risk protiviti