KOVRR

Cyber Decisions. Financially Quantified.

Quantifying Cybersecurity Control Impacts

www.kovrr.com

Introduction: The Value of Objective Security Control Mapping

Cybersecurity maturity models are critical tools for managing cyber risk, allowing chief information security officers (CISOs) to evaluate an organization's digital vulnerabilities systematically and build targeted, measurable strategies that reduce these shortcomings. Those models are typically applied to some security control framework to help determine where an organization is on its security journey. However, the diversity of available frameworks, such as ISO 27001/2, CIS, and NIST CSF, poses challenges for quantifying their impact consistently.

Without such standardization, comparing controls across the different cybersecurity frameworks is complex, leaving organizations to subjectively determine which risk reduction measures effectively reduce expenses to specific event types or attack vectors, for instance. Moreover, these gaps hinder model analysis and risk quantification efforts, as the variations in risk and threat definitions and scope obscure true cybersecurity control upgrade implications.

To address these issues, Kovrr developed a uniform approach to control for impact measurement, first aligning control definitions across control frameworks and then mapping the controls to the adversarial behavior that each control impacts, according to the MITRE ATT&CK framework. This approach provides a clear link between the application of a specific control at a company and the specific limitations of adversarial behaviors and techniques.

Combined with event-based modeling, CISOs and other cyber risk analysts can leverage this alignment and mapping to quantify the specific impact controls will have on their cyber security risk profile.

Consequently, organizations gain a consistent, quantifiable understanding of how well their security investments and initiatives mitigate real-world threats, making it easier for them to prioritize and justify upgrades, allocate resources, and build more resilient cybersecurity strategies based on clear, actionable insights.

Overview: Standardized Control Impacts

Obtaining an accurate understanding of which cybersecurity controls, products, and third-party service provider packages have the most significant impact on reducing cyber risk can be particularly challenging, even for mature enterprises. Consequently, Kovrr has recently established a data-driven process for evaluating the actual, real-world effect these implementations will have on an organization's risk exposure. Kovrr's Upgraded Security Control Modeling Process

Kovrr's Upgraded Security Control Modeling Process

- Enterprises use a variety of cybersecurity control frameworks such as ISO, CIS, and NIST CSF. Kovrr maps each control framework to a common controls catalog to gain a consistent view of control impact.
- Then, we map the control catalog to the known adversarial techniques that they prevent based on the MITRE ATT&CK framework. This process links the detailed safeguards and controls to behaviors we capture as part of Kovrr's event-based modeling.
- Finally, Kovrr adjusts the effectiveness that applying controls will have on each adversarial technique according to how effective the security controls will be at mitigating the behavior. This step includes adjustments for the occurrence of zero-day vulnerabilities, the scope and coverage of available software tools, and the potential for misconfiguration and error.

The outcome is a method for effectively applying individual security controls from different frameworks in a consistent and equivalent manner. For example, Multi-Factor-Authentication (MFA) implementation in the CIS cybersecurity framework should yield an equivalent impact to MFA implementation in the NIST CSF.

This uniform process also results in an objective way of measuring the impact of security controls across all known and unknown cyber attack techniques used by adversaries. However, it's important to note that these measurements do not reflect the specific cyber risk reduction for a real-world company whose exposure levels are dependent on a number of other factors.

Indeed, to calculate this security control implication for a particular company, it is essential to apply the control impacts on the company-specific exposure to the respective attack techniques by assessing the technique exposure and likely attack paths adversaries will take to exploit system vulnerabilities.

This evaluation is done by leveraging Kovrr's on-demand cyber risk quantification models, which capture an organization's unique exposure to cyber risk, event frequency, and potential event severity and subsequently apply the controls before running simulations. To learn more about the cyber risk quantification modeling methodology, explore Kovrr's knowledge base, Trust.

Standardization Methodology Deep Dive

Stage 1: Common Cybersecurity Control Assessment

There is a wide variety of cybersecurity frameworks available, and security teams will opt for the one most applicable to their organization's sector, experience, and governance requirements. Due to this variability, one of the most important outcomes Kovrr wants for its security control modeling approach is to ensure that applying the same respective controls across the different maturity models has the same consequences in terms of cyber risk reduction.

To demonstrate the process Kovrr has implemented to achieve this consistency, we will use the CIS v8.0, ISO 27001/2, and NIST CSF v2.0 frameworks, which are most commonly used across large corporations throughout Europe and the United States.

Each of the cybersecurity frameworks (CIS, ISO, NIST CSF) is first mapped to a common cybersecurity control catalog. In this case, Kovrr uses NIST 800-53, a comprehensive catalog of security controls originally designed for government use but is increasingly being leveraged by enterprises as the common base.

Control definitions within each maturity model are provided as descriptions and, therefore, need interpretation to make sense. Instead of relying on internal assumptions or unstandardized expert insights, Kovrr instead harnesses guidance from NIST IR 8477, Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings.

This document outlines the application of 'Set Theory Relationship Mapping (STRM),' which can be used to determine the intersection between different control descriptions[1]. It is then used to determine the level of coverage between a cybersecurity maturity model (such as CIS or ISO) and the target catalog (NIST 800-53).

Ultimately, Kovrr's output is a mapping document that relates each distinct framework to the NIST 800-53 catalog of controls.

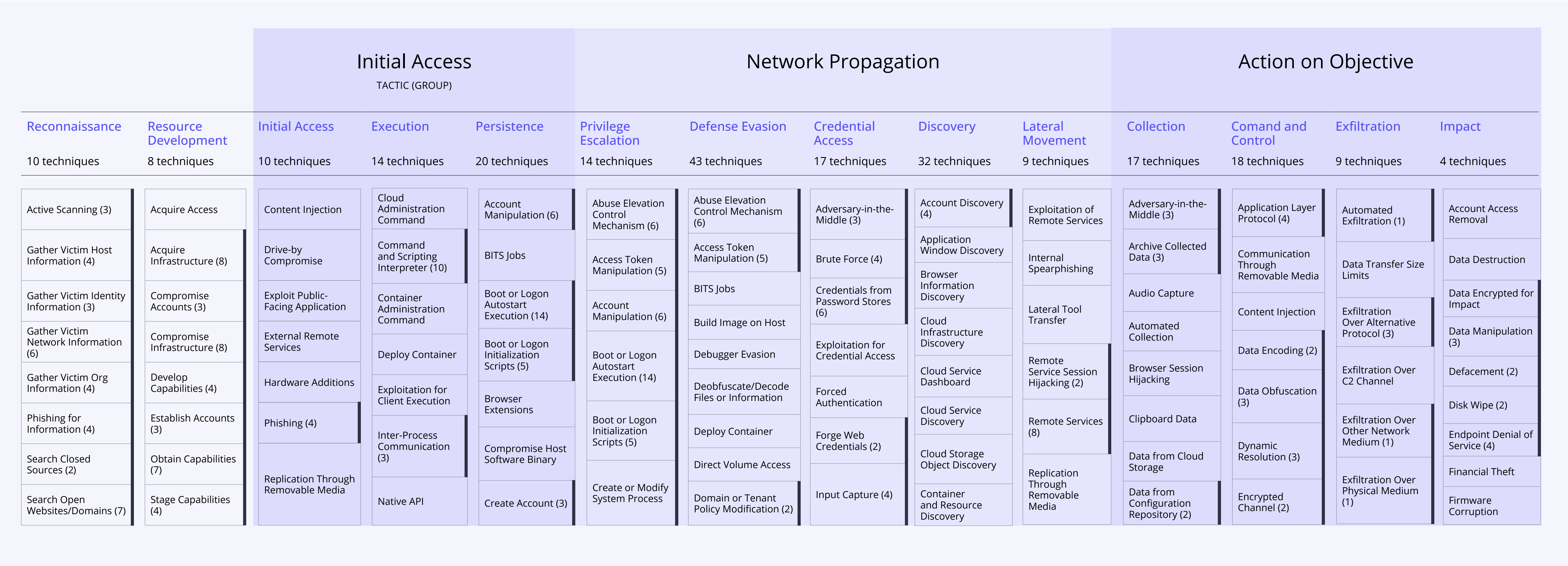
- Weighted by the intersection of the control (based on STRM)
- Weighted by Kovrr's relative view of the importance of each of the NIST 800-53 controls.

This documentation ensures consistency between the different control maturity models by using the relationship to a common catalog of controls.

Stage 2: Cybersecurity Control Impact

After ensuring consistency between respective controls in the various cybersecurity frameworks, the next phase in the standardization process is to relate said controls to the types of attack techniques they are designed to prevent. The technique catalog Kovrr employs is the MITRE ATT&CK framework, which outlines and groups known attack techniques into adversarial tactic groups.

[1] In particular, Kovrr leveraged the application of this document computed by the Secure Controls Framework: "Secure Controls Framework (SCF) - 2024.3.xlsx" by Secure Controls Framework Council, LLC is licensed under CC BY-ND 4.0.



		Initial Access TACTIC (GROUP)			Network Propagation					Action on Objective			
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Comand and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	4 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)		Deploy Container	Input Capture (4)	Cloud Storage Object Discovery		Data from Cloud Storage	Encrypted Channel (2)		Endpoint Denial of Service (4)
Search Open Websites/Domains (7)	Stage Capabilities (4)					Direct Volume Access		Container and Resource Discovery		Data from Configuration Repository (2)			Financial Theft
						Domain or Tenant Policy Modification (2)							Firmware Corruption

Figure 1: Known Attack Techniques, MITRE ATT&CK Framework

Kovrr groups these techniques further into three phases of attack:

- **Initial Access:** This group is focused on the attacker's ability to breach the perimeter and establish a persistent presence within the target's digital environment.
- **Network Propagation:** This group is focused on the attacker's ability to traverse the target's network to uncover valuable assets, such as data and critical business systems, and includes techniques under discovery, lateral movement, defense evasion, and privilege escalation.
- **Action on Objective:** This group is focused on the execution of a harmful act on company systems, such as data exfiltration, disruption of critical systems, and system damage.

The MITRE ATT&CK framework also includes a Reconnaissance phase, but Kovrr strictly focuses on the three main 'active' phases. For the mapping between the control catalog and specific techniques, NIST provides a mapping between the controls catalog (800-53) and the attack techniques. We, therefore, can easily map the controls against the techniques they are designed to prevent.[2]

Subsequently, we can also now look at the coverage of different control schemes relative to each other. Figure 1 shows the relative coverage by attack phase of CIS, NIST CSF, and ISO 27001/2.

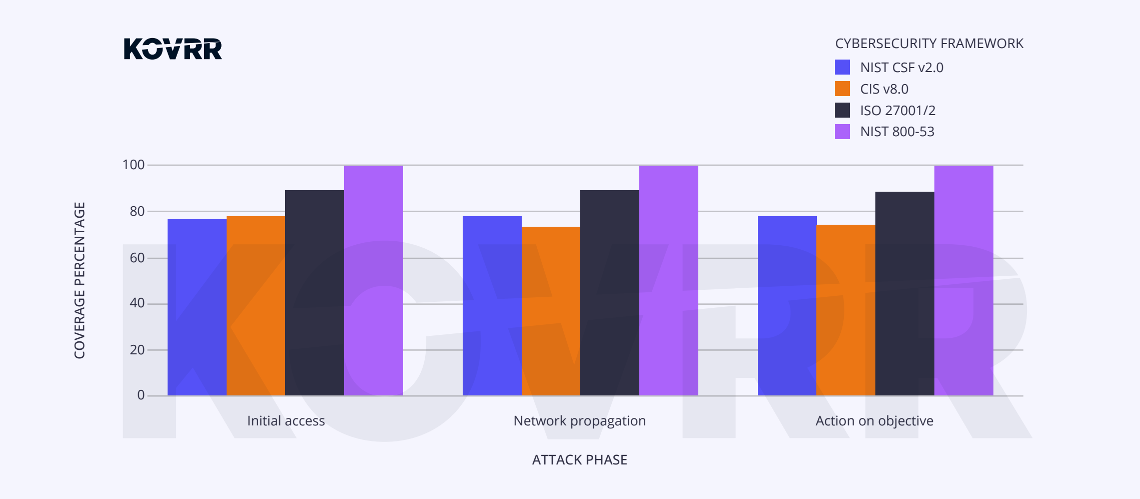


Figure 2: Relative Control Coverage by Attack Phase

After NIST 800-53 as the baseline (100% coverage), the next most complete framework is ISO 27001/2 (88-90% coverage across each attack phase), with NIST CSF and CIS having strengths in propagation, damage, and frequency, respectively.[3]

[2] Not all techniques are covered by the control in the NIST 800-53 catalog, which we acknowledge in the control coverage mapping (see Stage 3).

[3] Most organziations use standard names interchangibly even though those with deep compliance knowledge will understand that NIST CSF references 800-53 for control language and the controls in ISO 27001 are actually spelled out in 27002.

Stage 3: Real-World Cybersecurity Control Effects

With this base mapping, there is now a detailed coverage of the framework controls that impact each of the adversarial techniques within each tactic, impacting each attack phase. However, because it is also the case that controls are not fully effective when applied to real-world usage, the potential impact needs to be reduced for the following effects:

- **Non-Covered Techniques:** These are the attack techniques not covered by the currently documented NIST 800-53 controls (i.e., the known gaps captured at the tactic and attack phase levels). These are also gaps identified by the mapping of Kovrr's common control catalog against the known attack techniques.
- **Undocumented Techniques:** This is the margin accounting for the risk of new techniques or technique implementations still emerging that are not documented or controlled for (i.e., unknown gaps, zero-day vulnerabilities). Calibrating this parameter is done by evaluating the occurrence of zero-day exploits against each tactic.
- **Tool Design:** This effect accounts for the weaknesses in control designs (i.e., the practical consideration that cybersecurity tools do not cover all edge cases). For these gaps, Kovrr calibrates a margin for the ability of software and hardware to be effective at reducing a technique's success rate.
- **Implementation:** This is the allowance for tool misconfigurations, log monitoring, and human errors. The technique margin is based on the complexity of the specific control or technique.

In Kovrr's assessment of these factors, the tendency is to adopt conservative assumptions as we do not want to overstate the impact of controls on the reduction of risk.

Actionable Control Outcomes

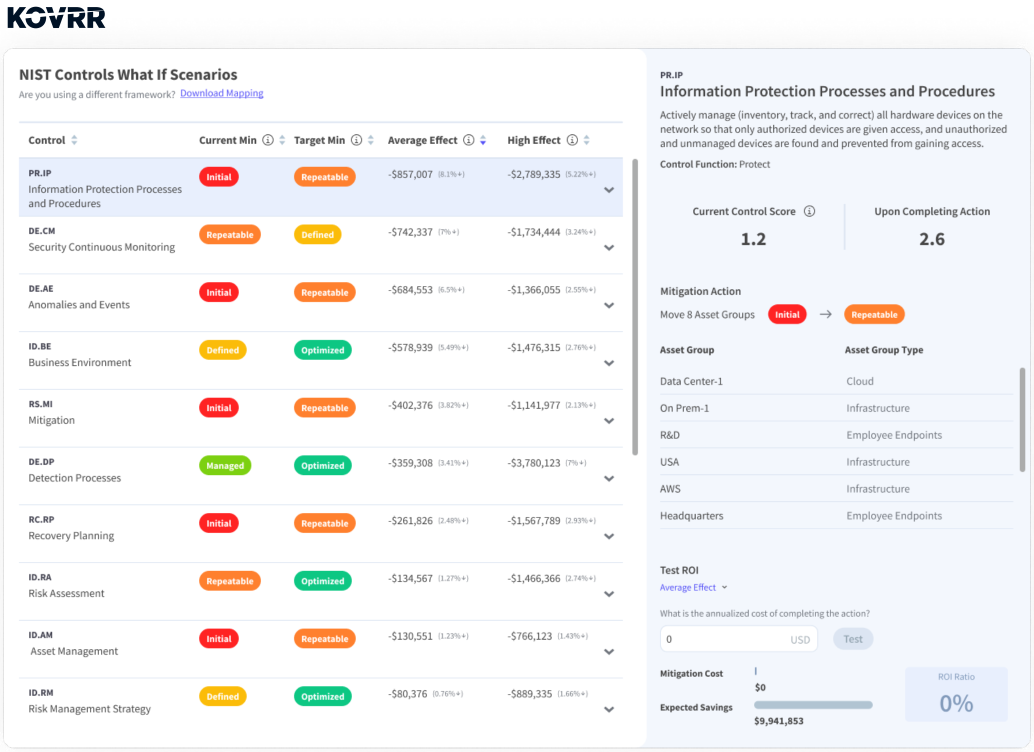
Attack techniques must be adjusted according to the organization's actual exposure to make Kovrr's standardized control mapping applicable and actionable. This adjustment process involves weighting techniques on:

1. Whether they exist or not within the company infrastructure
2. The likelihood and frequency of adversarial techniques o adjust for the volume and type of attacks.
3. Company exposure to potential damage, especially by quantifying the level of risk presented by data exposure (i.e., PII, PCI, PHI, intellectual property).

We do this by applying the organization's cybersecurity maturity model controls to Kovrr's cyber risk modeling approach.

Building a Unified Approach to Cybersecurity Risk Management

Kovrr's novel and standardized approach to mapping cybersecurity controls represents a pivotal advancement in cyber risk quantification and risk modeling. Aligning the controls from a diverse set of cybersecurity maturity models, such as ISO 27001/2, CIS, and NIST CSF, with the NIST 800-53 catalog and then mapping them to the MITRE ATT&CK framework, this methodology addresses longstanding inconsistencies in evaluating the effectiveness of security measures and enables organizations to understand the impact of their security upgrades more accurately.



NIST Controls What If Scenarios

Are you using a different framework? Download Mapping

Control	Current Min	Target Min	Average Effect	High Effect
PR.IP Information Protection Processes and Procedures	Initial	Repeatable	-$857,007 (8.1%↓)	-$2,789,335 (5.22%↓)
DE.CM Security Continuous Monitoring	Repeatable	Defined	-$742,337 (7%↓)	-$1,734,444 (3.24%↓)
DE.AE Anomalies and Events	Initial	Repeatable	-$684,553 (6.5%↓)	-$1,366,055 (2.55%↓)
ID.BE Business Environment	Defined	Optimized	-$578,939 (5.49%↓)	-$1,476,315 (2.76%↓)
RS.MI Mitigation	Initial	Repeatable	-$402,376 (3.82%↓)	-$1,141,977 (2.13%↓)
DE.DP Detection Processes	Managed	Optimized	-$359,308 (3.41%↓)	-$3,780,123 (7%↓)
RC.RP Recovery Planning	Initial	Repeatable	-$261,826 (2.48%↓)	-$1,567,789 (2.93%↓)
ID.RA Risk Assessment	Repeatable	Optimized	-$134,567 (1.27%↓)	-$1,466,366 (2.74%↓)
ID.AM Asset Management	Initial	Repeatable	-$130,551 (1.23%↓)	-$766,123 (1.43%↓)
ID.RM Risk Management Strategy	Defined	Optimized	-$80,376 (0.76%↓)	-$889,335 (1.66%↓)

PR.IP

Information Protection Processes and Procedures

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Control Function: Protect

Current Control Score	Upon Completing Action
1.2	2.6

Mitigation Action

Move 8 Asset Groups Initial → Repeatable

Asset Group	Asset Group Type
Data Center-1	Cloud
On Prem-1	Infrastructure
R&D	Employee Endpoints
USA	Infrastructure
AWS	Infrastructure
Headquarters	Employee Endpoints

Test ROI

Average Effect

What is the annualized cost of completing the action?

0 USD

Mitigation Cost $0

Expected Savings $9,941,853

ROI Ratio 0%

Figure 3: Kovrr's Data-Driven Security Control Recommendation Insights

This refined approach shifts the focus away from subjective assumptions to objective data-driven insights and offers a more targeted understanding of how specific controls reduce particular risks associated with various attack techniques and phases. Moreover, to further bolster outcome accuracy, Kovrr integrates real-world variables, including implementation challenges and emerging vulnerabilities, to ensure that outcomes remain relevant and actionable.

Leveraging this innovative mapping methodology, organizations can now objectively measure how well their controls mitigate their overall exposure to cyber threats, a capability previously hindered by fragmented frameworks and uneven definitions. Regardless of the cybersecurity framework they harness for cyber risk management purposes, CISOs and cybersecurity leaders will now be better positioned to prioritize critical upgrades and justify investments based on real-world impact.

AUTHORED BY:

Peter Dyson

Head of Analytics, Kovrr

KOVRR
Cyber Decisions. Financially Quantified.