SOLUTION BRIEF
Cybersecurity Framework
Risk Management

The Cybersecurity Framework in Action: An Intel Use Case

Intel Publishes a Cybersecurity Framework Use Case

Advancing cybersecurity across the global digital infrastructure has long been a priority for Intel. President Obama issued Executive Order 13636—Improving Critical Infrastructure Cybersecurity—in February 2013, and over the ensuing year Intel collaborated with government and industry to develop the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"). The first version of the Framework was delivered on February 12, 2014, and soon thereafter Intel launched a pilot project to test the Framework's use at Intel.

The Framework Provides Clear Benefit

Intel's pilot project assessed cybersecurity risk for our Office and Enterprise infrastructure. We focused on developing a use case that would create a common language and encourage the use of the Framework as a process and risk management tool, rather than a set of static compliance requirements.

Our early experience with the Framework has helped us harmonize our risk management technologies and language, improve our visibility into Intel's risk landscape, inform risk tolerance discussions across our company, and enhance our ability to set security priorities, develop budgets, and deploy security solutions. The pilot resulted in a set of reusable tools and best practices for utilizing the Framework to assess infrastructure risk; we plan to use these tools and best practices to expand Intel's use of the Framework. We hope other organizations will also embrace the Framework, utilizing it for the benefit of their own security systems and sharing their results with industry and government partners.

Next Steps for the Framework at Intel and Beyond

The Framework embodies a longstanding pillar of Intel's cybersecurity strategy: supporting collaboration between government, industry, and non-governmental organization stakeholders to improve cybersecurity in a way that promotes innovation, protects citizens' privacy and civil liberties, and preserves the promise of the Internet as a driver of global economic development and social interaction.

As the Framework continues to evolve and mature, we believe it should include key elements such as the cyberthreat intelligence lifecycle, which is essential to developing a robust understanding of cybersecurity attacks. Intel's pilot project has verified that the Framework can provide value to even the largest organizations and has the potential to transform cybersecurity on a global scale by accelerating cybersecurity best practices across the compute continuum.

By focusing on risk management instead of compliance, the Cybersecurity Framework has the potential to transform cybersecurity on a global scale.

Introduction

Security has long been an Intel priority. Security along with power-efficient performance and connectivity comprise the three computing pillars around which Intel concentrates its innovation efforts. In early 2014, Intel formed the Intel Security Group, a new business unit to further the security pillar. This business unit combines our subsidiary McAfee with all other security resources within Intel, forming a single organization focused on accelerating ubiquitous protection against security risks for people, businesses, and governments worldwide.

Intel has long shared the sentiment with the U.S. and global governments that we cannot delay in collectively addressing the evolving cybersecurity threats that face us all, and Intel and Intel Security will continue to lead efforts to improve cybersecurity across the compute continuum. One way we have demonstrated such leadership is by investing billions of dollars over the last decade to develop software, hardware, services, and integrated solutions to advance cybersecurity across the global digital infrastructure. We also work collaboratively with government, industry, and non-governmental organization stakeholders to improve cybersecurity in a way that promotes innovation, protects citizens' privacy and civil liberties, and preserves the promise of the Internet as a driver of global economic development and social interaction.

Our support for the Cybersecurity Framework (hereafter referred to as the Framework), created as part of U.S. Executive Order 13636, is grounded not only in our prioritization of security but also on thought and operational leadership. The Framework was developed through a process of coordination and collaboration between private industry and public enabling organizations. Through frequent dialogue and collaboration with the National Institute of Standards and Technology (NIST) during the implementation phase, we have devised and implemented an internal risk and management use case for the Framework. We conducted a pilot project to develop this use case.

The Pilot in Context

We are at the preliminary stages of understanding the Framework. As the development of the Framework was nearing its completion, former NIST Director Pat Gallagher said we were "at the end of the beginning." Dr. Gallagher's words hold true today, less than a year since Framework 1.0 was released. Nonetheless, as an organization currently using the Framework, we will continue to evolve and use the Framework on an ongoing basis.

By implementing the Framework, we anticipate that Intel will achieve the following benefits:

- Harmonization of risk management methodologies, technologies, and language across the enterprise
- Improved visibility into Intel's risk landscape, helping identify both strengths and opportunities to improve
- Better-informed risk tolerance discussions
- Ability to better set security priorities, develop capital and operational expenditure budgets, and identify potential security solutions and practices

Throughout the development process, Intel actively supported the emergence of the Framework from its initial public comment phase by participating in the Framework development workshops and by providing comments to the draft documents that NIST published. Intel believes that the strength of the Framework lies in its accessibility and flexibility; we are committed to proactively developing a Framework use case to both demonstrate industry leadership and provide key learnings to drive the evolution of the Framework. We believe the Framework's evolution is and will continue to be an industry-led effort as we move forward.

Utilizing the Cybersecurity Framework at Intel

From the early days of development, the Intel team responsible for engaging with the Framework planned to conduct a pilot project to test its use at Intel. Once the 1.0 version of the Framework was released and we knew the final configuration, we looked for a business unit to partner with for the pilot. Because we were in new territory, we sought a mature business unit with a robust cybersecurity program and with a large range of products and services we could use to test some of the Framework's limits. Intel IT met all these requirements, making it the obvious choice.

Intel IT is much more than a service organization. As an integral part of the Intel business, it delivers value by offering solutions to other business units that drive other products. Intel IT's cybersecurity program has a large number of cybersecurity experts, all of whom could easily provide independent assessment and evaluation under the Framework with minimal training. Intel IT also uses a mature model of cyber functions within the enterprise (the *DOMES* model detailed in the Design section) that enabled us to further simplify the pilot.

We have recently completed the pilot project, which clearly demonstrated the value of the Framework. We plan to apply what we learned during the pilot to expanding Intel's use of the Framework. Most importantly, we verified that by focusing on risk management rather than compliance, the Framework has the potential to transform cybersecurity on a global scale and accelerate cybersecurity across the compute continuum.

Methodology

Intel uses different risk management tools in different situations, depending on the environment being managed and the type and scope of the risks. We consider the Framework to be a top-level security management tool that helps assess cybersecurity risk across the enterprise. Intel's approach was to conduct the pilot using the Framework to create an enterprise-level risk heat map that could be used to do the following:

- Set risk tolerance baselines
- Identify areas that need more detailed or technical assessments
- Identify areas of overinvestment and underinvestment
- Assist in risk prioritization

Design

For assessment purposes, Intel divides its compute infrastructure into five critical business functions: *Design, Office, Manufacturing, Enterprise*, and *Services (DOMES).* For the pilot project, we used the Framework to perform an initial high-level risk assessment on only the *Office* and *Enterprise* environments, rather than attempt to apply the Framework across the entire computing domain. Because *Office* and *Enterprise* are similar environments from a risk management perspective, the subject matter experts (SMEs) involved in the Framework risk assessment pilot were essentially the same people. Also, the *Office* and *Enterprise* environments most closely match the existing Framework Categories (see the Cybersecurity Framework Terminology sidebar), while we believe the other business functions,

Cybersecurity Framework Terminology

Core. A set of cybersecurity activities and references that is common across critical infrastructure sectors and organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.

Functions. One of the main components of the Framework, Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five Functions are Identify, Protect, Detect, Respond, and Recover.

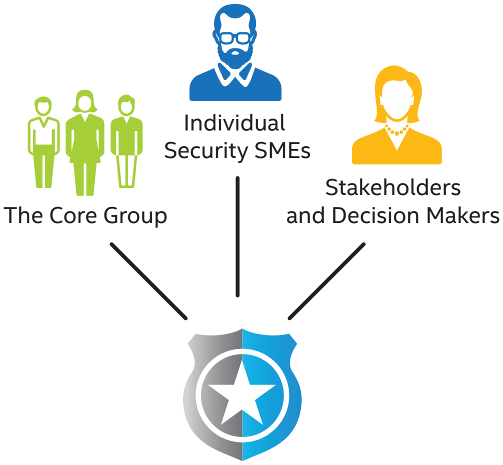
Categories. The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include Asset Management, Access Control, and Detection Processes.

Subcategories. The subdivision of a Category into specific outcomes of technical and management activities. Examples of Subcategories include External information systems are cataloged, Data-at-rest is protected, and Notifications from detection systems are investigated.

Tiers. The Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs and integrated into an organization's overall risk management practices.

Profiles. A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a current profile (the "as is" state) with a target profile (the "to be" state).

For a more comprehensive glossary of terms, refer to the Cybersecurity Framework document. www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf



Pilot Project Participants

such as *Manufacturing* and *Design*, may require more customization of the Framework Categories.

The pilot project involved three main groups of people:

- The Core Group, comprising 8 to 10 senior security SMEs and mid-to-senior-level security capability or program managers, who set target scores, validated Categories, developed Subcategories, and performed an initial risk assessment and scoring.
- Individual security SMEs, who scored the risk areas.
- Stakeholders and decision makers, who approved target scores, reviewed assessment results, and set risk tolerance levels.

The activities of these groups are described in more detail in the Implementing the Pilot Project section.

Goals

We established the following goals for the pilot Framework project, which sought to assess cybersecurity risk for the Office and Enterprise infrastructure:

- Establish organizational alignment on risk tolerance objectives.
- Inform the budget planning and prioritization processes.
- Communicate an aligned cybersecurity risk picture to senior leadership.
- Create a set of reusable tools and best practices for utilizing the Framework to assess infrastructure risk.

Early in the planning, we believed the Framework could transform a discussion about risk tolerance objectives from implicit to explicit. Today it is not unusual for an organization to have a disconnect between the C-level and the technical implementation staff level concerning risk tolerance, and often the organization is unaware of this problem. With a definitive, universal understanding of what an organization's governance considers an acceptable level of risk, the organization can now compare current and target scores to determine where improvements may be made.

Implementing the Pilot Project

During the implementation of the pilot project, we did not treat the Framework as a recipe book, but rather as the framework that it is. As such, we felt empowered to tailor it to meet our business needs. We believe that organizations implementing the Framework should also consider tailoring it to fit their individual business processes and priorities, to maximize the benefits they can gain.

We customized the Framework in the following areas:

- **Tier definitions.** We augmented the generic Tier definitions listed in the Framework to provide more concrete guidance to our assessors, as applicable to our particular environment.

  We started with the traditional security triad of People, Processes, and Technology, and mapped the Framework definitions into that structure. We then added a new element, Ecosystem, which we believe is equally essential to a modern corporate security program. Important organizational and governance issues, not included in the core model, are now included in this new element.

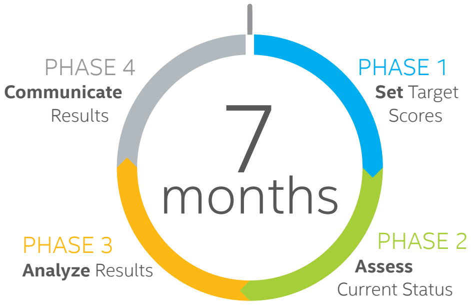
  Our modifications remained aligned to the Framework Tiers' graduated maturity scale and intent. Table 1 lists our customized Tier definitions.

Table 1. Customized Tier Definitions

FOCUS	TIER 1	TIER 2	TIER 3	TIER 4
AREA	PARTIAL	RISK INFORMED	REPEATABLE	ADAPTIVE
People	• Cybersecurity professionals (staff) and the general employee population have had little to no cybersecurity-related training. • The staff has a limited or nonexistent training pipeline. • Security awareness is limited. • Employees have little or no awareness of company security resources and escalation paths.	• The staff and employees have received cybersecurity-related training. • The staff has a training pipeline. • There is an awareness of cybersecurity risk at the organizational level. • Employees have a general awareness of security and company security resources and escalation paths.	• The staff possesses the knowledge and skills to perform their appointed roles and responsibilities. • Employees should receive regular cybersecurity-related training and briefings. • The staff has a robust training pipeline, including internal and external security conferences or training opportunities. • Organization and business units have a security champion or dedicated security staff.	• The staff's knowledge and skills are regularly reviewed for currency and applicability and new skills, and knowledge needs are identified and addressed. • Employees receive regular cybersecurity-related training and briefings on relevant and emerging security topics. • The staff has a robust training pipeline and routinely attend internal and external security conferences or training opportunities.
Process	• A risk management process has not been formalized; risks are managed in a reactive, ad hoc manner. • Business decisions and prioritization are not factored into risk and threat assessments. • Risk and threat information is not communicated to internal stakeholders.	• Prioritization of cybersecurity activities is informed by organizational risk objectives, the threat environment, or mission requirements. • Risk-informed, management-approved processes and procedures are defined and implemented, and the staff has adequate resources to perform its cybersecurity duties. • Cybersecurity information is shared within the organization on an informal basis. • Management has approved the risk management practices, but these practices may not have been established as organizational-wide policy.	• Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business or mission requirements and a changing threat and technology landscape. • Consistent risk management practices are formally approved and expressed as policy, and there is an organization-wide approach to manage cybersecurity risk. • Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.	• Cybersecurity risk management is an integral part of the organizational culture. • The organization actively adapts to a changing cybersecurity landscape, evolving and sophisticated threats, predictive indicators, and lessons learned from previous events in a timely manner. • The organization continually incorporates advanced cybersecurity technologies and practices. • There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures.
Technology	• Tools to help manage cybersecurity risk are not deployed, not supported, or insufficient to address risks. • Tools may be in place but are not adequately tuned or maintained. • Technology deployed lags current threats. • Tool deployment may not adequately cover risk areas.	• Tools are deployed and supported to address identified risks. • The tools in deployment are tuned and maintained when resources are available. • The technology deployed, for the most part, keeps pace with current threats. • Tool coverage of the risk area is complete when deployed.	• Metrics are used to evaluate the usefulness and effectiveness of the deployed tools. • The tools in deployment are routinely tuned and maintained. • The technology deployed keeps pace with current and emerging threats. • Tool coverage of the risk area is complete and updated as changes are recognized.	• The tools deployed in the environment are regularly reviewed for effectiveness and coverage against changes in the threat environment and internal ecosystem. • The tools and technology deployed anticipate emerging threats.
Ecosystem	• The organization does not understand its role in the larger ecosystem or act accordingly. • The organization does not have processes in place to participate in or collaborate with external organizations on cybersecurity issues.	• The organization knows its role in the larger ecosystem but has not formalized its capabilities to interact and share information externally. • The organization may participate in or collaborate with external organizations on cybersecurity issues on an ad hoc basis.	• The organization understands its ecosystem dependencies and partners and can act accordingly when it receives information from these partners.	• The organization manages risk and actively shares information with partners to ensure that accurate, current information improves ecosystem cybersecurity before events occur.

- **Categories.** In the Detect Function, we added a fourth Category, Threat Intelligence, because it is an important part of Intel's security processes. We expect additional Categories to emerge as we apply the Framework to Intel's *Design, Manufacturing*, and *Services* environments.
- **Subcategories.** After much consideration, we decided not to use most of the Subcategories as defined by the Framework. While the supplied Subcategories are appropriate for most environments, we created our own Subcategories to better reflect how Intel manages each Category. For example, in Asset Management we created the Subcategories of Information, Client, Server, Network, People, and Virtual, which align with the scheme Intel IT Security uses to manage assets. In addition, we found Subcategories were necessary to our assessment pilot only if that level of granularity helped inform a business decision. For example, if the Asset Management Category received a low score, the Subcategories could help identify the specific aspects needing improvement.

Pilot Project Phases



Project Phases

Our pilot project consisted of four phases: set target scores, assess our current status, analyze the results of that assessment, and communicate those results to managers and senior leadership. An organized, phased approach enabled us to successfully implement the Framework in our *Office* and *Enterprise* environments.

We completed the project in about seven months.

Phase 1 – Set Target Scores

The Core Group held a one-day, face-to-face session and a half-day virtual session during which the following actions took place:

- Agreed on methodology and maturity descriptions
- Validated Functions and Categories and defined new Subcategories aligned to Intel's capabilities, programs, and processes
- Assigned target scores by Function and Category
- Assessed current status and scored Functions and Categories

As a result of this initial phase we were able to validate that our approach aligned with Intel's existing risk management methodologies and could be a meaningful tool for prioritization and risk tolerance decisions. Our chief information security officer (CISO) and other key stakeholders also validated our target scores, further raising our confidence that we had set them accurately.

Phase 2 – Assess Current Status

We identified senior SME scorers to conduct an independent risk assessment based on the Framework. Using learnings from our Core Group sessions, we developed individual scoring tools and provided training through virtual one-hour sessions (see Training Topics for more information). Once trained, the SMEs individually scored the Categories and noted specific Subcategories where opportunities to improve existed.

By design, participants were not aware of the target scores that the Core Group set. The total time that each SME used for the assessment was 2 to 3 hours, which included training, using the self-scoring tool, and participating in a validation of the aggregated scores.

Phase 3 – Analyze Results

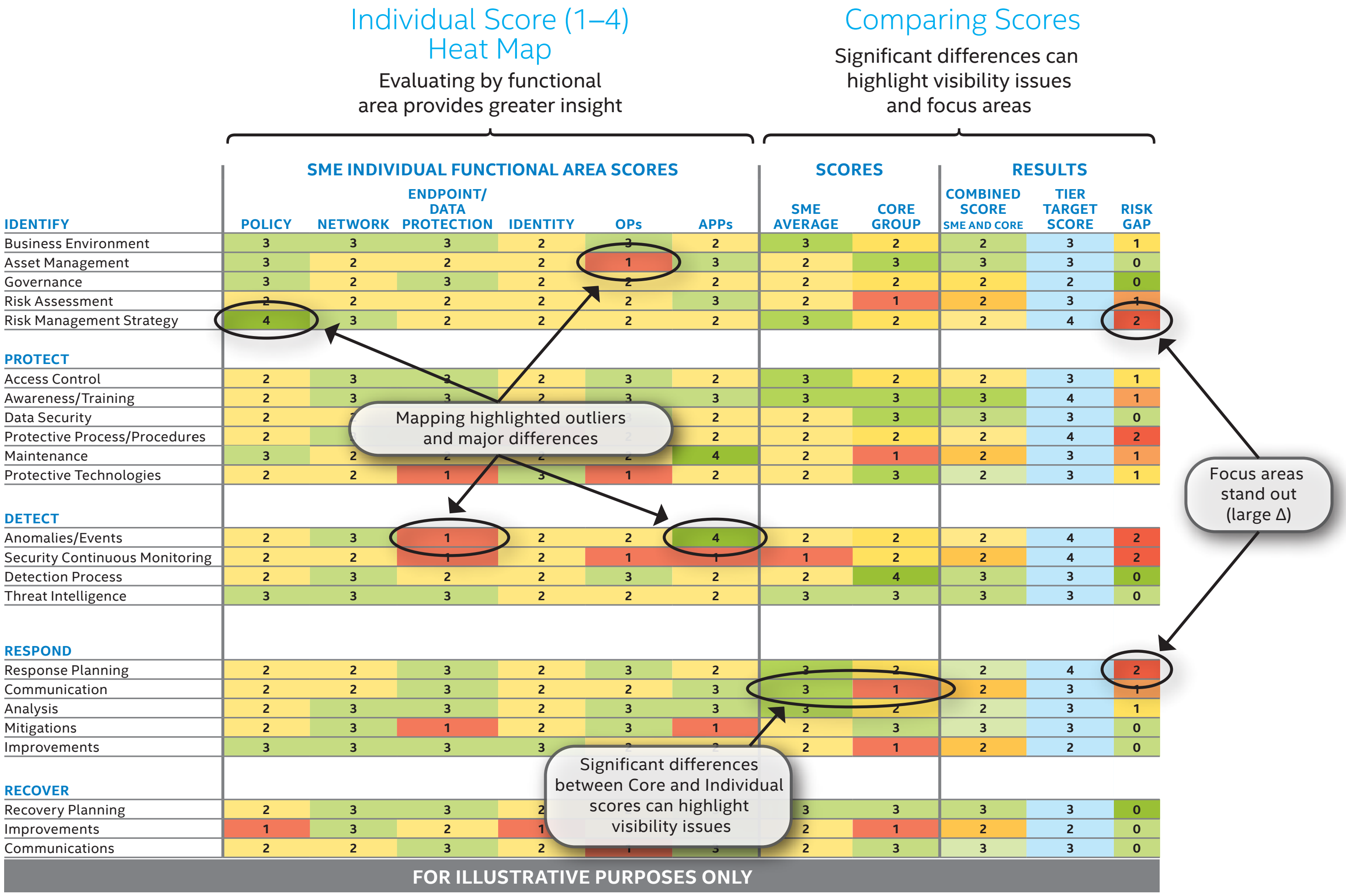
We analyzed the individual SME scores and compared them to the Core Group scores and the target scores (see Figure 1). Significant differences between Core Group and individual SME scores can identify visibility issues, either by the individual SME or the Core Group.

Using a heat map format to identify score differences greater than one, we examined areas of concern at the Subcategory level to further identify specific areas for improvement.

Phase 4 – Communicate Results

We reviewed our findings and recommendations with the CISO and staff. A key component of this phase was to revalidate target scores with the CISO and key stakeholders, in the context of the assessed scores. This process fostered a dialogue and helped us agree on risk tolerance and prioritization.

We also informed the capability and process owners who were impacted by the results of our discussion. Conveying this information helped us prioritize the key issues in the budgeting and planning cycles and examine where additional, more granular risk assessments should be prioritized.

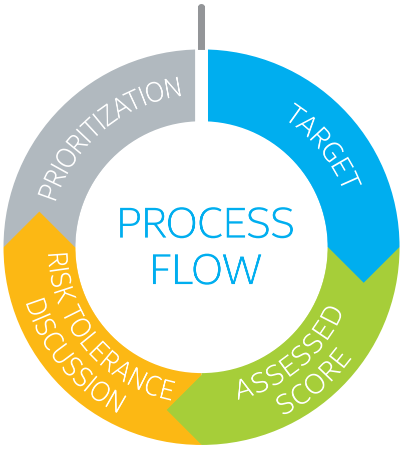

Individual Score (1–4)
Heat Map
Evaluating by functional
area provides greater insight
Comparing Scores
Significant differences can
highlight visibility issues
and focus areas
Mapping highlighted outliers
and major differences
Significant differences
between Core and Individual
scores can highlight
visibility issues
Focus areas
stand out
(large Δ)
FOR ILLUSTRATIVE PURPOSES ONLY

	SME INDIVIDUAL FUNCTIONAL AREA SCORES						SCORES		RESULTS		
IDENTIFY	POLICY	NETWORK	ENDPOINT/ DATA PROTECTION	IDENTITY	OPs	APPs	SME AVERAGE	CORE GROUP	COMBINED SCORE SME AND CORE	TIER TARGET SCORE	RISK GAP
Business Environment	3	3	3	2	3	2	3	2	2	3	1
Asset Management	3	2	2	2	1	3	2	3	3	3	0
Governance	3	2	3	2	2	2	2	2	2	2	0
Risk Assessment	2	2	2	2	2	3	2	1	2	3	1
Risk Management Strategy	4	3	2	2	2	2	3	2	2	4	2
PROTECT											
Access Control	2	3	3	2	3	2	3	2	2	3	1
Awareness/Training	2	3	3	2	3	3	3	3	3	4	1
Data Security	2	2	[illegible]	2	3	2	2	3	3	3	0
Protective Process/Procedures	2	3	[illegible]	[illegible]	2	2	2	2	2	4	2
Maintenance	3	2	2	2	2	4	2	1	2	3	1
Protective Technologies	2	2	1	3	1	2	2	3	2	3	1
DETECT											
Anomalies/Events	2	3	1	2	2	4	2	2	2	4	2
Security Continuous Monitoring	2	2	1	2	1	1	1	2	2	4	2
Detection Process	2	3	2	2	3	2	2	4	3	3	0
Threat Intelligence	3	3	3	2	2	2	3	3	3	3	0
RESPOND											
Response Planning	2	2	3	2	3	2	3	2	2	4	2
Communication	2	2	3	2	2	3	3	1	2	3	1
Analysis	2	3	3	2	3	3	3	2	2	3	1
Mitigations	2	3	1	2	3	1	2	3	3	3	0
Improvements	3	3	3	3	2	2	2	1	2	2	0
RECOVER											
Recovery Planning	2	3	3	2	2	3	3	3	3	3	0
Improvements	1	3	2	1	[illegible]	[illegible]	2	1	2	2	0
Communications	2	2	3	2	1	3	2	3	3	3	0

FOR ILLUSTRATIVE PURPOSES ONLY

Figure 1. A heat map resulting from charting individual and group scores and their comparisons. *Note: The scores given are examples and not the actual scores.*

Repeatable Process Flow



Training Topics

We provided training to the SMEs who would be performing the individual scoring. We also trained facilitators who will be able to conduct future risk assessment sessions with Core Group members and SMEs to set the target score and perform the Tier target scoring.

- **SME training.** Topics included a brief history of the Framework and why Intel is implementing it, an explanation of how the assessment fits within Intel's decision making process, and a use case example. These one-hour training sessions were delivered virtually and included a question-and-answer period at the end.
- **Facilitator training.** Topics included guidance on the customized Tier maturity descriptions, the difference between the target and assessed scores, and how the prioritization/risk tolerance discussion is handled. We stressed the importance of adhering to the process flow and repeating the process year over year.

Results and Benefits

One of the most important and valuable benefits of the Framework pilot project was the internal discussions it helped foster. Conversations about defining the organization's Profile to determine the various levels of risk the organization is willing to accept are extremely valuable in aligning and prioritizing an organization's cybersecurity risk management activities. The target score versus assessed score discussions were especially instructive, as they enabled participants to discuss and compare risks across domains in a common language and on common ground. They also helped facilitate agreement between stakeholders and leadership on risk tolerance and other strategic risk management issues, understandings which in turn can guide the organization in security project prioritization and funding.

One of the most important outcomes of our pilot was proving the value of establishing an organization-specific Profile through internal dialogue based on the threats, vulnerabilities, and impacts the organization faces. Because these security aspects are best understood by an organization going through this process itself, we believe that creating a tailored Tiers Profile will provide the most value for organizations.

We also gained the following benefits:

- The Framework pilot project was effective in improving alignment to a common risk management methodology and language across internal stakeholder communities.
- When we started to define our own Subcategories, we again found value in the dialogue, which resulted in improved cross-team alignment on the processes and capabilities that comprised a Category. In addition, the Subcategories specific to Intel enabled SMEs and stakeholders to better understand the Categories. Finally, by aligning the Subcategories to our capabilities, we can more easily see where more detailed assessment is needed.
- Mapping assessments of common Core items by SMEs in a single risk heat map enabled quick identification of outliers, significant variances, and visibility issues. Highlighting these issues led to additional discussion and assessment, allowing us to further improve visibility into our risk landscape.

  By similarly mapping results from across other elements of our infrastructure (*Manufacturing, Design,* and so on) we anticipate being able to visualize certain organizational trends and groupings regarding our risk landscape. Gaining the benefit of these new insights would be more difficult without a unifying mechanism like the Framework.

- The pilot project resulted in developing tools that we can reuse as we expand the Framework's use across Intel. These tools included the following:
  - Risk-scoring worksheet
  - Heat map
  - Customized Tier definitions (People, Process, Technology, Ecosystem)
- The training materials for assessors and facilitators developed during the pilot project can be reused.

We achieved these results with a cost of under 175 FTE (full-time employee) hours. This low cost was due to several factors, including the Framework's alignment to existing industry risk management practices and our own established risk management culture and set of practices across Intel business units.

<175

We achieved results with a cost of under 175 full-time employee hours.

Key Learnings

The following list summarizes the key learnings attained during our pilot project.

- **Start where you are comfortable.** It made the most sense for us to start with the *Office* and *Enterprise* business functions because our IT Security organization had already begun similar efforts that we could leverage as far as management commitment and resources. These existing efforts meant that the *Office* and *Enterprise* risks were fairly well understood, so we could apply the Framework quickly. Also, the existing Framework Categories map well to the *Office* and *Enterprise* environments.

  Now that we have proved the validity of the Framework and shown that we can gain value from it, we can scale the application of the Framework to our other *DOMES* functions, such as *Design* and *Manufacturing*.
- **Perform continual iteration with the decision makers throughout the process.** Cyber risk management is not an end result; it is a continual process. Therefore, an ongoing process of iteration and validation results in a ongoing dialogue about risk. This process also results in a more successful Framework implementation, because the SMEs and the decision makers give and receive feedback—better aligning the Framework to the organization's business processes and priorities.
- **Use group collaboration mixed with individual scoring.** We found that the Core Group's initial work, combined with individual SME assessment and scoring, provided more effective results than if we had used just a single approach. For example, the dialogue that occurred between the Core Group members was especially helpful in setting the target scores. In contrast, the individual SME scoring and input proved valuable because it provided a deeper drill down and a SME-specific perspective, such as networking or operations.
- **Tailor the Framework to your business.** We believe that an organization should define a Tiers Profile that best fits that organization's needs. Additionally, adding, changing, or deleting Categories and Subcategories helps the Framework align with an organization's business environment. All of the work that our own team did provided invaluable discussion and insights that we could not have found externally, imported from other sources.

Conclusion

While we are at the preliminary stages of fully understanding the Framework and how it can be deployed across Intel, our early experience with the Framework has proved valuable. Some of the benefits realized through our Framework pilot project in the *Office* and *Enterprise* environments include harmonization of risk management technologies and language across the enterprise; improved visibility into Intel's risk landscape, helping identify both strengths and opportunities to improve; better-informed risk tolerance discussions; and the ability to better set security priorities, develop capital and operational expenditure budgets, and deploy security solutions.

We plan to extend our successful Framework pilot project to other areas of Intel's critical business functions, such as *Design, Manufacturing,* and *Services* over the coming months.[1] As we continue working with the Framework at Intel, we hope to gain a better understanding of Tiers and plan to further explore the use of Categories and Subcategories. As various internal risk management and governance processes start or reach appropriate milestones, we will also introduce Framework concepts and integrate applicable portions into these processes.

We believe that as the Framework matures and evolves it should include the cyberthreat intelligence lifecycle. Automated indicator sharing is included in the Framework Roadmap;[2] however, that is just the mechanism by which intelligence can be shared. Cyberthreat intelligence is a much broader discipline, essential to a robust cybersecurity risk management program and needs attention in the Framework. Organizations must have a robust understanding of the following cyberthreat intelligence aspects to best prepare for and respond to cybersecurity attacks:

- Relevant threat agents and actors
- Threat agents' and actors' tactics, techniques, and procedures
- Incidents and campaigns

Incident handling and vulnerability management are also essential pieces of cybersecurity risk management and warrant consideration for inclusion in future versions of the Framework.

Because we believe other organizations can also benefit from deploying the Framework, Intel and Intel Security are participating in extensive outreach regarding the Framework. This outreach includes meeting with governmental officials, attending conferences, seminars, webinars, and summits, and publishing blogs. Raising awareness and encouraging best practices is an integral and ongoing part of Intel's efforts to foster improvements in global cyber risk management; in our initial experience the Framework has proved a useful tool in furthering these overall efforts.

To read about the Cybersecurity Framework, visit: **nist.gov/cyberframework**

For more information about Intel's technology solutions for federal government, visit: **intel.com/federal**

Follow the conversation: **#intelfederal**

Authors

Tim Casey
Senior Strategic Risk Analyst,
Intel Security Group

Kevin Fiftal
Civilian Director, Intel Americas

Kent Landfield
Director, Standards and Technology
Policy, Intel Security Group

John Miller
Director, Cybersecurity Policy &
Strategy, Intel Global Public Policy

Dennis Morgan
Chief Security Architect,
Intel Information Technology

Brian Willis
Manager, Threat Intelligence and
Infrastructure Protection,
Intel Security Group

Contributors

The authors wish to thank their colleagues who contributed to the pilot process, provided technical content, and reviewed this document. The authors would like to acknowledge Jack Lawson and Amit Agrawal for their valuable assistance throughout the development of this document. Thank you also to Jason Kimrey of Intel for his support and leadership of this project.

[1] For more information about how Intel is approaching security in its Manufacturing environment, see "Factory of the Future," 2014. www.mcafee.com/us/resources/white-papers/wp-factory-future.pdf

[2] For more information, see the "NIST Roadmap for Improving Critical Infrastructure Cybersecurity," 2014. www.nist.gov/cyberframework/upload/roadmap-021214.pdf

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS AND SERVICES. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS AND SERVICES INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Printed in USA ♻ Please Recycle 0115/KFIF/KC/PDF

Look Inside.™