White Paper
Information Security
January 2025

IT@Intel: Prioritizing Investments and Maximizing Security Using Capability-Based Planning

Intel IT improves information security capabilities and aligns them with Intel's business needs using a systematic scoring methodology and integration with enterprise architecture strategies

Intel IT Authors

Jason Devoys
Enterprise Security Architect

Magaly Perez
Enterprise Security Architect

Table of Contents

Executive Summary

Intel's Information Security (InfoSec) group has adopted capability-based planning (CBP) because it provides a foundational framework for evolving our capabilities to securely enable Intel's overall business strategy. This shift helps us align our group's strategies, prioritize projects and resources, communicate more effectively with business stakeholders, and, most importantly, reduce complexity. This makes our operations more Agile and responsive to changing business needs.

CBP is a planning methodology that drives business-focused outcomes by providing a systematic, objective, and holistic view of a group's capabilities. In our case, these capabilities center around InfoSec, such as Digital Identity and Access Management and Cyber Risk Management. Using a four-phase cyclical process of alignment, assessment, planning, and management, we can:

- Determine the maturity of every capability using a precise, mathematical formula.
- Identify and prioritize gaps between the current capability maturity and the desired level of maturity.
- Create a roadmap to resolve those gaps.

This comprehensive method of capability mapping and scoring delivers a unified view of capabilities and objectives to help teams collaborate and optimize cross-functional efficiency.

Contributors

Meital Israel, Program Manager, Information Security
Q Oka, Strategic Engagement Manager, Intel IT
Jeff Sedayao, Domain Engagement Manager, Intel IT

Acronyms

CBP	capability-based planning
InfoSec	Information Security

Business Challenge

Intel's Information Security (InfoSec) leaders, like many technology leaders, face the daily challenge of making decisions based on competing business priorities while also considering the rapidly evolving cyber threat landscape. While we have already achieved a significant level of maturity in our Agile delivery methods, a natural next step was to look at how we could further embrace business architecture and, more importantly, a capability-centric approach to enable us to focus on solving the following problems:

- Teams sometimes miscommunicate due to the lack of a standardized "capability" language.
- Dependencies between teams and programs are not always apparent.
- The prioritization methodology at the team or program level is inconsistent.
- The role that architecture plays in guiding the implementation efforts is not clear, both short term and long term.

These issues underscore the necessity to extend our Agile methodologies to achieve a more strategic unified approach to prioritization and planning, with enterprise architecture at the core. We believe that a consistent methodology empowers us to mitigate risks more effectively across the fast-changing cyber landscape and enables strategy-driven execution.

Solution

Our group took a leading role in addressing these difficulties by adopting capability-based planning (CBP).[1] Our experience and success with CBP can serve as a model for other Intel IT groups, as well as for IT departments at other companies that want to implement CBP themselves.

An Overview of CBP

Before using CBP, we found that traditional planning lacked a strategic viewpoint. Resource planning focused on people, skills, time, and technologies but didn't consider capability maturity. We learned that instead of concentrating on organizational hierarchies or specific technologies, which are subject to constant change, CBP enabled us to concentrate on processes, information, locations, and events to attain the desired outcomes for our business.

CBP is a planning methodology that focuses on business outcomes and goals. Its purpose is to provide an objective view of an enterprise's capabilities so that projects or work efforts can be coordinated across organizational boundaries seamlessly. CBP remains business-driven by focusing on planning, engineering, and delivering strategic business capabilities to the enterprise. It combines the requisite efforts of all lines of business to achieve the desired capability.

In summary, CBP provides a holistic view of capabilities that are defined and managed through a partnership between the business and IT. The capabilities are assessed, and the identified gaps are prioritized and fed into the planning process for resolution. CBP is compatible with our Agile DevOps methodology; we plan and execute capability increments (projects/programs) based on strategic importance to the company and its business goals.

Enterprise architecture is the vehicle for CBP—architecture and strategy are two sides of the same coin. We use enterprise drivers, internal drivers, and the target vision to feed capabilities into a business outcome statement. Then, the CBP methodology guides transformation through enterprise architecture to produce strategy, architecture development, and tangible results.

CBP Stages

CBP involves a recurring cycle of four stages: align, assess, plan, and manage (see Figure 1).

Figure 1. The four stages of capability-based planning (CBP).

[1] See https://pubs.opengroup.org/togaf-standard/business-architecture/business-capability-planning.html for more information.

Align

Because our group is focused on InfoSec, we have a specific set of capabilities. Other IT groups, such as those supporting manufacturing or those responsible for client device health, would have different capabilities. However, the alignment process is the same. Figure 2 illustrates a generic, level-2 (L2) capability map for a Cyber Security-focused organization.

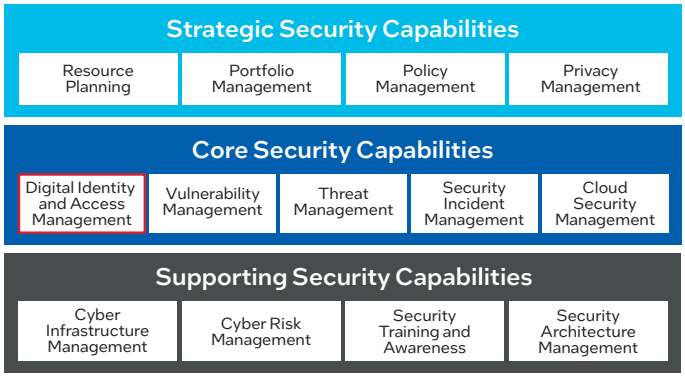

Figure 2. High-level InfoSec capability map.

Now, let's drill down into just one of those capabilities from Figure 2: Digital Identity and Access Management. Figure 3 shows how this L2 capability can be further broken into sub-capabilities (L3, L4, L5, and so on). With this detailed view of all our capabilities, we are ready for the next phase.

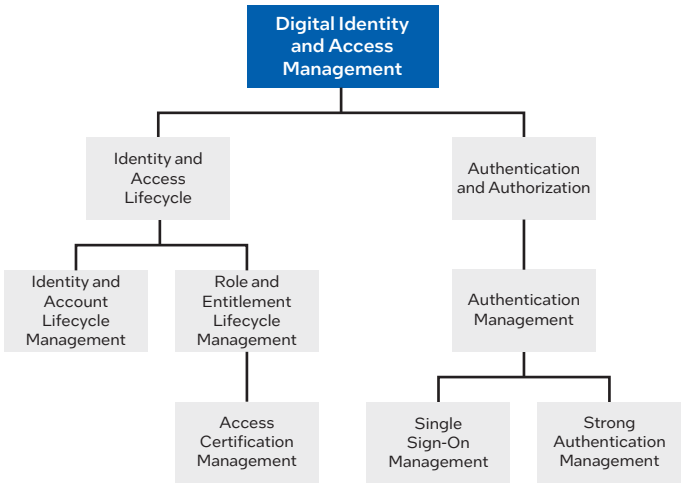

Figure 3. Lower-level InfoSec capability model.

Assess

During this phase, we systematically score and prioritize each sub-capability based on a formula. For some capabilities, it may be appropriate to perform a formal risk assessment to determine risk level and gaps in controls, which also enables us to detect any changes in the rapidly changing cyber threat landscape. This process provides the basis for the subsequent "Plan" phase. The formula identifies the sub-capabilities we need to transform along with the gaps between the current capability maturity and the desired level of maturity. The "Developing Our CBP Formula" section describes our scoring techniques in more detail.

We perform capability assessments once per quarter, aligned with our Agile methodology "releases." After the initial assessment, when we started using CBP, subsequent assessments do not start from scratch; we can update maturity scores for various features based on the previous three months of work.

Plan

After using the formula to identify which capabilities are the most important to improve or build, we use the Agile methodology to develop the following:

- Capability increments
- Three-year capability roadmap
- Features and user stories

You can think of capability increments as projects or programs. They are significant chunks of work that are grouped together to achieve common goals and help move the needle on a capability's maturity. During our Agile DevOps "Pre-Release Planning"—and via the close collaboration between architects, project managers and technical leaders—these capability increments are subsequently broken down into features and user stories. These features and user stories are usually time bound to a specific release of three months and are then assigned to project team members for implementation.

The planning phase is a crucial step that ensures a seamless connection between strategy, enterprise architecture, and execution. This comprehensive approach provides full traceability, which allows us to maintain alignment with our overarching goals throughout the process.

Manage

To ensure everything goes according to plan, we have established capability increment oversight and roadmap and execution monitoring.

As mentioned previously in the "Assess" phase, we execute the CBP cycle during each release, four times per year. Capability increments usually span multiple releases. So, it's important to be able to track progress to completion. This is where monitoring and oversight comes into play. Using our Agile methodology, we perform system demonstrations throughout a release to show evidence of continued progress. Additionally, at the end of a release, our Agile Train coaches and project managers help us to determine if we met the objectives that were set at the beginning of the release.

Subsequently, we revisit our roadmaps and make any adjustments as the timeline advances. We also perform post-implementation reviews known as retrospectives, to capture what went well, what didn't go so well, and what we need to do to improve. Our approach to monitoring and oversight sets us up for success for the next CBP cycle.

Choosing a CBP Framework

We based our CBP framework on the NIST 800-171 framework ("Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"[2]). This is a well-known framework that is designed for the cybersecurity domain. It's an industry best practice to adopt and adapt an industry framework rather than invent our own. This approach not only allows us to represent our security program but also aligns us with an industry-wide common language. It's important to note that other IT groups may choose to use a different framework that could be more useful for a different focus area, like supply chain or manufacturing. The key is that we're all part of this collaborative effort.

The important thing is to avoid allowing the framework to limit the overall vision. The framework didn't tie us down; we simply used it as an input. Also, after choosing a framework, we spent considerable time ensuring that the capability map was accurate. Investing in this effort is crucial for unlocking CBP's full benefits and ensuring organizational resilience in the face of change. Don't underestimate the value of this investment.

Developing Our CBP Formula

Once we had a framework and a comprehensive capability map, we developed a scoring formula that helped us pinpoint the areas where we needed to improve. Our systematic, objective approach gives IT and business leaders a repeatable, consistent, measurable, and data-driven view of their landscape that informs and justifies their decisions—all while revealing a holistic representation of an entire enterprise.

When assessing a sub-capability, we use three inputs, each with a defined range of values, and compare that to the forecasted target maturity for that sub-capability.

- **Strategic importance** (range is 1-3). This input assesses how important this capability is to Intel's overall strategy. The strategic importance of a capability can be as follows:
  - **1 – Base:** Can't function without it but doesn't have to be best-in-class.
  - **2 – Competitive:** Needs to be best-in-class.
  - **3 – Differentiating:** Secret sauce, needs to be built in-house because it is not available off-the-shelf.
- **Business goal importance** (range is 1-3). This input assesses the criticality of the capability to the business unit. The business goal importance of a capability can be as follows:
  - **1 – Business-Important:** Does not immediately impact or degrade the ability of the business to perform.
  - **2 – Business-Critical:** Directly impacts the business unit's critical functions or may have a non-impactful dependency on a mission-critical application.
  - **3 – Mission-Critical:** Directly impacts Intel's ability to function—ship, order, build, pay, close, network, communicate, and design.
- **Maturity level** (range is 1-5). This input assesses how mature the capability is. The maturity level of a capability can be as follows:
  - **1 – Initial:** Basic, ad hoc, and undocumented, with limited organizational support.
  - **2 – Responsive:** Partial capability is in place, with some repeatable processes, but is not necessarily a best practice or maintained.
  - **3 – Defined:** Well-defined, with significant tools and technology for key resources and in-progress metrics.
  - **4 – Managed:** Mature capability with advanced tools and technology, consistent processes across most regions, governance, and well-established metrics.
  - **5 – Optimized:** Advanced capability with leading-edge tools and technology, consistent processes across all regions and business units, advanced governance and metrics are driving change.

Besides calculating a current, baseline maturity level, we also calculate a target maturity level. The target maturity level for a capability is based on a forecasted target maturity rank for a specific timeline, which estimates the maturity level for the next calendar year, given we've made improvements toward narrowing the gaps we have identified. Ideally, we aim for a target maturity level score that falls between "Level 3 - Defined" and "Level 4 - Managed" because striving for "Level 5 - Optimized" is usually impractical and would diminish the return on investment in CBP as a whole.

Once every sub-capability of a capability has been assessed, we feed all the inputs into a dashboard that determines an overall capability score by calculating the average value of each of the sub-capability inputs. Let's look at an example of how the scoring works (see Figure 4).

Capability 1 Summary

L3	Strategic Importance *Range 1-3*	Business Goal Importance *Range 1-3*	Current Maturity Level *Range 1-5*
Sub-capability 1	3 - Differentiating	1 - Important	4 - Managed
Sub-capability 2	2 - Competitive	2 - Business Critical	2 - Responsive
Sub-capability 3	3 - Differentiating	3 - Mission Critical	1 - Initial
Sub-capability 4	1 - Base	3 - Mission Critical	3 - Defined
Overall Result (L2)	**2.25** Competitive	**2.25** Business Critical	**2.5** Defined
Target Capability Maturity Level *Range 1-5*	**3.5** Defined		

Figure 4. Sub-capability scoring example.

This example shows an L2 capability with four L3 sub-capabilities. In the lower section of the figure, you can see sub-capability 1 has inputs of Differentiating/Important/Managed, sub-capability 2 has inputs of Competitive/Business Critical/Responsive, and so on. The compiled score for each of the L2 capability inputs is the average of the four sub-capability ratings: For example, for the current maturity level, the compiled score is:

(4+2+1+3)/4 = 2.5 Compiled Score

[2] For more information, visit https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final.

The value of 2.5 for this L2 capability input means its maturity level is about halfway between being Responsive and Defined. The other L2 capability input scores (strategic importance and business goal importance) are calculated the same way.

Using the individual capability scores, we can calculate an overall capability assessment score using the following formula:

$$\text{Capability Assessment Score} = \frac{\sum_{i=1}^{N} \left([\text{Strategy}]_i \times [\text{Business Goals}]_i \times (6 - [\text{Maturity}])_i \right)}{N}$$

Where N = Number of capabilities

The dashboard can display an overview of all capability assessments, which helps product owners and program managers objectively prioritize decisions. The higher the assessment score, the more important it is to address the gaps between the capability's current state and its target maturity level. These high-scoring capabilities are given priority because they present a higher risk to the business. We mitigate the risk by hardening the capability, thereby improving Intel's overall security posture.

Encouraging Collaboration

We conduct a specific cross-Agile Release Train collaboration event every quarter as part of our planning process. Each Agile Release Train sends a representative to the event and presents what they will be working on in the coming three quarters. If a capability increment has dependencies on other Agile Release Trains, this collaboration helps uncover them, and we can use the CBP tool to communicate the necessary changes. We have held several collaboration events so far and found that they increase visibility, with everyone speaking the same CBP language.

Results

We have seen benefits from adopting CBP both in our own group, and potentially across Intel as CBP adoption grows.

InfoSec-Specific Benefits

Identifying and assessing our capabilities lets us clearly understand what is required to drive maturity within each security domain, such as Digital Identity and Access Management or Cyber Risk Management. This, in turn, allows us to craft actionable and informed strategies that prioritize resources effectively, ensuring we can adapt to emerging business demands with agility.

The standout benefit of CBP lies in its ability to manage risks more effectively, consistently, and objectively. We can identify potential vulnerabilities and gaps in our organization's structure by comprehensively evaluating our capabilities. With this knowledge, we implemented targeted risk mitigation measures, safeguarding the organization against potential threats.

Here are some detailed benefits of CBP for our InfoSec group:

- Strengthened InfoSec strategic alignment
- Optimized resource allocation for critical security capabilities
- Proactive risk management
- Enhanced security performance tracking
- Improved collaboration for shared security
- Responsive adaptation to third-party security frameworks

Intel-Wide Benefits

As other Intel IT groups—and even business units—see the positive outcomes of CBP, we hope they also begin to adopt it, which would multiply the benefits across all of Intel. Furthermore, CBP has already fostered collaboration across departments and teams. With a unified understanding of capabilities and objectives, teams can work in sync to break down silos and optimize cross-functional efficiency.

In addition, third-party auditors, who are brought in to evaluate how our InfoSec group aligns with business needs, have validated what we have done. They were able to understand it and considered it a strong sign of our group's overall maturity.

Conclusion

Establishing the CBP methodology gave us a comprehensive view of our capabilities, enabling us to devise actionable strategies, optimize resources, enhance agility, manage risks, and foster collaboration. The integration of cybersecurity initiatives further underscores the relevance and value of CBP in aligning business objectives and mitigating potential threats. As a result, our organization stands ready to navigate the dynamic business landscape with resilience and adaptability, setting a benchmark for excellence in the industry.

Our comprehensive method of capability mapping and a formulaic scorecard captures the strategic importance, business goal importance, and capability maturity score. It highlights what is required to execute initiatives successfully. Our solution addresses our long-standing InfoSec planning challenges but can also be applied to other IT groups and even other industries. Adopting CBP is an excellent way to align every decision with its strategic vision and capabilities and drive sustained enterprise success.

Related Content

If you liked this paper, you may also be interested in these related stories:

- Security Architecture Enables Intel's Digital Transformation
- Enterprise Architecture: Enabling Digital Transformation at Intel
- Enterprise Technical Debt Strategy and Framework
- Data Center Strategy Leading Intel's Business Transformation
- Data Center Facilities Risk Management
- Advancing Intel's Security Posture with CrowdStrike

For more information on Intel IT best practices, visit intel.com/IT.

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation on **X** or **LinkedIn**. Visit us today at **intel.com/IT** if you would like to learn more.