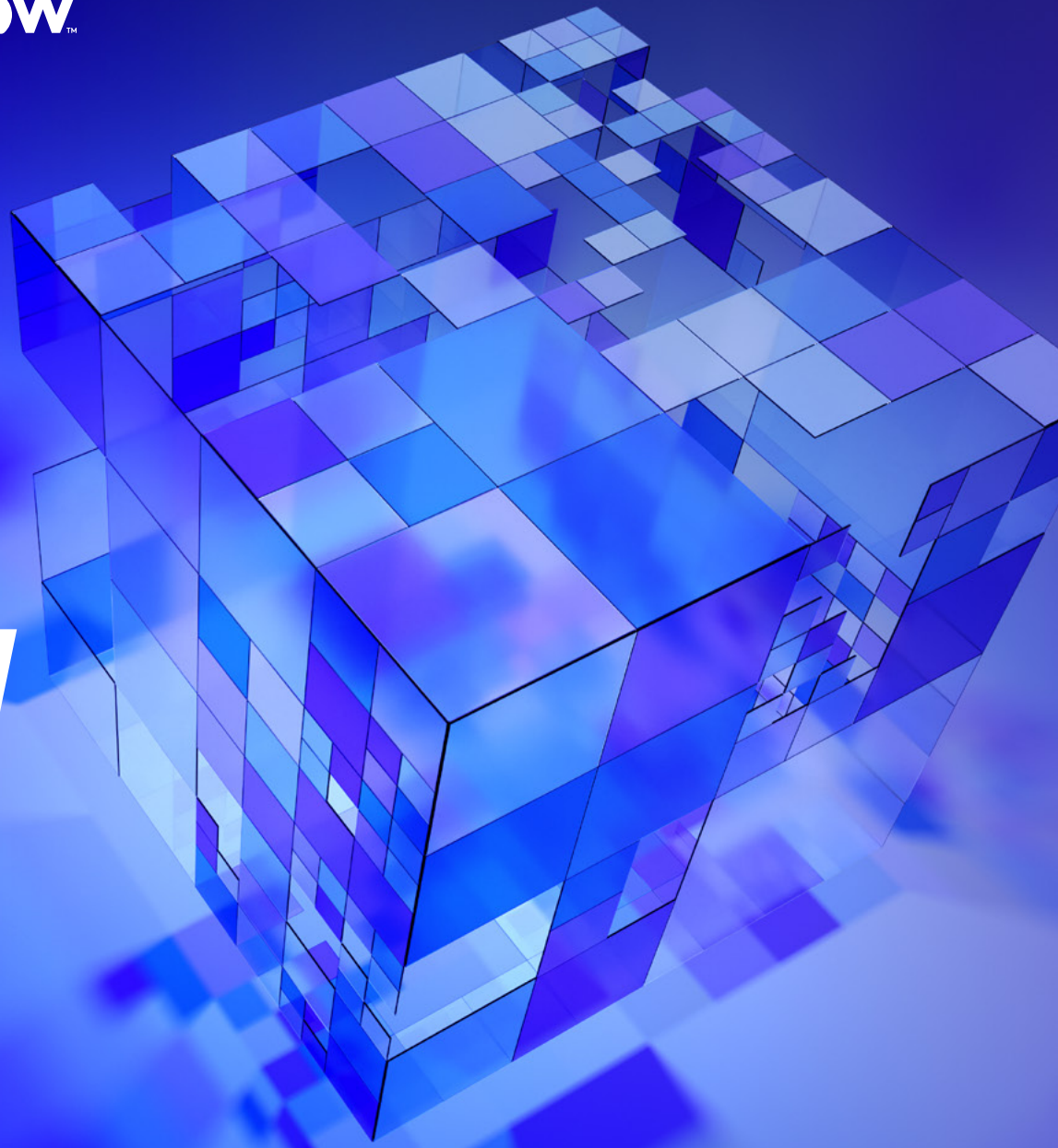
KPMG | servicenow

Constructing a cohesive cybersecurity foundation

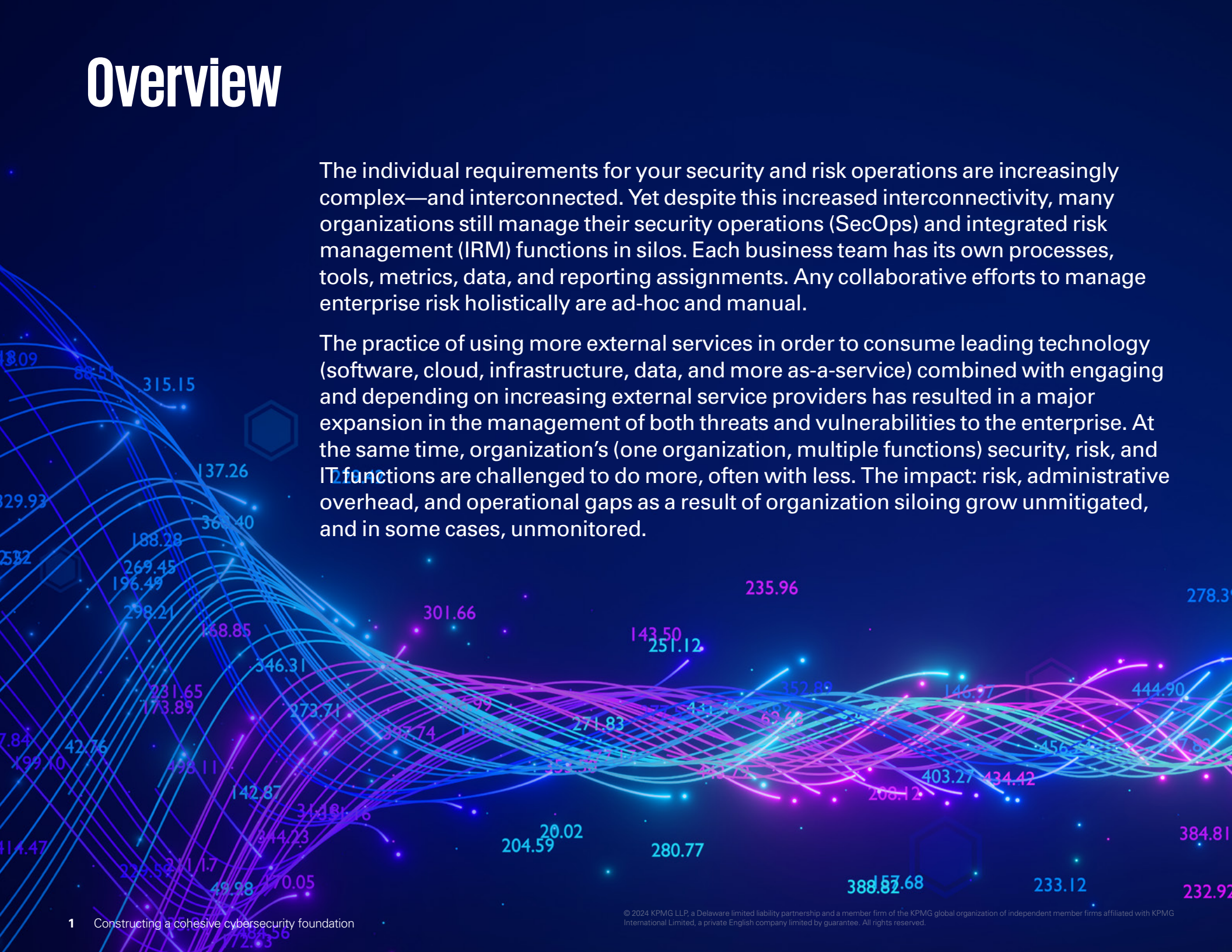
Unifying your Integrated Risk Management and Security Operations data with your CMDB



Overview

The individual requirements for your security and risk operations are increasingly complex—and interconnected. Yet despite this increased interconnectivity, many organizations still manage their security operations (SecOps) and integrated risk management (IRM) functions in silos. Each business team has its own processes, tools, metrics, data, and reporting assignments. Any collaborative efforts to manage enterprise risk holistically are ad-hoc and manual.

The practice of using more external services in order to consume leading technology (software, cloud, infrastructure, data, and more as-a-service) combined with engaging and depending on increasing external service providers has resulted in a major expansion in the management of both threats and vulnerabilities to the enterprise. At the same time, organization's (one organization, multiple functions) security, risk, and IT functions are challenged to do more, often with less. The impact: risk, administrative overhead, and operational gaps as a result of organization siloing grow unmitigated, and in some cases, unmonitored.



A unified defense model

Creating a unified defense model means connecting the risk and security products and processes, and most importantly, the data that supports them. This can be achieved by maturing and optimizing your ServiceNow Configuration Management Database (CMDB).

The CMDB is the cornerstone of insight-rich data for security operations and integrated risk management. It is the foundation that provides an accurate, comprehensive, and up-to-date view of the IT environment. This single source of truth is indispensable for maintaining a robust security posture and managing risks effectively. From vulnerability management to incident response, access control, compliance, and risk and impact determination, the CMDB's data is pivotal in all these areas. Therefore, maintaining the integrity and accuracy of the CMDB is of utmost importance for any organization's security and risk management strategy. It is the lighthouse guiding the way in the vast sea of IT infrastructure, illuminating potential risks and vulnerabilities. Without it, navigating the complex waters of cybersecurity would be significantly more challenging. Hence, the CMDB is not just an important source of data; it is the most crucial one and must always be the beacon of truth.

So, how do organizations ensure that the CMDB is capturing all the necessary data elements that are needed for an integrated security and risk operation, and ensuring it is properly maintained to allow for both automated maintenance and, more importantly, automated testing and response to threats?

A security and risk enabled CMDB improves the security posture of your organization.

To ensure the CMDB is capturing all the data elements needed to have an integrated and automated approach to risk and cyber protection, detection, and response capabilities requires data from security tools such as vulnerability scanners and Security Information and Event Management (SIEM) systems, IT compliance, and IT risk data. This is critical to support:

1. **Enhanced Threat Detection:** Vulnerability scanners, SIEM solutions and other 3rd party security technologies help detect and alert on system vulnerabilities and potential malicious activities, and these detections are pulled into ServiceNow for additional contextualization from the CMDB. This enriched data aids in prioritizing and assigning ownership for assessing and remediating potential threats and vulnerabilities.
2. **Improved Threat Hunting and Incident Response:** The additional context provided through enhanced CMDB data elements and correlation with other events, allows for quicker investigation and more relevant action to reduce response times.
3. **Contextual Understanding:** The CMDB, when integrated with vulnerability scanners and SIEMs, provides a comprehensive view of vulnerabilities and events affecting a given asset or service, as well as the current state of all cyber risk across the organization.
4. **Effective Risk Management:** By identifying the criticality of the configuration items across your enterprise, you can prioritize investigating and responding to organizational risks.
5. **Automated Compliance Management:** Linking assets associated with controls can provide real-time validation of IT compliance, configurations, and control testing results.

Proactively anticipate vulnerabilities and mitigate ever-changing security risks

Correlation of data from IRM and SecOps sources enhances the integrity and the quality of the CMDB, making it easier to assess hardware and software threats and vulnerabilities, prioritize potential threats, and speed the investigation and remediation of issues. Security and risk data can be synced for more efficient and accurate collaboration, decision-making, and reporting based on a comprehensive and up-to-date view of the enterprise's risk posture.

The steps to creating a security and risk-enabled CMDB: Assess, Automate, Scale

The journey to creating a security and risk-enabled CMDB requires planning, cross-organization alignment, and a commitment to creating a holistic, sustainable, and automation-driven configuration management function. The journey is summarized in the three key phases outlined on the following pages.

Phase 1: Assess

The first step in the overall journey is to conduct a fair, objective, and benchmark-driven assessment of your organization's CMDB, the data, and data elements that reside in it presently. This assessment should also include a review of data sources (integrations), the quality of the data, and how the CMDB is maintained from operational and quality assurance perspectives.

The assessment must also include an initial definition of the stakeholders involved, and should consist of representation from the organization's security, risk, and IT cohorts. After identifying the stakeholders, development of the future-state (desired) design of a security and risk-enabled CMDB is critical so that the assessment can be benchmarked accordingly. It should also be aligned to a common taxonomy that facilitates the needs of stakeholders, including those who may sit in organizations outside of IT, such as cyber security, and the associated data contributors.

Once you have determined what "good" looks like and your future state, begin assessing your current state by reviewing:

Your CI inventory: Connect CMDB librarians with associated IT cyber teams (IT compliance, IT risk, vulnerability management, and security operations) to identify value-add data and its alignment with the CMDB.

- Understand use cases
- Identify any missing configuration item (CI) classes
- Inventory business applications, servers, databases, network devices, and computers
- Inventory services

Your relationships and mapping: Determine where relationships exist between CIs and risk entities, and create them where they do not yet exist.

- Review and validate any existing relationships
- Create and execute a plan to establish the relationships between CIs and risk entities, including establishing the associated entity classes and types.

Your attributes: Review and validate the attributes from an IT stakeholder perspective; implement out-of-the-box attributes under IT guidance as applicable.

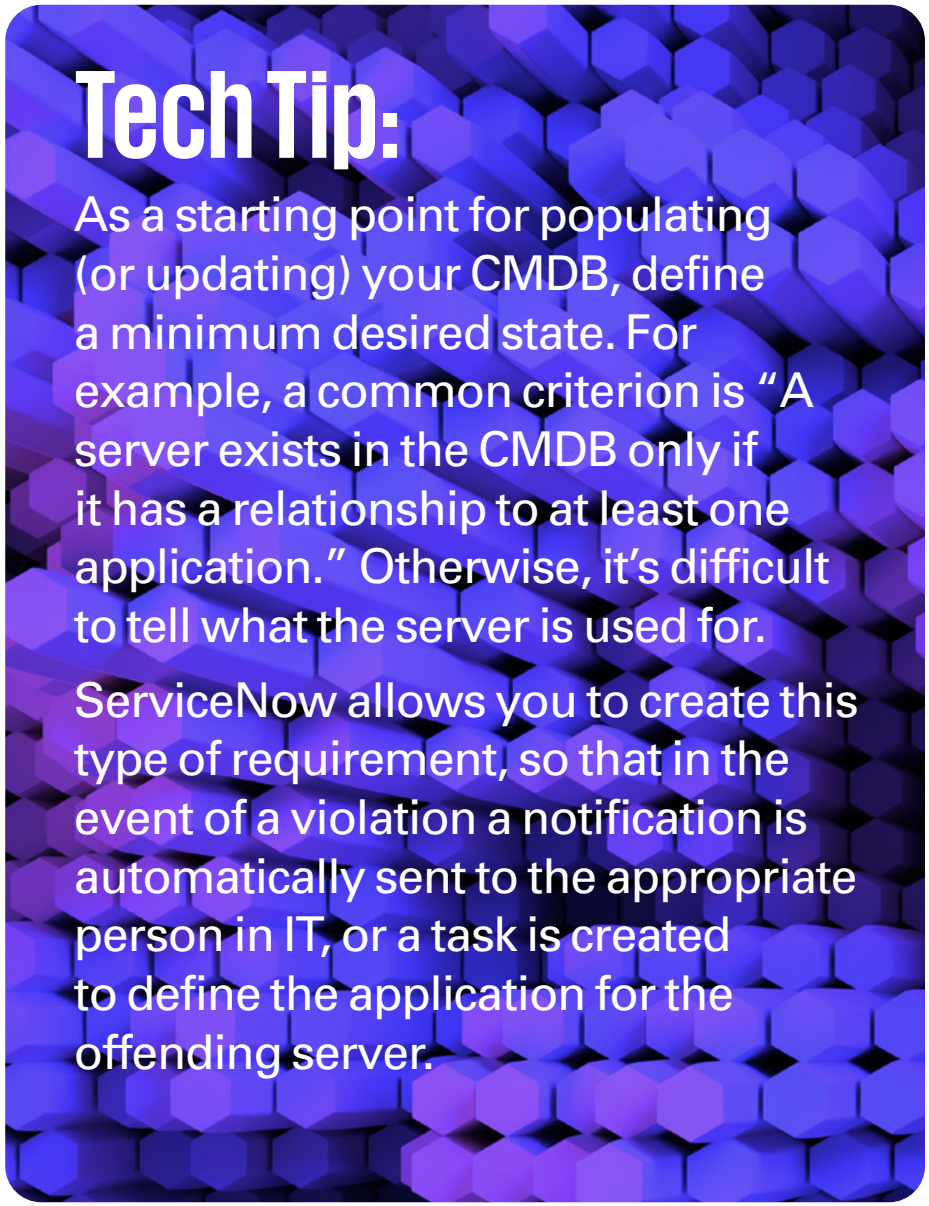
- Align to minimally-viable, core attributes
- Create class-specific attributes using a standardized taxonomy
- Include asset details
- Assign to users and groups

Your cyber related data: Define the cyber data elements required to support vulnerability response, security incident response, threat intelligence, and asset configurations, such as:

- Support groups for infrastructure versus application related issues, and the ability to discern each
- Reporting requirements and CMDB attributes required to support impact analysis for organization and technical views (i.e. business units, service owners, discrete services, networks, systems, etc.)
- Taxonomy for prioritization (i.e. DMZ, internal vs. external, Internet facing), and alignment between cyber tools and the CMDB.
- Risk exception, approval, and associated escalation processes and involved parties
- Involved Parties for communicating during major events such as data loss, breach, etc. and associated visibility requirements and restrictions (i.e. Legal, HR, Compliance, Risk, Executives)
- Identification of High Value Targets: Assets, Networks, Users

Note: Special consideration should be taken when standing up Security Operations as those programs and processes will inherently identify and need to respond to events for assets that may not be explicitly managed in the CMDB.

Once you have completed your assessment and determined the current state maturity of your CMDB, you can then put together a plan to modernize it to support the security and risk objectives we've discussed.



Phase 2: Automate

Once you have enhanced your CMDB to be risk and security-enabled, the next step is to introduce automation. Automating the entry of data into the CMDB and mapping CI relationships are crucial for resiliency. Automation streamlines risk, security, and IT operations, reduces manual errors, and enhances overall efficiency. It provides a clear, accurate visualization of the IT infrastructure, aiding in impact analysis, change management, risk management, and incident prevention, response, and remediation. Automation allows for a near real-time up-to-date CMDB, which allows for persistent, automated identification of potential vulnerabilities in the environment. It enables businesses to assess the impact of security incidents on CIs and their relationships, facilitating swift, informed responses to mitigate risks. CMDB automation is not just a business efficiency tool, but a vital component of a robust security and risk management strategy.

Considerations for automation should include:

Your infrastructure CI inventory: Integrate data and establish quality management tools and processes.

- Integrate vulnerability scanner(s), SIEM, IT compliance, and IT risk data
- Reconcile CIs to the CMDB, and automate the classification of deltas (endpoints such as laptops, computers, servers, and printers) as unmatched to be used as a litmus test and feedback loop to determine if the CMDB should contain these additional CI's
- Add agent-less discovery or agent-based tools
- Establish quarterly data certification reviews to ensure the accurate alignment of business owners, approval groups, and support owners to their associated CIs.

Your relationships and mapping: Automate manual mapping activities between business applications and their downstream infrastructure.

- Manually map upstream and downstream entities
- Enable filters to automatically map entities to entity types

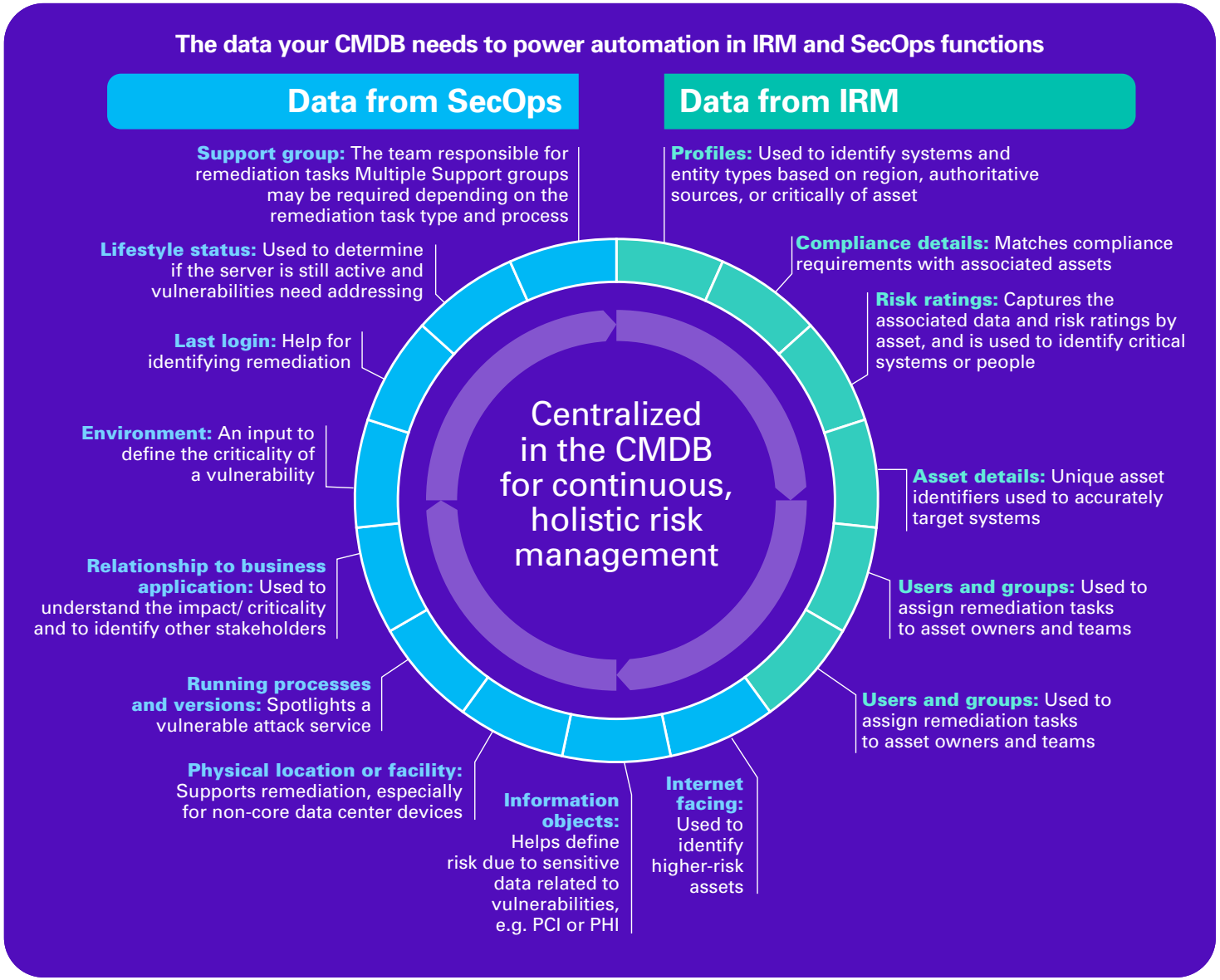
Your attributes:

Supplement out-of-the-box attributes with custom attributes designed per the coordinated input of risk, security, and IT stakeholders using an standardized taxonomy and aligned to support requirements and commonalities.

- Tech attributes from discovery
- Business services
- Risk ratings
- Compliance details
- Profiles

Design to protect: What to capture in the CMDB to automate and improve your IRM and SecOps processes

You can't protect what you can't identify, monitor, and measure. Capturing the right data in your CMDB, and rationalizing existing data, is critical to creating an optimized and automated risk and security-enabled CMDB.



Phase 3: Scale

The CMDB is an ever-evolving capability, and organizations in the third stage have implemented automated data populating and mapping tools, like ServiceNow Discovery and Service Mapping, and have well-established—and easily scalable—governance processes in place.

From their 360-degree view of the enterprise's risk-related physical, virtual, and cloud infrastructures, organizations in this stage can confidently extend strategic CMDB configurations to integrate more data and to automate new business processes.

As you begin to scale, you should consider:

Your infrastructure CI inventory: Extend CMDB enablement capabilities to other parts of the business.

- Support data-driven business outcomes
- Create and manage service models for the enterprise
- Enable enterprise wide integrated security and risk monitoring and mitigation capabilities

Your relationships and mapping: Implement automation-at-scale, including the assignment of business criticality based on the associated compliance of CIs with HIPAA, PCI, SOX, and other regulatory requirements. Then, IT cyber teams can quickly assess associated threats, vulnerabilities, and risks, and determine the impact of either accepting risk or performing mitigation.

- Automate upstream/downstream entity mapping based on CI relationships
- Automate mapping between entities and entity classes

Your attributes: Attributes are continuously updated based on new risks, risk ratings, incidents, and cross-enterprise input.

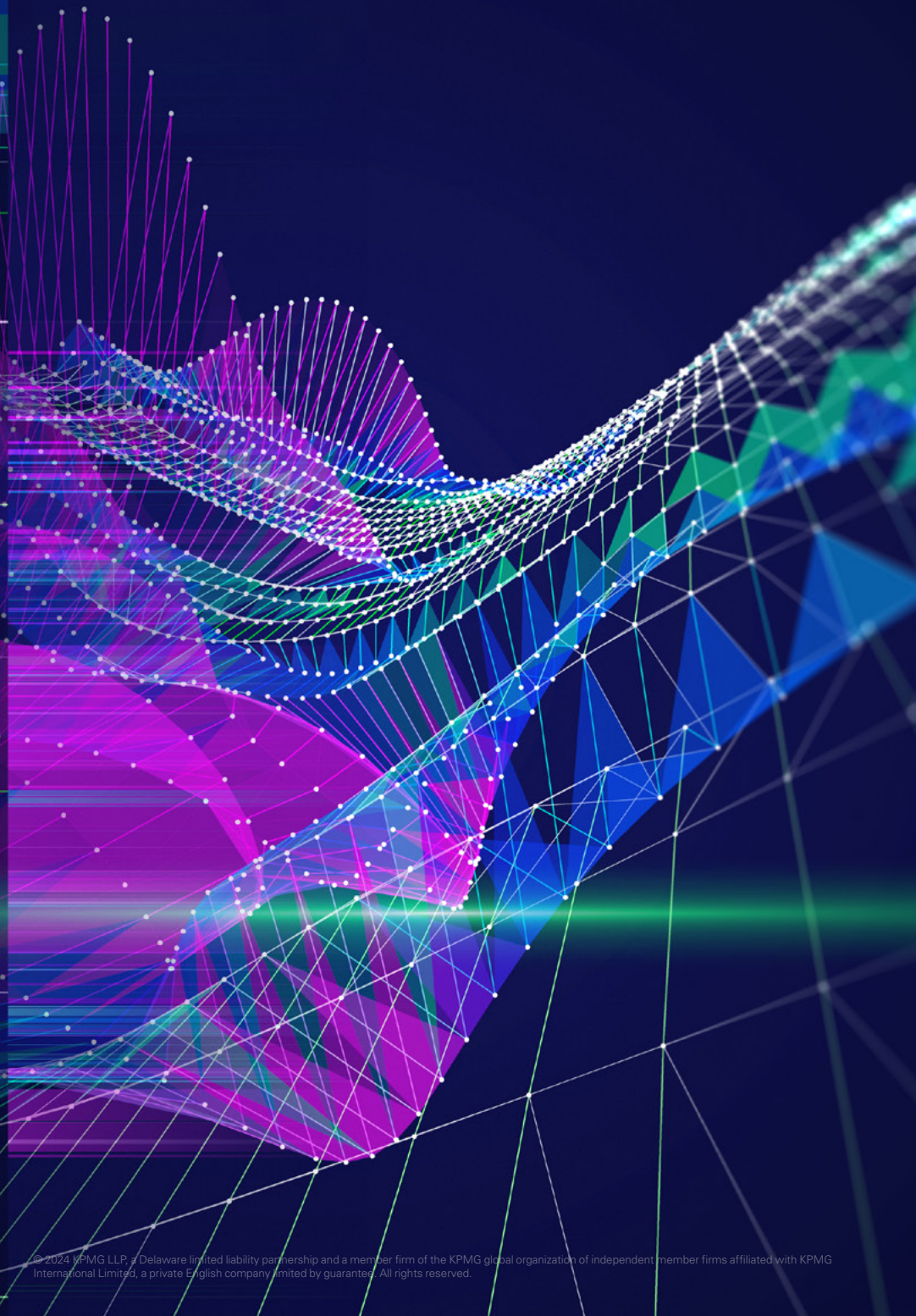
- Update attributes on CIs based on downstream IRM/SecOps process outputs

Take your first step toward creating a risk and security-enabled CMDB

The requirements for security and risk management are increasingly complex and harder to see. Organizations need a holistic view of the new, expanding risk landscape, and they need the ability to respond faster and with greater accuracy.

ServiceNow's native CMDB improves visibility and efficiency by de-siloing data and making it actionable in real time. Its cloud-based CMDB enables organizations to proactively manage technology, cyber risks, and compliance; continuously report on enterprise-wide risk; maintain business continuity and operational resilience; and manage third-party and supplier risks.

KPMG helps organizations optimize their technology with governance systems thoughtfully designed and deployed—unleashing the continuous maturation of your teams, systems, and cybersecurity posture.



Contact us

P. Michael Lutz
Principal, Advisory
mikelutz@kpmg.com
+1 415 963 5158

Angela Leggett
Managing Director,
Cyber Security Services
aleggett@kpmg.com
+1 614 241 4637

Caleb Queern
Managing Director,
Cyber Security Services
cqueern@kpmg.com
+1 512 320 5104

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates and related entities.

Learn about us in: | **kpmg.com**