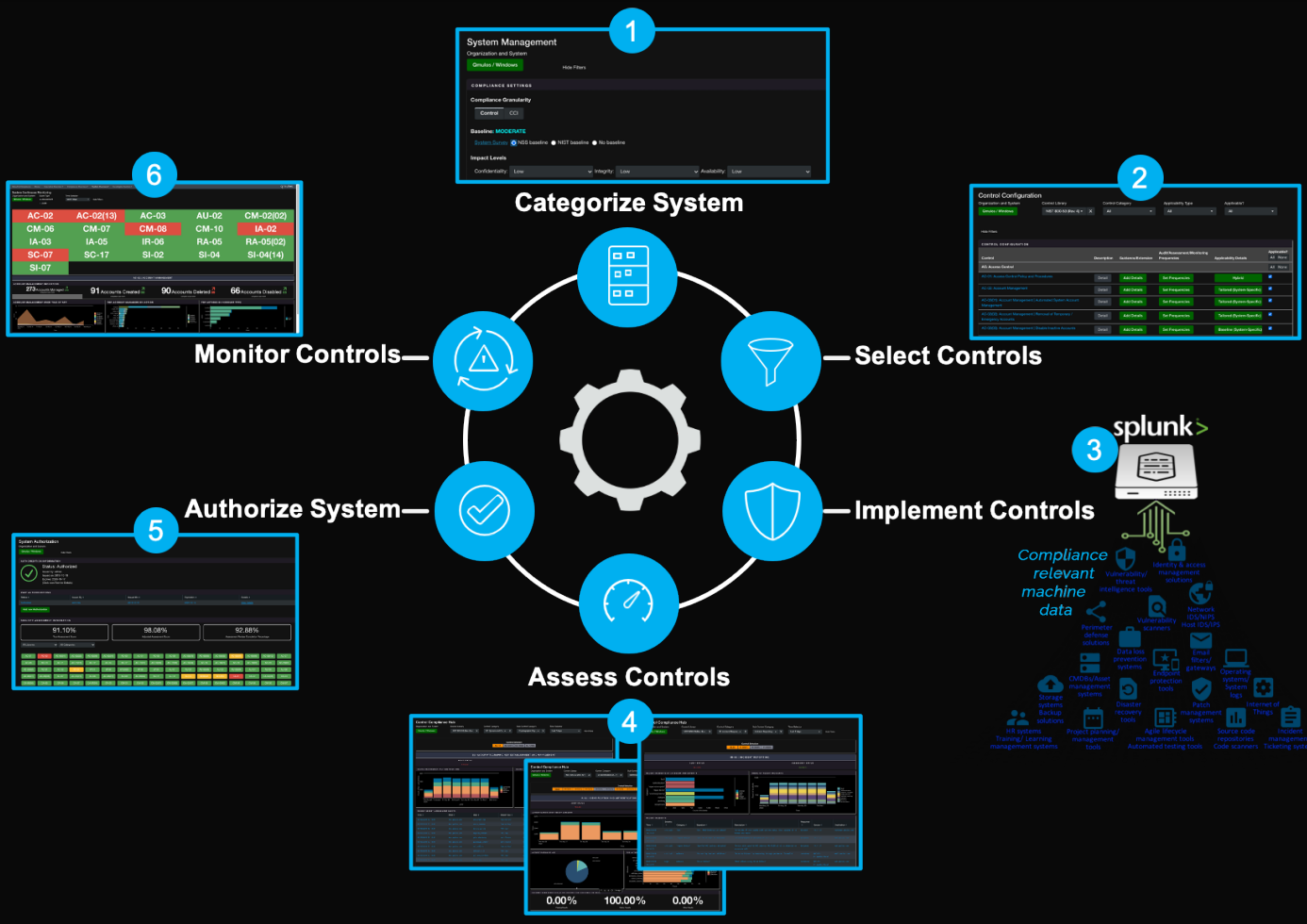
qmulos

DATA-DRIVEN RMF BLOG SERIES

Qmulos will be publishing a six-part blog series on a data-driven approach to the Risk Management Framework (RMF) defined in “NIST Special Publication 800-37 Risk Management Framework for Information Systems and Organizations.”

Why use a data-driven RMF approach?

A data-driven approach to RMF uses data automatically collected from your IT environment to streamline, automate, and inform decision-making to manage the cybersecurity risks with developing and operating your information systems. Traditional approaches focus on documenting and reviewing implementation statements along with static snapshots of technical evidence to assess if security controls are correctly implemented and operating effectively. As a result, this creates hundreds of pages of documentation based on outdated data, and provides little actual security value. Rather than just reviewing implementation statements and taking a “trust me” approach, a data-driven approach uses the machine data (e.g. logs, configuration settings, events, transactions, etc.) that’s automatically collected from your systems so that you can continuously monitor and verify that the controls are providing the required levels of protection.



In each part of this series, we'll be discussing each step of the RMF. Summarily, we will describe the key objective of that step, typical implementation, and what it means from a data-driven perspective. Furthermore, we'll discuss how our flagship continuous monitoring and compliance automation solution Q-Compliance enables a data-driven approach to implement that particular step of the RMF. Finally, we will explain how traditional approaches and GRC tools implement that step, and highlight benefits of the data-driven approach. Stay tuned, bookmark this page and check back regularly for links to each part as we publish them.

1. Part 1 – Categorize
2. Part 2 – Select
3. Part 3 – Implement
4. Part 4 – Assess
5. Part 5 – Authorize
6. Part 6 – Monitor

qmulos

qmulos

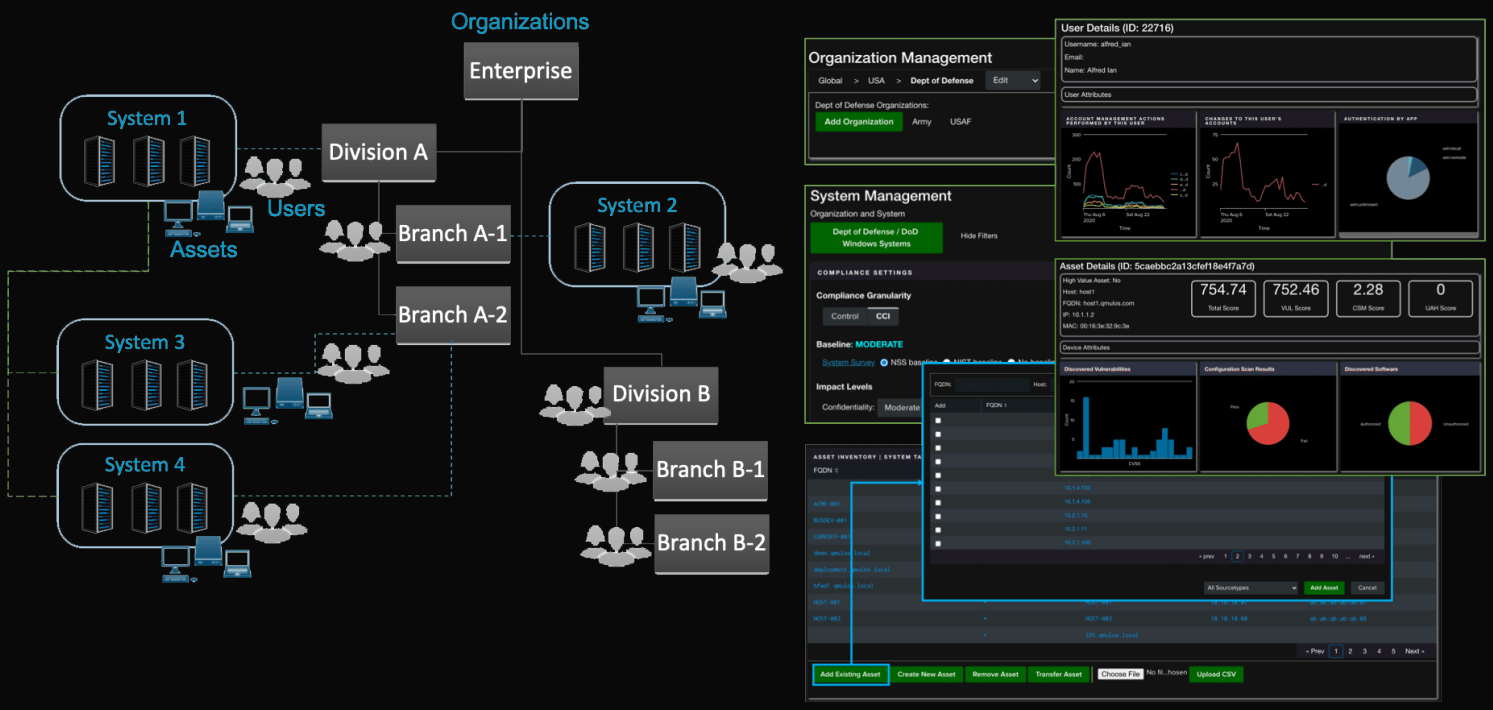
DATA-DRIVEN RMF SERIES – PART 1: CATEGORIZE

In part 1 of this series, we look at how the Categorize step of the Risk Management Framework is implemented using a data-driven approach. The main objective of the Categorize step is "to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems."[RMF]

So, break that down for me.

In essence, the Categorize step identifies what needs to be protected and the level of protection that is required. Identifying what needs protection requires documenting the characteristics of the system from a security and privacy perspective. Furthermore, this step includes defining things such as the authorization boundary; environment of operation; physical or other processes controlled by system elements; system component inventory; life cycle of the information types managed by the system; and system users and roles, amongst many other things.

From a data-driven perspective this means defining the subjects that you need to collect data about and monitor in subsequent steps of the RMF, i.e. the risk management subjects. Accurately and comprehensively defining these data subjects (i.e. entities in data modeling terms) in the beginning is critical to ensuring that you have the right set of data to fuel the entire process. In Q-Compliance, we support this critical first step with a foundational data model that comprehensively represents all the risk management subjects, e.g. organizations, systems, assets, users, etc. along with dynamic and flexible mechanisms to define and update them as they evolve over time, as shown in Figure 1.



Well, what are my options?

Many traditional GRC tools allow you to define these subjects as they are core to the RMF process. However, with those tools, you define and document, and that's it. They just stay as static documentation! In comparison, when you define your risk management subjects in Q-Compliance, you are not doing it just to create static documentation, you are setting up the key entities of a comprehensive risk and compliance data model which become the subjects of our analytics and scoring algorithms to help you streamline and automate subsequent steps of the RMF. For example, organizations aren't just names that show up in some document, they become completely navigable hierarchies of any level of breadth and depth so that you can gain a broad view of your entire enterprise's risk posture as well as pinpoint problematic departments.

Additionally, in Q-Compliance, systems, authorization boundaries, and asset inventories aren't just lists of IP addresses that appear in static spreadsheets. They are dynamically defined and act as containers and filters of machine data that's collected from your environment. Furthermore, data is presented on live

dashboards, allowing continuous monitoring, all in near real-time. Even more-so, users aren't just points-of-contact that show up in a System Security Plan. Instead, they are the subjects of rich analytics that monitor for access control, authentication, privileged access and potential insider threat activities.

Categorize with Q-Compliance:

The risks and threats that organizations are faced with today, are too numerous and dynamic. As such, taking a static documentation-based approach to implement this important foundational step of the RMF doesn't cut it anymore. The benefits of using Q-Compliance to implement a data-driven approach to Step One – Categorize include:

- Comprehensive data model to define your risk management subjects and all of their important security and privacy characteristics. No longer are they just static words in a document.
- Dynamic mechanisms to update the characteristics of the risk management subjects as they evolve over time.
- Advanced analytics and scoring algorithms that turn your risk management subjects into "living entities". These entities can be continuously monitored and assessed as they progress through the RMF lifecycle.
- Rich and intuitive dashboards to view and analyze your risk management subjects across the enterprise. The ability to drill down into individual sub-organizations, systems, users, assets and even individual events.

Explore the other RMF steps.

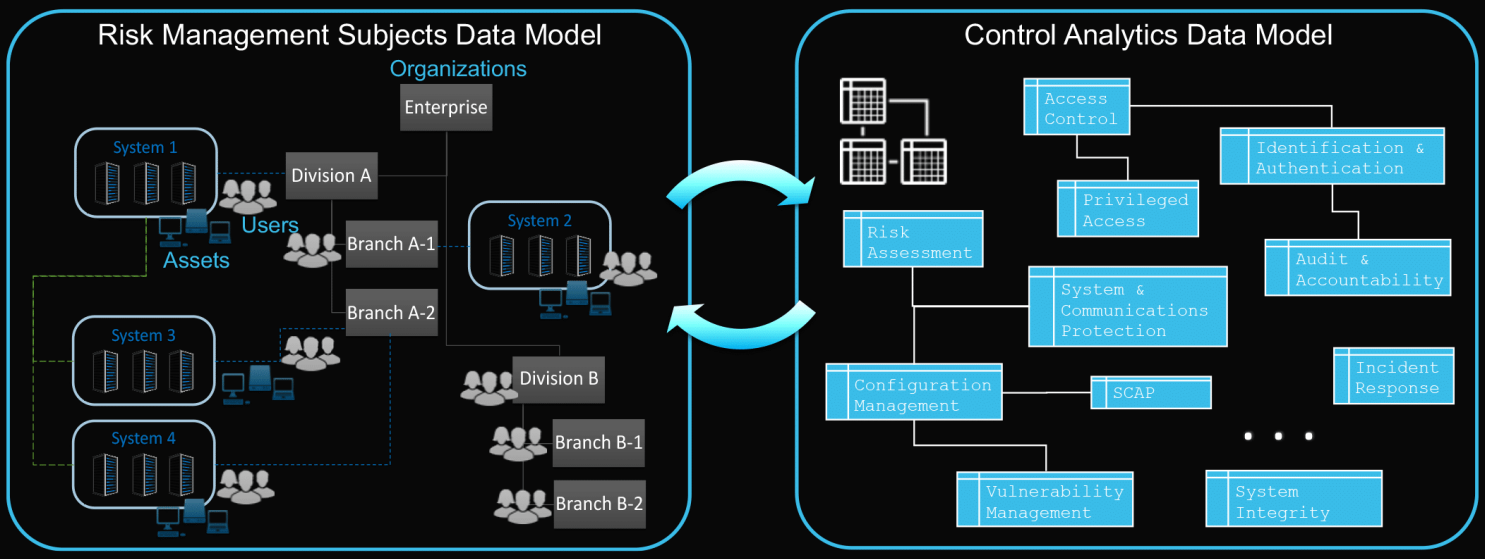
qmulos

DATA-DRIVEN RMF SERIES – PART 2: SELECT

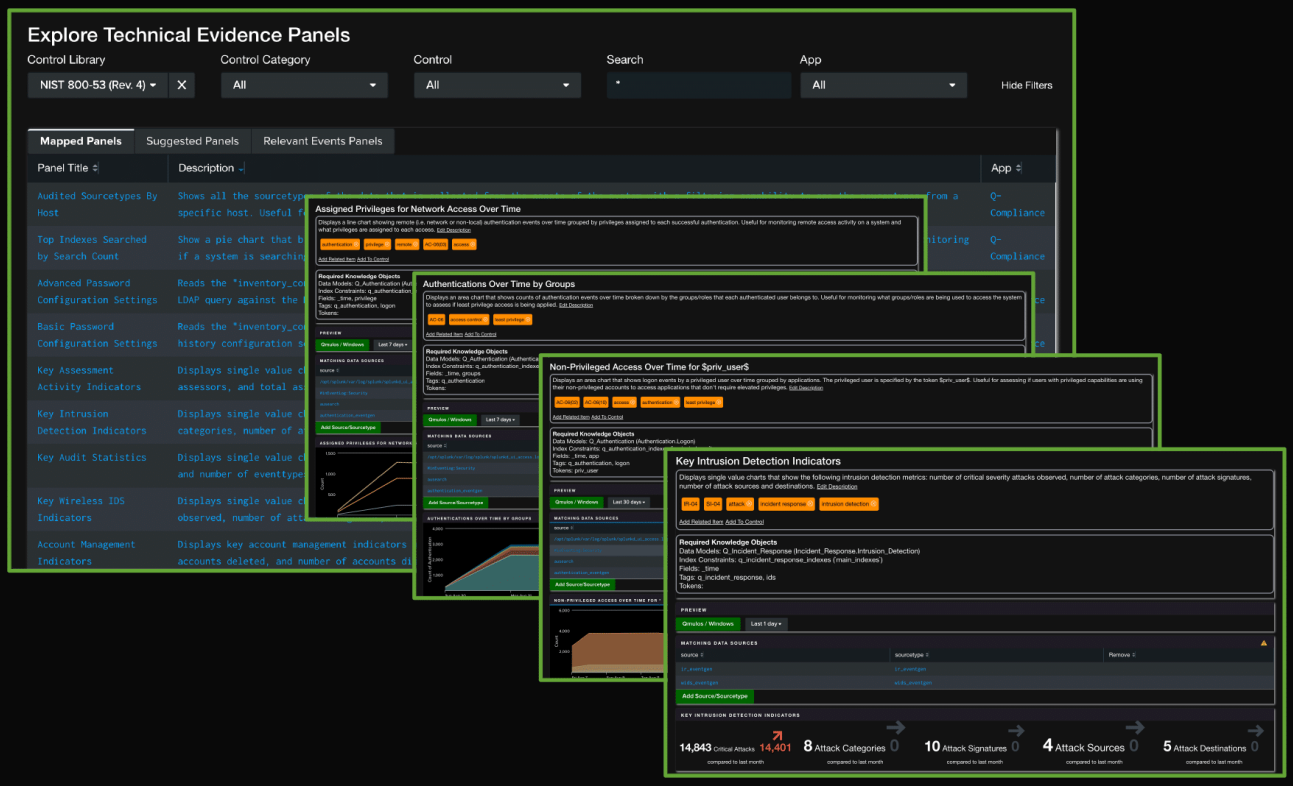
In part 2 of this series, we investigate implementing the Risk Management Framework's Select step, using a data-driven approach. The main objective of the Select step is to, "select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation." To achieve this, you firstly analyze the security and privacy objectives that have been defined in the Categorize step. Secondly, you determine what controls can be applied to implement those objectives using predefined baseline sets of controls and/or a more granular tailoring approach.

The Data-driven answer to "Select"

From a data-driven perspective, when you apply security controls you need to also enrich the supporting data set with additional entities that model the security domains of those controls. These additional entities and their associated attributes and events are linked with the risk management subjects that were identified in Step One – Categorize so that you can capture the data required to assess if those controls are correctly implemented and operating effectively. In Q-Compliance, we support this with a high performance analytics data model that complements the foundational data model that represents the risk management subjects, as shown in Figure 1.



In Q-Compliance when you select and apply controls to your systems, you are not doing that to just fill out the Minimum Required Controls section of your System Security Plan or to list them in the spreadsheet of your Security Controls Traceability Matrix. When you apply controls to your system in Q-Compliance, you are also applying the purpose-built analytics based on the control analytics data model that will help you continuously monitor and assess the effectiveness of those controls. Q-Compliance includes hundreds of out-of-the-box analytics that cover the controls from the world's most comprehensive security controls catalog — NIST 800-53, as shown in Figure 2.



Q-Compliance makes it easy to select and apply controls to your information systems. You can select a single high-water mark impact level for your systems or specify individual impact levels for the confidentiality, integrity and availability objectives and Q-Compliance will automatically apply the required controls based on the NIST 800-53 and CNSSI 1253 standards. You can also create and apply custom overlays with predefined sets of controls. For fine-grained tailoring, you can also apply or remove individual controls and control enhancements, inherit from common control providers, and add specialized control guidance and extensions. With our Dynamic Control Architecture, you can even select and apply custom controls. When applying controls to your systems using any of these methods you are also automatically applying the corresponding analytics that will help you assess and monitor these controls in steps four and six of the RMF.

The benefits of using Q-Compliance's data-driven approach to implement Step Two – Select include:

- Quick and flexible mechanisms to select and apply controls to your information systems
- High performance control analytics data model to help you collect the data needed to assess and monitor the controls

- Automatic application of hundreds of out-of-the-box analytics that will help you assess and monitor the controls
- Dynamic Control Architecture that lets you apply multiple control libraries and analytics besides NIST 800-53, even custom control

Explore the other RMF steps.

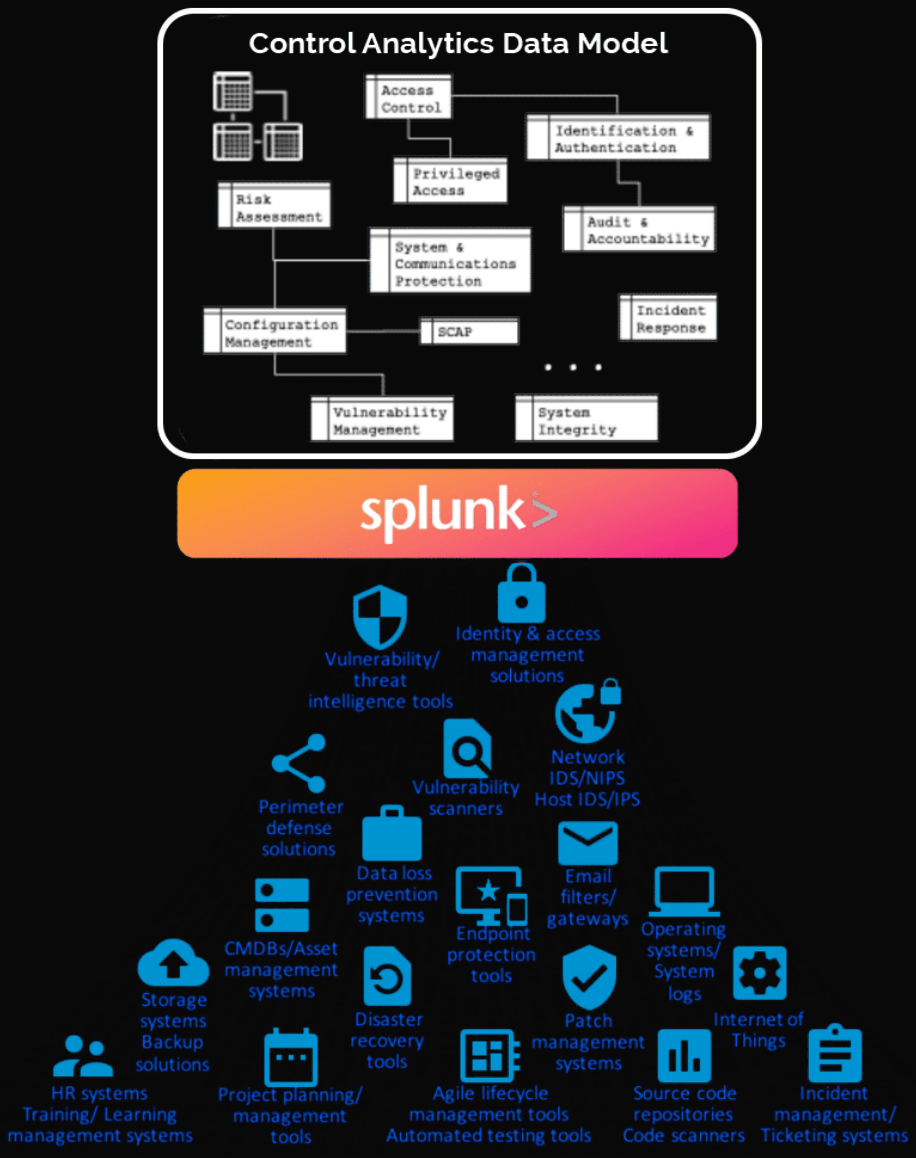
DATA-DRIVEN RMF SERIES – PART 3: IMPLEMENT

In part 3 of this series, we investigate meeting the Risk Management Framework's Implement step, using a data-driven approach. The main objective of the Implement step is to "implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation." Thus, to achieve this, you design and develop custom security functionality in your systems; integrate commercial and open source components and security tools; rely on common control providers for shared capabilities; and establish and implement security policies and practices to operate and maintain your systems and controls to provide the required levels of assurance.

With traditional GRC tools, the focus is only on documenting implementation statements in the Implement step. At Qmulos we realize that documenting is not all that should be done. We believe all data is security relevant. Thus, it should be collected to fuel the data-driven RMF process. And all of the activities, systems and tools in the Implement step generate a VERY rich stream of machine data.

The Implement Step using Q-Compliance

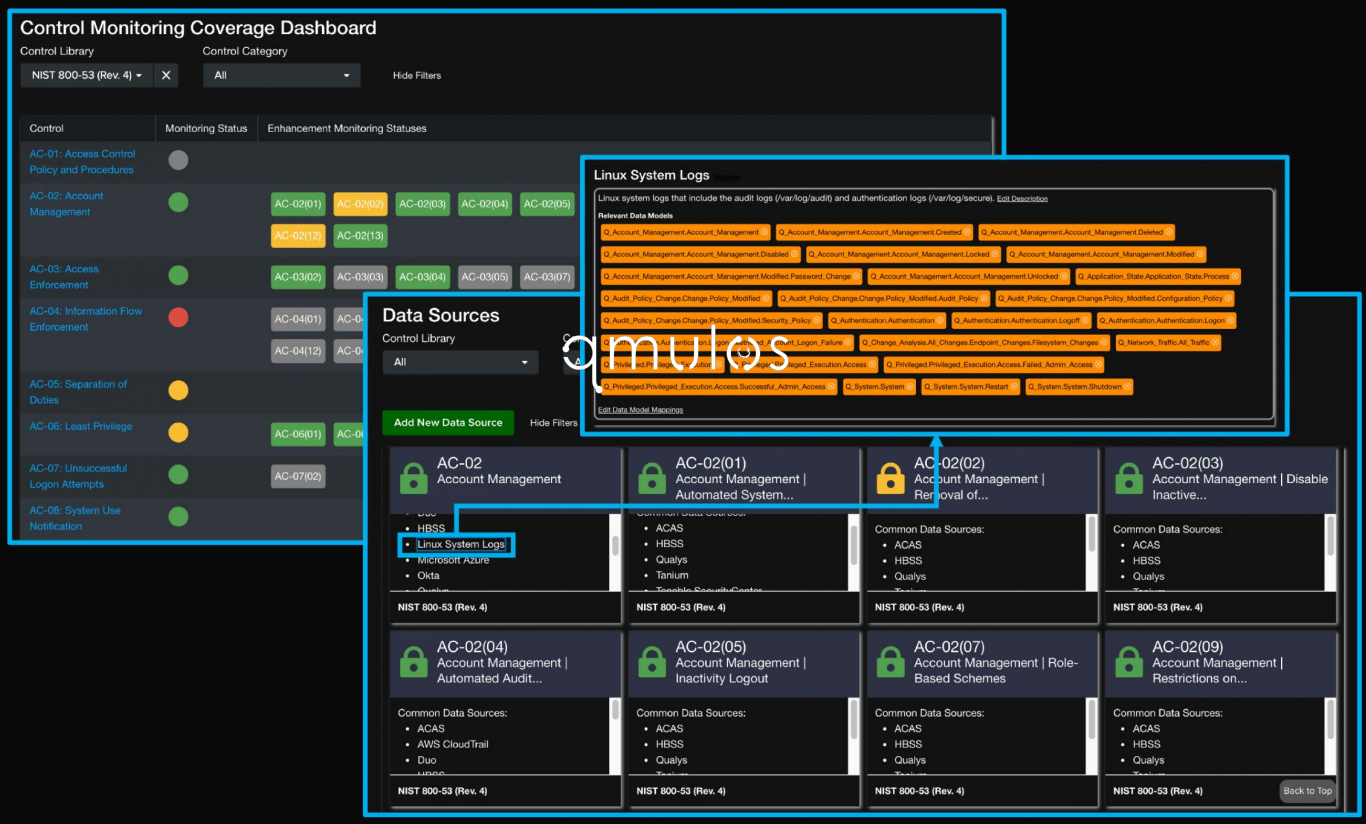
Our flagship software solution, Q-Compliance, is built on top of the Splunk's Data to Everything platform. This allows us to collect, store and analyze all of this data in real-time, as shown in Figure 1. Our solution integrates with ANY cyber security tool, application, device, and platform from on-premises or in the cloud. As a result, Q-Compliance's flexibility provides a revolutionary real-time single source of truth about an organization's actual security state.



The log, configuration, and event data that are collected are used to populate the Control Analytics Data Model in Q-Compliance that we described in Part 2 of this series. This data model normalizes differences in data formats from different data sources so that a common set of compliance analytics can be applied regardless of the underlying data source (e.g. a Cisco firewall vs Palo Alto Networks, Tenable vulnerability scanner vs. Rapid7, etc.). As you start ingesting data from your control implementations, the data automatically flows to execute the control analytics for the relevant subjects (organizations, systems, assets, users, etc.).

To assist with onboarding of the control implementation data, Q-Compliance provides capabilities such as the Control Monitoring Coverage dashboard, shown in Figure 2, to tell you which controls have relevant data to drive the analytics and where there are gaps. When you have gaps, the Data Sources dashboard, also

shown in Figure 2, can help you fill those gaps by listing common sources that can provide data for each control.



The benefits of using Q-Compliance for Step Three – Implement include:

- High performance, scalable platform to collect ANY data from ANY source on premises or in the cloud
- Thousands of out-of-the-box connectors/adaptors to integrate with various data sources
- High performance analytics data model that abstracts away tool-specific dependencies for interoperability. This enables you to easily change control implementations or tools
- Analytics that help you identify your gaps in control monitoring coverage and recommendations for potential tools and/or data sources

Explore the other RMF steps.

qmulos

DATA-DRIVEN RMF SERIES – PART 4: ASSESS

In part 4 of this series, we explore the Risk Management Framework Assess step, using a data-driven approach. The main objective of the Assess step is to "determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization."[RMF] To achieve this, you apply a combination of examine, interview and test methods throughout the system lifecycle.

The 3 steps to Assessing

Per NIST SP 800-53A: "The examine method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities). The interview method is the process of holding discussions with individuals or groups of individuals within an organization to once again, facilitate assessor understanding, achieve clarification, or obtain evidence. The test method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior". As you can imagine, each of these steps takes time, teamwork, and a variety of tools and resources.

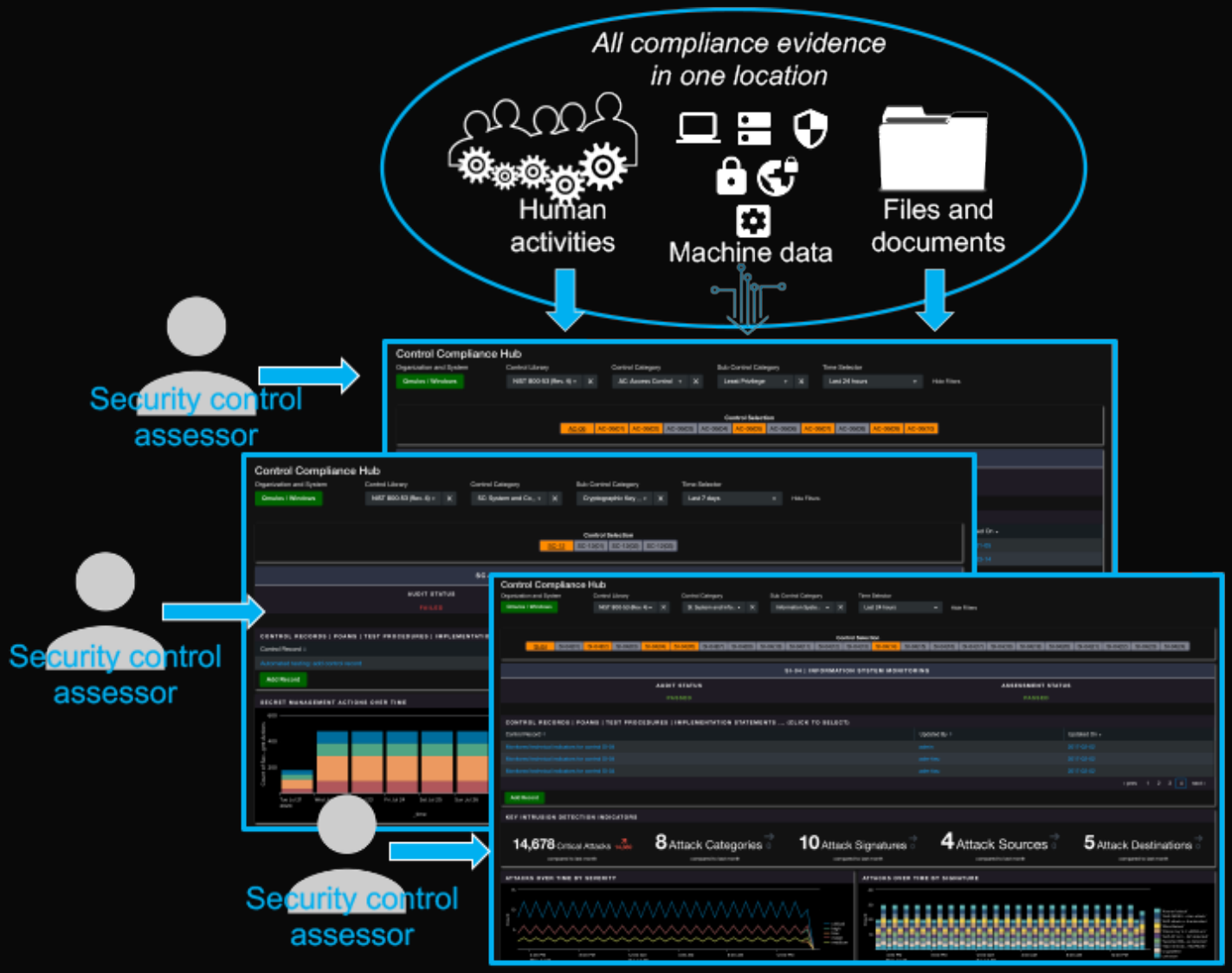
With traditional approaches, control assessors rely heavily on reviewing implementation statements and interviewing developers and other technical staff to determine if the controls are implemented and operating properly. Some manual interviews and examinations may still be required to provide a "white-box" approach to understanding and evaluating the control implementations.

The Data-driven approach using Q-Compliance

However, a data-driven approach reduces the reliance on such techniques which are labor intensive and don't provide timely results. Instead, a data-driven

approach automatically collects machine data and applies analytics to observe the behavior and outcomes of each control. Furthermore, the data-driven approach uses these analytics to assess if the controls are providing the required levels of protection. Q-Compliance supports this data-driven approach to control assessments with a high performance Control Analytics Data Model. Q-Compliance achieves this by collecting the machine data and displays it in hundreds of out-of-the-box control analytics (described in Part 2: Select and Part 3: Implement of this series) to help you monitor and assess that controls are implemented and operating properly.

To support control assessments, Q-Compliance provides a Control Compliance Hub dashboard, shown in Figure 1, below. The Control Compliance Hub is a "one-stop-shop" to collect and review all of the evidence required to assess controls. Traditionally, you would log into different hosts, access different tools, and/or send out multiple data calls and perform your assessments using potentially months-old data. We recognize that this is neither efficient nor does it add security value. Also, not all controls are technical in nature and thus may require manually collected evidence and assessment actions. However, the Control Compliance Hub supports multiple evidence types! These range from control records capturing human activities performed on the control, to machine data for technical evidence, to files and documents for policies, procedures, screenshots, etc.



Technically, how does Q-Compliance Assess accurately?

Of course, where Q-Compliance really shines, is its technical evidence indicators on the Control Compliance Hub. The Hub allows you to examine and/or test assessment objects (i.e., specifications, mechanisms, events, or activities). All of this is achieved using near real-time machine data that is centrally and automatically collected by the underlying Splunk instance on which Q-Compliance is deployed. The technical evidence indicators are built on top of the high-performance data model. The model computes using the control analytics and presents the data using rich and intuitive visualizations which are easily understood.

Behind the scenes, time and event driven alerts fire, detecting events/conditions, automatically passing or failing the control's assessment. The comprehensive set

of indicators and analytics within Q-Compliance range from monitoring account management, authentication, access control, privileged access; to asset management, configuration management, vulnerability scanning and patching; to endpoint protection, perimeter defense, incident response; etc. – covering all the technical security domains represented by the NIST 800-53 control families. For more unique requirements, you can easily customize the analytics and visualizations using your own custom-built ones or from any of the thousands of third-party apps available on Splunkbase, Splunk's marketplace for community-developed applications and technical add-ons.

The benefits of using Q-Compliance's data-driven approach for Step Four – Assess:

- Reduced reliance on manual methods and outdated data
- One-stop shop dashboard to collect and assess all evidence types for each control
- Hundreds of out-of-the box analytics and visualizations to help you assess controls with real-time machine data
- Robust alerting mechanism to automatically detect compliance issues in near real-time
- Easily customizable dashboards that allow you to configure custom or third-party control analytics and visualizations to support any unique requirements

Explore the other RMF steps.

qmulos

DATA-DRIVEN RMF SERIES – PART 5: AUTHORIZE

In part 5 of this series, we explore implementing the Authorize step of the Risk Management Framework using a data-driven approach. The main objective of the Authorize step is to "provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable."[RMF] We know, you might have to reread that. Summarily, the Authorize step determines if the results of the control assessment deem authorization of your system. Are the required levels of data confidentiality, integrity, and availability met? If so, are you ready to authorize the system?

The Data-Driven Approach

That might seem pretty simple but it's not; at least it isn't if you're not using a data-driven approach. The typical approach is for the authorizing official to review hundreds of pages of documentation. This documentation may include the system's security and privacy plans, control assessment reports, and plans of actions and milestones that address any deficiencies that were discovered. This is a laborious process where the authorizing official just has to trust that the information in the documents is accurate and correct and that the state of the system and the threats that it faces haven't changed since the documents were written (which can easily be from three to six months ago).

Conversely, using a data-driven approach means not having to rely on qualitative information written in documents, potentially several months old. The results of the control assessments automatically feed scoring algorithms that quantify the risk and compliance posture of your system. These scores are continuously updated based on continuous assessments of controls driven by machine data that is automatically collected and you can continuously update the authorization status of the system based on this. This is the true holy grail of ongoing assessment and

authorization.

Authorization using Q-Compliance

Q-Compliance supports this data-driven approach to authorizing systems with the System Authorization dashboard, shown in Figure 1, which serves as a "live authorization package" with all of the information in real-time that an authorizing official need to make an authorization decision. We make it easy with compliance scores and color-coded control charts, providing a summary view of the assessment results. Furthermore, clicking any of the color-coded control icons displays the Control Compliance Hub, specific to that control. Within the Control Compliance Hub are the details of the assessment along with supporting evidence. The scores and charts are updated in real-time as assessment statuses are captured or updated.

All of the Plans of Actions and Milestones (POA&Ms) for the system are also displayed on the System Authorization dashboard so that authorizing officials can see if there are any uncompleted or overdue POA&Ms as they make their decisions.

At the bottom of the System Authorization dashboard are documents for the authorizing official to review as we recognize that many organizations still require the documentation. Behind the scenes are automation actions to grant or deny system authorizations based on time-driven or event-driven conditions, e.g. automatically grant or deny an ATO when a system's compliance scores exceed or fall below a certain threshold or when a critical set of controls pass or fail their assessments.

The benefits of using Q-Compliance's to implement Step Five – Authorize:

- Reduce laborious hours of reviewing hundreds of pages of compliance documentation
- Ability to make authorization decisions based on quantitative risk and compliance scores and not just documents that are months old
- Easily drill into any control dashboard to see live supporting evidence for a real-time representation of the system's security state
- Dynamically update a system's authorization status as its compliance posture and acceptable level of risk changes

Explore the other RMF steps.

DATA-DRIVEN RMF SERIES – PART 6: MONITOR

In part 6 of this series, we explore the Monitor step of the RMF is implemented using a data-driven approach. The main objective of the Monitor step is to "maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions." It starts with monitoring for changes in the system, environment and adversaries. Then it is essentially a repeat of steps two, three, four and five; i.e. selecting additional controls to address changes in the environment or the adversaries' tactics, techniques and procedures; implementing those new controls and/or updating the implementation of existing controls; assessing the new controls or re-assessing updated controls; and finally revisiting the authorization decision for the system based on all the changes. The Joint Task Force that created the RMF realized that cyber defense is never ending and added this step to make the process continuous and on-going.

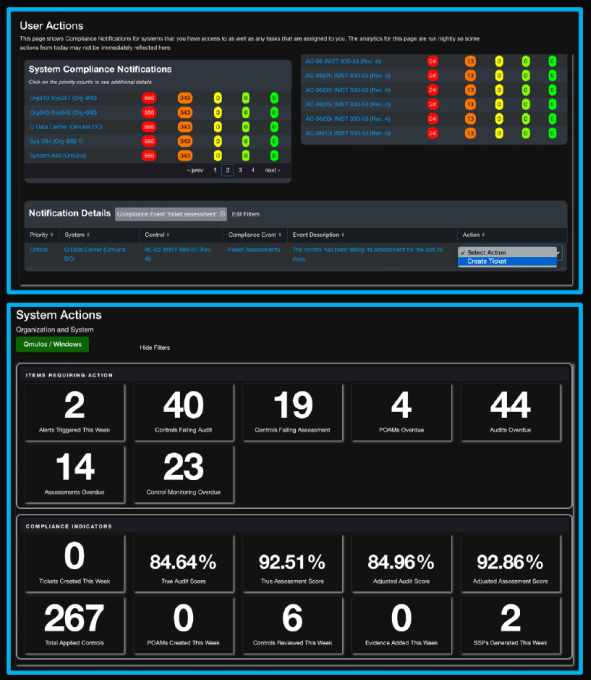
If you are implementing Step 6 – Monitor without a data-driven approach, forget it. You might as well skip the step and go back to the three-year certification and accreditation cycle. Without a data-driven approach you will not have timely visibility into 1) changes in the threat landscape; 2) configuration drift that is occurring in your systems; 3) new vulnerabilities that are discovered and exploits that are using them; 4) user activities that are putting your systems at risk. In essence, you won't have timely visibility into any of the events and activities that truly necessitate continuous monitoring.

Q-Compliance and its capabilities for Step 6

Because Q-Compliance supports all other steps of the RMF with a data-driven approach, it automatically supports Step 6. For example, the same analytics and visualizations that enable a data-driven approach to Step 4 – Assess also allow you to continuously monitor for changes that may impact the effectiveness of those controls. In addition to these underlying capabilities, Q-Compliance has purpose-built features specifically targeted to enable the Monitor step. Below, the table lists the key data and automation capabilities required to support continuous monitoring from NIST SP 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" and describes how Q-Compliance supports each of them.

ISCM Capability from NIST SP 800-137	How It's Supported in Q-Compliance
Pull information from a variety of sources	Integrates with any cyber security tool, application, device, and platform. From on-premises or in the cloud, it provides a real-time single source of truth about an organization's actual security state
Use open specifications such as the Security Content Automation Protocol (SCAP)	Qmulos provides industry's only SCAP input for Splunk to ingest the results of security scanners, vulnerability scanners, configuration management tools and other SCAP-compliant tools to populate the control analytics in Q-Compliance.
Offer interoperability with other products	Q-Compliance leverages thousands of technical add-ons in

such as help desk, inventory management, configuration management, and incident response solutions	Splunkbase as well as custom add-ons built by Qmulos. Additionally, we integrate and interoperate with all of the leading inventory management, configuration management, help desk and incident response tools.
Support compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines	Supports all of the applicable security and compliance standards from NIST, Department of Defense, Intelligence Community, and civilian agencies. These include but are not limited to: NIST SP 800-53 (rev. 4 and rev. 5), NIST SP 800-37, NIST SP 800-137, CNSS 1253, FedRAMP, NIST CSF, DISA STIGs, etc.
Provide reporting with the ability to tailor output and drill down from high-level, aggregate metrics to system-level metrics	Q-Compliance has dashboards and reports targeting all users in the organization at all levels of detail. For example, risk and compliance metrics across the entire enterprise to specific departments and systems with the ability to drill down into individual assets and events.
Allow for data consolidation into Security Information and Event Management (SIEM) tools and dashboard products	Q-Compliance is built on top of Splunk, the industry's leading SIEM platform. Any data in Q-Compliance is consolidated and correlated with other data in the platform.



Q-Compliance Dashboards

All of these capabilities in Q-Compliance are brought together to enable organizations to implement both time-driven and event-driven mechanisms to continuously monitor the risk and compliance posture of your systems and adjust the systems' security authorizations accordingly. You can set up schedule-based reminders for when certain controls need to be reviewed or monitored based on your organization's or system's ISCM strategy. You can set up automated alerts to detect events that affect the compliance or security posture of

your system and the specific controls that are impacted. These alerts can even trigger workflows using Splunk's orchestration capabilities to automatically remediate the findings (e.g. apply a patch, change a configuration setting, quarantine a device, etc.); fail a control; create a Plan of Action & Milestone; or revoke the ATO of a system. As these things are occurring in the background, you will be notified through rich and intuitive dashboards, as shown in Figure 1. Furthermore, the dashboards enable you to prioritize your day-to-day security and compliance activities to maintain an acceptable level of risk for your organizations and systems.

Within Q-Compliance, the available dashboards display the latest representation of the system's state, to include object and event-level details. Firstly, the System Continuous Monitoring dashboard provides a one-stop-shop for all users (that are authorized to see each system) to monitor all the controls that have been designated for continuous monitoring using real-time events in Splunk that are relevant to each control and system. Secondly, the System Actions dashboard provide system owners, Information System Security Officers (ISSOs), and other users with system-level responsibilities with a key summary of the items that require action and up-to-the-minute compliance indicators. Thirdly, the User Actions dashboard provide a more user-focused view of the information based on each user's area of responsibility. These dashboards enable users to take actions to maintain and/or improve the security and compliance posture of their systems.

The benefits of using Q-Compliance for Step 6 – Monitor include:

- Timely visibility into changes in the system, environment and adversaries that impact the risk posture of your systems
- Continuously monitor ALL technical controls, not just the typical small subset of vulnerability and configuration management controls like other tools
- Automated actions triggered by findings from continuous monitoring. E.G. fail a control, create a POAM, revoke a system ATO, apply a patch, change a configuration setting, etc.
- Seamless integration with the rest of the RMF steps. I.E. any actions performed in steps one through five are automatically reflected in step six and vice-versa. This truly enables the continuous cycle envisioned by the creators of RMF.

Q-Compliance's support for a data-driven approach for steps one through five of the RMF makes it a breeze for you to implement Step 6. Additionally, why go through the motions with a manual approach and stale data when it provides little to no security value?

Explore the other RMF steps.