Whitepaper

Meeting NIST Risk Management Framework Requirements

Centrally Manage Governance, Risk and Compliance across Data Centers and Cloud

The world of information security, risk management, and regulatory compliance continues to grow more complex, virtualized, and distributed. Agencies must continuously monitor an increasingly diverse and complex landscape of systems to address information and network security, operational risk, and regulatory frameworks to meet auditing and compliance requirements. Additionally, agencies must proactively protect their systems and customers from evolving cyber threats. With new attack vectors introduced into the Internet daily, it only takes one breach to adversely affect every part of an agency.

Governance, risk and compliance (GRC) is an increasingly recognized term that refers to a new strategy for managing overall governance, enterprise risk management and compliance with regulations. GRC is a structured approach that aligns IT with business objectives while effectively managing risk and meeting compliance requirements. Many agencies have multiple groups responsible for the functions and processes involved in GRC that operate in silos that may not share information concerning numerous frameworks and systems. The result is not only inefficiency through redundancy and possible gaps in coverage, but also a failure to gain a clear full view of risk.

Virtustream Viewtrust risk management and continuous compliance monitoring software provides a near real-time view of compliance posture, alerting when critical configuration standard guideline parameters have fallen outside predefined threshold values. Through a holistic view of infrastructure risks, whether on-premises or in clouds, Viewtrust enables agencies to remediate systems in a proactive, efficient, repeatable and consistent manner across the entire business regardless of location.

In this paper, we will review each aspect of continuous monitoring and highlight Viewtrust's automation tools and techniques within the context of the Risk Management Framework.

What Is the Risk Management Framework?

The Risk Management Framework (RMF) is a unified information security framework for the U.S. Federal Government that replaces the legacy Certification and Accreditation (C&A) processes applied to information systems. The RMF is a critical component of an organization's information security program used in the overall management of risk. Defined by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 1, the RMF provides guidelines for applying the framework to federal information systems. The framework includes such items as conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization and security control monitoring. The guidelines also allow the elimination of authorization termination dates if a robust continuous monitoring program such as Viewtrust is in place. To qualify, the continuous monitoring program must provide the authorizing official with information for conducting ongoing risk determination and risk acceptance activities regarding the security state of the information system and the ongoing effectiveness of security controls. Agencies must still maintain formal authorizations and acceptance of risk but may leverage results of continuous monitoring assessments to support the ongoing Authorization to Operate (ATO).

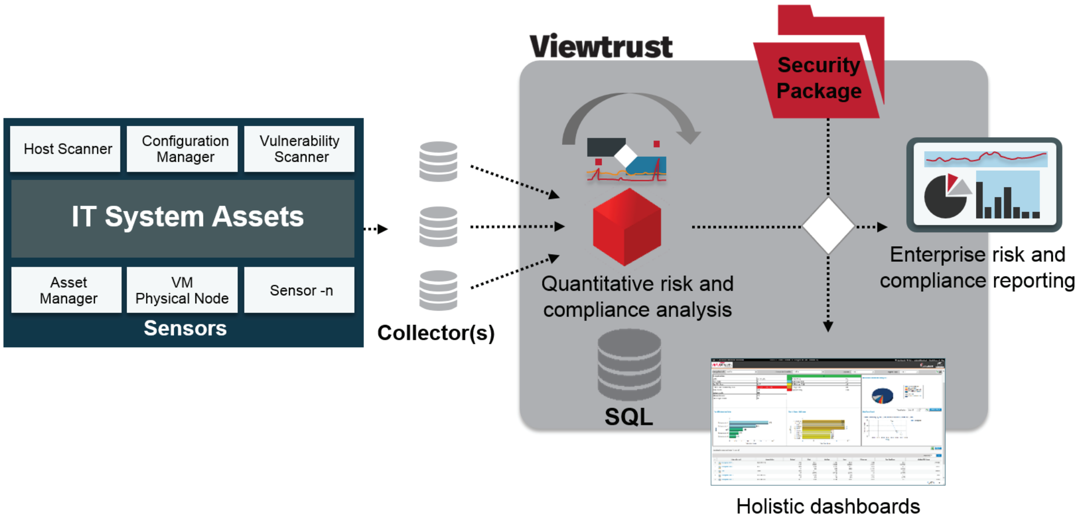


Figure 1: Viewtrust Operational Deployment Model

Continuous Monitoring

NIST SP 800-137 defines continuous monitoring as ongoing awareness of information security, vulnerabilities and threats to facilitate risk-based decision making. Continuous monitoring involves the ongoing assessment and analysis of the effectiveness of all security controls and provides ongoing reporting on the security posture of information systems to support risk management decisions to help maintain risk tolerance. It also includes policy monitoring and documentation updates for annual or significant change related re-certifications.

Continuous monitoring of a system requires compliance with three essential requirements:

- Change and configuration management of assets
- Security control monitoring using automated tools
- Documentation updates and reporting

Change and Configuration Management (CM) of Assets

NIST SP 800-128 provides guidelines for managing and administering the security of federal information systems and associated environments of operations. CM concepts and principals described in NIST SP 800-128 support NIST SP 800-53 by detailing how the CM function facilitates asset management, incident management, help desk and disaster recovery functions, and aids in software development testing and release management. CM enables greater automation of processes and supports compliance with policies and preparation of audit. CM comprises a collection of activities that begin with the establishment of the baseline configuration where each item tracked is a configuration item (CI). A CI provides information on asset hardware, operating system and applications installed including version numbers and patches. Each baseline configuration must be formally reviewed and agreed upon and can be altered only through a change control process. A configuration management plan (CMP) is created and describes roles, responsibilities, policies and procedures that govern the change in the configuration of assets and systems.

The CMP includes information on each CI and defines the activities and roles to manage and control change. CM controls for the security of information systems involve a set of activities grouped into four phases: planning, implementing, maintaining and monitoring. Additional Information Assurance (IA) control families include all the technical controls such as the access control, audit and accounting, identification and authentication, system and communication protection and operational control.

Security Control Monitoring Using Automated Tools

Security control monitoring helps determine if the controls implemented or inherited by the system continue to be effective over time as the system changes. Through automated tools, continuous security control monitoring involves the monitoring of each control with varying frequencies based on:

- Control volatility; the more volatile controls must be monitored more frequently
- Organization and system risk tolerance
- Threat information that might affect the system

It is difficult to obtain manually required details and frequency given the increasing size, scope, and

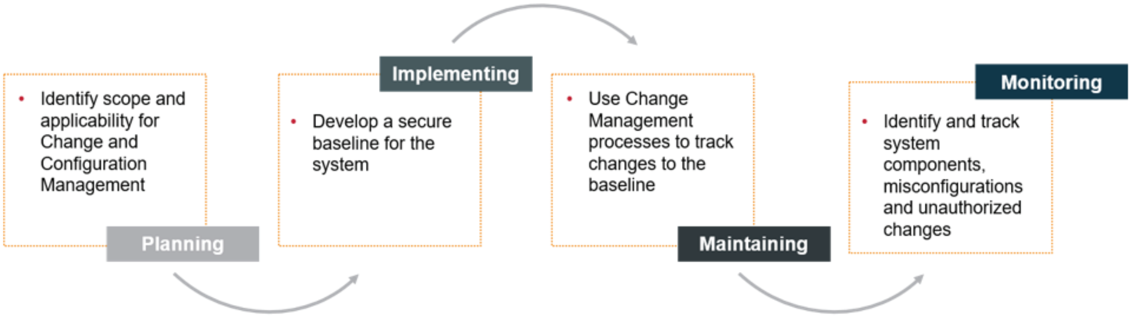

Identify scope and applicability for Change and Configuration Management
Planning
Implementing
Develop a secure baseline for the system
Use Change Management processes to track changes to the baseline
Maintaining
Monitoring
Identify and track system components, misconfigurations and unauthorized changes

Figure 2: Change and Configuration Management Phases

complexity of today's systems. Automated monitoring and reporting tools are needed to provide the situational awareness data necessary to support risk-based decisions, on-going authorization evaluation and configuration management. Some technical and operational controls lend themselves to automation more easily than others. These controls can be evaluated and monitored using vulnerability assessment tools or event management and alerting systems that provide situational data based on logs and Simple Network Management Protocol (SNMP) alerts.

A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic operating environment that faces changing threats, vulnerabilities, technologies, and missions. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness about the security state of the information system. Continuous monitoring helps provide ongoing updates to the security plan, the security assessment report, and the plan of action and milestones (POA&M) - the three principal documents that make up a security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system.

Vulnerability and Configuration Assessment Tools

Vulnerability and configuration assessment tools help identify the impact of asset changes and the vulnerabilities introduced and also provide an initial severity assessment, implications and possible solutions for mitigation. Compliance with NIST Security Content Automation Protocol (SCAP) specifications provides a standard format for checking security configuration settings with automated tools. SCAP compliant tools also provide information on the controls being affected based on open vulnerability assessment language (OVAL) and extensible configuration checklist description format (XCCDF) benchmark tests with results provided in assessment summary result (ASR) and asset reporting format (ARF) standard.

Situational Awareness with Event Management

Enterprise event management and compliance reporting capabilities are imperative to assess the ongoing security posture of a system and its assets from the vast amount of disparate data collected from many systems. The ability to view the impact of the events on a system and corresponding IA controls is critical to providing a coordinated response and maintaining the confidentiality, integrity and availability of the information system. Situational awareness data from an asset must be mapped to the appropriate system and IA control that may have been affected. This information is used by the system owner and the designated approving authority on evaluating the risk to the information system, and the remediation action may then be documented as a task or POA&M item.

Documentation Updates and Reporting

Critical documents including the system security plan (SSP), security assessment report (SAR), security test and evaluation (ST&E) report and the POA&M must be updated and kept current as per the continuous monitoring process. These essential documents and supporting artifacts are required for any authorizing official to evaluate risk and grant continued authorization. POA&M reports are especially critical, as they must be provided to the Office of Management and Budget (OMB) upon request or at least quarterly.

SSP documents must reflect changes in the system and its assets based on the change and configuration management process and any updates to the control implementation, while the SAR and ST&E documents must reflect the testing and validation of the controls to identify any risks introduced due to these changes. Any newly identified threat or an impact on the existing POA&M item must be reflected and reported to the authorizing official and OMB.

Significant time and effort are involved in keeping these detailed documents updated to accurately reflect the current system state. Just as asset information becomes potentially stale within twenty-four hours of documentation, SSP and SAR documents can also become rapidly outdated. Automation tools are the best way to keep this large volume of documents updated on an on-going basis.

Viewtrust Enables Risk Management and Continuous Monitoring

Viewtrust risk management and continuous compliance monitoring software provides agencies with a near real-time view of their entire compliance posture, showing when critical configuration standard guideline parameters have fallen outside predefined threshold values.

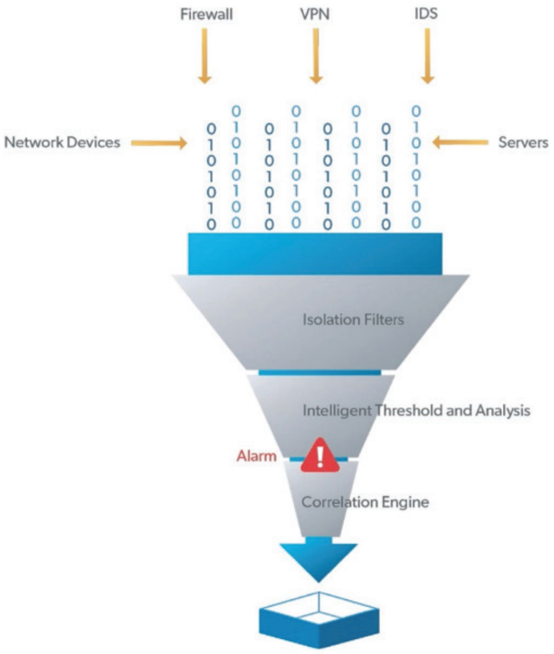


Figure 3: Viewtrust can ingest, collect, store and process sensor data from a variety of sources

Viewtrust provides a scalable data ingest, collection, storage and processing platform that supports critical Federal enterprise environments, monitoring millions of devices and processing a multitude of data input types from thousands of sensors. Viewtrust delivers accurate and timely insights into operational risks by providing a 360° view of assets, vulnerabilities and compliance with approved configuration baselines including automated alerts when critical threshold values have been exceeded or sensitive configuration parameters have been changed.

Through continuous monitoring of the IT landscape, Viewtrust identifies potential risks to enable proactive remediation and delivers the reporting and associated artifacts necessary to address regulatory oversight. In addition, Viewtrust meets many compliance requirements such as FISMA, SOX, PCI DSS, HIPAA/HITECH, ISO 27001, FedRAMP and more, besides providing for custom user-defined compliance frameworks.

Viewtrust Monitoring Data Lifecycle

Viewtrust uses certified components and interchangeable plug-in modules with support for many storage options. The platform ingests data from a wide range of proprietary and SCAP-compliant sensor inputs. The Viewtrust monitoring data lifecycle operates as follows:

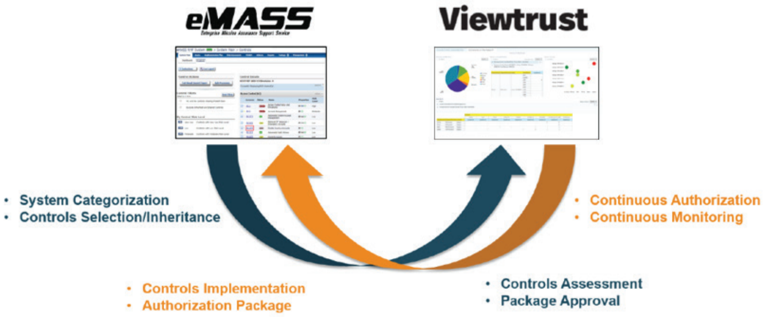
- **Data Ingest Layer**: Data is gathered from the system through pull and push interaction across the device spectrum.
- **Data Adaptation/Transfer Layer:** Viewtrust processes incoming data and uploads the information to the relational database management system (RDBMS). Data can also be forwarded to long-term storage.
- **Data Staging Layer:** In addition to staging data, this layer also serves as the storage area used for data processing during the extract, transform and load (ETL) process which obtains and computes the data to organize into a format that can be easily matched to the application. Deployed on a RDBMS, data repositories accommodate diverse data sizes and frequency. The environment can be established based on any standard RDBMS product suite such as Oracle and Microsoft SQL Server.
- **Business Logic Layer:** Risk-scoring algorithms compute risk based on asset, system, geo-location and mission criticality, ensuring that regulatory compliance control requirements are met through automated risk mitigation workflows. Data is processed using various compliance and risk scoring models and associated algorithms based on organizational business objectives.
- **Presentation and Analytics Layer:** Data is readied for data analytics and display through the Viewtrust dashboards, delivering the reporting and associated artifacts that address regulatory oversight requirements.

Viewtrust Component for Federal Information Security Management Act (FISMA) Assessment and Authorization (A&A) Documentation

Viewtrust transforms the compliance effort into a paperless process that centralizes and expedites the development of A&A documentation packages and improves on the traditional, manual process which can be prone to high error rates and inherent operational delays. Viewtrust's integrated document management system allows users to work independently, yet provides the ability to collaborate simultaneously on a single document when necessary and eliminates the need for document versioning and check-out/check-in. Wizards guide the user through the process reducing the overall cost of developing and maintaining compliance documentation and maintaining ATO.

Integration with DISA eMASS

Viewtrust integrates directly with the U.S. Defense Information Systems Agency (DISA) Enterprise Mission Assurance Support Service (eMASS) application, enabling IA teams to automatically publish compliance statements, assessments, artifacts and POA&M into eMASS. Viewtrust automation significantly reduces the time spent completing steps three and four of the RMF. [1,2]



Summary

Many federal agencies find that conducting continuous risk and compliance monitoring can be a struggle given today's complexities in information security, risk management and regulatory compliance. Virtustream Viewtrust provides a comprehensive yet cost-effective solution for continuous monitoring of risk and compliance, providing a near real-time view of the entire compliance posture and alerts when critical configuration standard guideline parameters have fallen outside predefined threshold values. Viewtrust enables agencies to remediate systems in a proactive, efficient, repeatable and consistent manner across the entire business regardless of location. It provides lifecycle compliance monitoring by continuously monitoring the IT landscape, identifying potential risks to enable proactive remediation, and delivers the reporting and associated artifacts necessary to address regulatory oversight.

Viewtrust meets many compliance requirements such as FISMA, SOX, PCI DSS, HIPAA/HITECH, ISO 27001, FedRAMP and more, besides providing for custom user-defined compliance frameworks. It automates compliance management by transforming the compliance effort into a paperless process that centralizes and expedites the development of A&A documentation packages and enables IA teams to automatically publish compliance statements, assessments, artifacts and POA&M into eMASS.

Contact

For more information, please contact us at info@virtustream.com or visit us at www.virtustream.com.

About Virtustream

Virtustream, a Dell Technologies business, is the enterprise-class cloud service and software provider trusted by enterprises worldwide to migrate and run their mission-critical applications in the cloud. For enterprises, service providers and government agencies, Virtustream's xStream management platform and Infrastructure-as-a-Service (IaaS) meets the security, compliance, performance, efficiency and consumption-based billing requirements of complex production applications in the cloud – whether private, public or hybrid.

[1] RMF Step 3 is specified as Implement Security Controls, where the security controls specified in the security plan are implemented, and description of how the controls are deployed within the system and environment of operation are documented.

[2] RMF Step 4 is specified as Assess Security Controls, where the security controls are assessed using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome concerning meeting the security requirements for the system.