CMS
ISSO Journal

...by and for CMS Cybersecurity Professionals

January-March 2024

Issue 27

CMS ISSO JOURNAL

January-March 2024 Issue 27

Highlights

Welcome to the first edition of the *CMS ISSO Journal* for 2024! This edition has several interesting articles and features, many of them of particular and immediate interest to ISSOs and their staffs.

- Want to know how improving your communication skills can improve you as an ISSO? Find out more in **Unlocking Career Success for ISSO: The importance of Communication Skills for Information System Security Officers.**
- Curious about the importance of data minimization? **Data Minimization Strategy: There's a lot to unpack** has the details.
- Phishing emails are more prominent than ever before. **Enhancing Email Vigilance at CMS: Emphasizing the Importance of Reporting Phishing** reminds you the importance of reporting suspicious emails!
- These are just a few of the many important and interesting things found in this edition. Happy reading!

The CMS ISSO Editorial Staff

The *CMS ISSO Journal* seeks to help enhance the proficiency and capabilities of the CMS Cybersecurity Community.

Published Quarterly, the *Journal* shares professional experiences and expertise of the CMS ISSO community, cybersecurity contractors, and interested CMS professionals.

The *CMS ISSO Journal* is freely distributable without restriction within and outside of CMS. You can find the *ISSO Journal* in multiple locations, including in Confluence at "ISPG ISSO Workforce Resilience Program" and in CFACTS. If you need a copy, send a request to isso@cms.hhs.gov

Articles published in the CMS ISSO Journal are eligible for continuing education units. If you have something that you want to share, let us know by sending an email to isso@cms.hhs.gov.

How are we doing? Let us know by sharing your thoughts on this or other issues in a brief survey at https://cmsgov.typeform.com/to/vPFO8LfU

Read the Journal online at ISPG ISSO Workforce Resilience Program (Confluence).

Journal Contents

Unlocking Career Success for ISSO: The Importance of Communication Skills for Information System Security Officers

Dr. Mary Margaret Chantre

The importance of communication skills for ISSOs (Information System Security Officers) cannot be underestimated. This article shares why communication skills in cybersecurity are the secret weapon for career advancement for ISSOs and other professionals in cybersecurity.

The roles and responsibilities of ISSOs have risen tremendously as data breaches continue to escalate at an alarming rate. The ISSO role has become increasingly crucial for organizations facing increasing cyber threats and to protect the confidentiality, integrity, and availability of their valuable and sensitive information assets. However, an ISSO's effectiveness hinges on clear and proactive communication. All ISSOs may not successfully identify, assess, or report data breaches and cyber-attacks to their managers, CISOs, or C-Suite and the board of directors (in the case of small and mid-sized organizations). Effective communication involves speaking to them in a language they can relate to. Further, it can also be your step to a more advanced role in your cybersecurity career ladder.

Why Communication Skills Matter So Much for ISSOs

ISSOs need to translate challenging technical concepts into comprehensible language for many audiences (from senior management to non-technical staff) so everyone can grasp the implications of security decisions, leading to better team collaboration. For the communication to be effective, they use jargon cautiously and explain matters in technical terms only when necessary. ISSOs can also help transform security awareness trainings into an engaging and impactful experience. Crafting compelling training materials and presentations that resonate with the audience can drive behavior change and promote a culture of security.

Most importantly, ISSOs generally communicate with almost all departments within their organization. Hence, they must collaborate and communicate effectively with IT and development teams, third-party consulting firms, and external vendors. Strong communication skills enable them to navigate negotiations that save CISO's already limited budget and help organizations get the best of the products and services that can help them strengthen their cybersecurity posture. They also help build strong working relationships.

Excellent communication skills also help ISSOs use well-balanced business language for more straightforward communication with high-level non-experts and presenting ideas to leadership and stakeholders.

Communication Skills for Job Acquisition and Career Advancement

Smart communication skills will not only help you perform better in your job as an ISSO but also act as a powerhouse for career advancement if utilized appropriately. Here's how.

- **Crafting a Compelling Resume and Cover Letter:** Communication shines through in written materials like resumes and cover letters. A professional yet engaging tone will reflect your strengths and passion for the field.

- **Acing the Job Interview via Effective Communication:** There are two parts to this process – paying close attention to the interviewer's questions and projecting confidence through positive body language and eye contact. You can show you're an expert through both.

- **Networking with Industry Professionals:** Engaging in meaningful conversations with genuine interest and asking thoughtful questions to peers can take you a long way. One must maintain a polished LinkedIn profile that showcases one's skills and accomplishments. Hone your 30-second pitch and connect with industry professionals effectively.

- **Public Speaking and Presentation Skills:** It doesn't matter if you're presenting to colleagues, teams, senior management, or at a conference – working on your public speaking and presentation skills will help deliver your message effectively.

- **Social Media Proficiency for Professional Branding:** Maintain a professional image on social media and avoid anything that can have a negative impact on yourself. Good practice is sharing industry news, insightful articles, and personal achievements on social media.

Communication for Discharging ISSO Roles and Responsibilities Efficiently

Beyond technical expertise, effective communication is an essential weapon in your arsenal as an ISSO while exchanging ideas with higher-ups and those in managerial positions for professional matters such as described below.

- **Writing Plans of Action and Milestones (POA&Ms):** ISSOs must craft comprehensible documents to communicate security initiatives effectively for technical and non-technical audiences and tailor them to their needs. IT professionals, security analysts, developers, and system administrators may require detailed technical information, including specific tools, configurations, and procedures. However, the management may only need a high-level overview of the business impact, risks addressed, and expected outcomes.

- **Requesting Authorization to Operate (ATO) Extensions:** Securing ATO extensions requires convincing stakeholders of the continued need for specific controls. For example, if control(s) require an extension, then presenting the impact of non-extension to the management is an art that requires crafting a compelling narrative focused on business impact.

- **Presenting Security Findings and Recommendations:** Security reports often fall prey to technical overload, so you'll need good communication skills to translate complex findings into compelling narratives that grab attention.

- **Negotiating with Vendors for Security Tools and Services:** Negotiating vendor contracts necessitates clear and persuasive communication, another area where ISSOs must demonstrate expertise to secure value for the organization.

- **Writing Precise and Persuasive Reports:** Information security reports (security incident report, vulnerability assessment report, compliance report) shouldn't just inform - they should propel action. Using concise language, highlighting key findings, and proposing actionable recommendations are a few things that can spark necessary change.

- **Influencing Organizational Security Culture:** Security teams struggle to communicate policies and risks, which hinders awareness and effective compliance. Dedicated communication creates a shared understanding of security risks and motivates employees to play their part productively.

- **Collaboration with Global Teams:** Effective communication is needed to build rapport with global teams so there's a clear information flow, alignment on security practices, and a unified approach to cybersecurity.

Applying Communication Skills in the Workplace

Have you ever heard of the Swiss Army knife? It's a multi-tooled pocketknife. Communication skills are similar to the Swiss Army knife in the workplace, unlocking opportunities and fostering success in various daily tasks and career advancements requiring varied skills. For example, ISSOs can keep email communication concise and actionable and get straight to the point so the message is understood and acted upon promptly. On the other hand, in the event of an incident, ISSOs should try to provide clear, informative, and timely responses to security inquiries to business stakeholders, regulators, customers, and employees. It'll help you foster a culture of trust and security awareness. ISSOs should practice listening and at the same time, contribute actively to the team or client meetings when needed. Inspiring and motivating others requires strong communication. You can create a productive and positive team by delivering clear instructions, providing constructive feedback, and fostering open dialogue.

Final Words

Mastering communication skills can unlock opportunities to the next level in ISSO's (Information System Security Officers) cybersecurity career. However, effective communication involves a continuous learning process. It's not something you merely acquire, like technical skills. It is an essential and highly sought-after quality that can aid you in translating complex technical information into understandable insights, strengthen relationships with stakeholders and the C-suite, and help you advance in the field of information security significantly.

Dr. Mary Margaret Chantre oversees the fulfilment of larger organizational goals. She pays detailed attention to program strategy, project delegation, and program implementation.

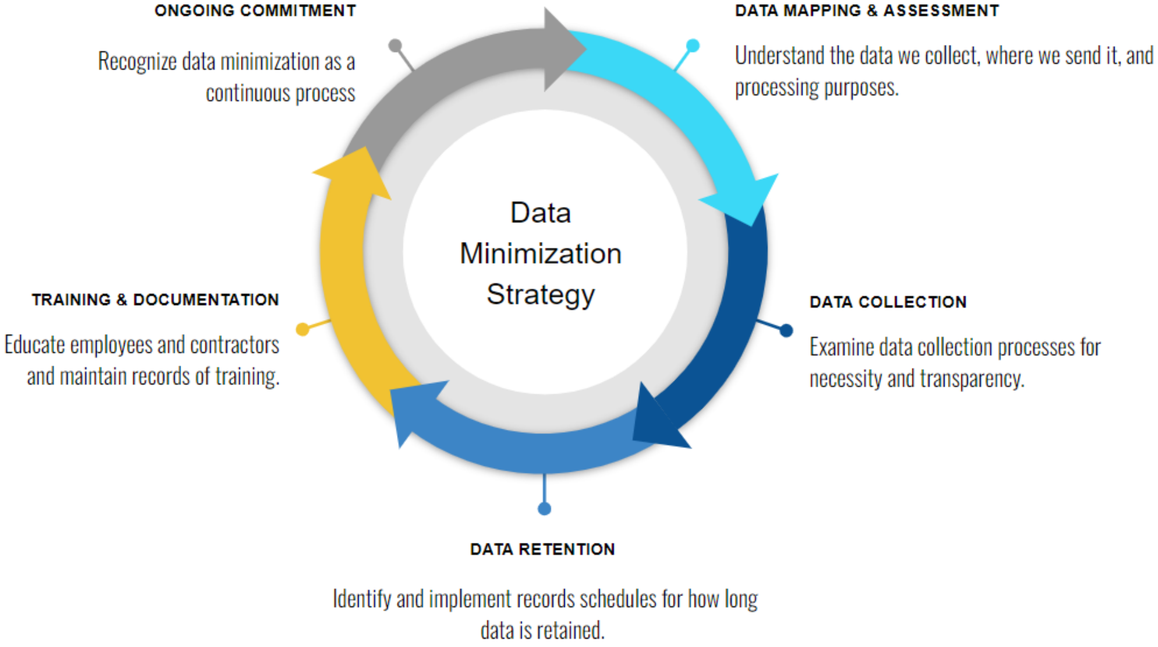
Data Minimization Strategy: There’s a lot to unpack.

Casey Douglas - CCSQ ISSO

One of the basic privacy principles is *Minimization* and is backed by many laws, policies, standards, and guidance. Minimization involves limiting personally identifiable information (PII) collection to only what is required to fulfill a specific business need or purpose. *Minimum Necessary* is a standard under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule which operates the same way but focuses on protected health information (PHI), a subset of PII.

Data minimization effectively works as a safeguard, minimizing what could be exploited because of either malicious intent or mishandling. Reducing the amount of unnecessary data minimizes the risk of data breaches and unauthorized access.

In CCSQ, we created a strategy that brings together existing CMS activities and processes to build a greater understanding of data minimization.



ONGOING COMMITMENT

Recognize data minimization as a continuous process

DATA MAPPING & ASSESSMENT

Understand the data we collect, where we send it, and processing purposes.

DATA COLLECTION

Examine data collection processes for necessity and transparency.

DATA RETENTION

Identify and implement records schedules for how long data is retained.

TRAINING & DOCUMENTATION

Educate employees and contractors and maintain records of training.

Data Mapping & Assessment:

Before we dive into data minimization, we need a solid grasp of our existing data. Sure, starting with PII, we can do a review of what's listed in the system's Privacy Impact Assessment (PIA). However, some systems send data between systems and with external parties. These external parties should be limited to data by a business need or purpose even if the system that is sending data contains more data than the receiving system or external party needs.

OIT's Enterprise Architecture Data Group (EADG) sends out an annual CMS System Census Survey. The information that's reported in the Data Exchange tab is what we're using to start mapping the data flows. Information that's included in this tab of the survey is used to show the relationship between FISMA systems and with external stakeholders and organizations.

The assessment starts with an in-depth review of the Data Exchange survey responses with the Survey Point of Contact (POC) to validate and gather more information on what was reported. There are many fields including the Exchange Partner/Stakeholder Name and questions such as "Contains PII?" and "Contains PHI?". To go a step further, beyond the "Yes" or "No" response, we'll find out exactly what data fields are included in each exchange and the purpose of sending or receiving that data.

Data Collection:

If the PII/PHI does not serve a business purpose, then we may not collect that PII/PHI. If the collection of PII/PHI does serve a business purpose and fits within applicable laws, then it should be collected, stored, shared, and retained within regulations. It sounds easy, but it's not.

PII that's collected or maintained at CMS must coordinate with a SORN's written description. CMS cannot collect data that is not described in the "Categories of Records" section of a SORN or disclose PII except if its subject to one of exceptions in the Privacy Act, or as written as a "Routine Use". For PHI, the HIPAA Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose within HIPAA's permitted uses and disclosures (uses and disclosures that are authorized by the individual are exempt).

We perform PTAs to determine if a SORN and PIA are needed. This is when we'll ask questions about data collection such as, "Do we really need this?" "What's the purpose?" "Does it fit within applicable laws?" "Is there a way to <insert purpose here> without this data?". We'll also consult with the CMS Privacy team, as needed.

Data Retention:

We're required to create and manage, safeguard, and retain or dispose of records according to an approved records schedule. CMS' record schedules authorize destruction of temporary records when their retention period expires provided no specific preservation obligations apply (e.g., litigation hold). OSORA's Records and Information Management (RIM) Team manages the Cross-Reference Tool (CRT) that is used as a lifecycle management tool for data stored in systems. The CRT tracks each system's status and notifies the Business Owner and Records Liaisons Officer (RLO) once a year for records that are up for disposition.

Records retention schedules are more than a line item in the PIA. Some systems are in production long enough to meet the retention period in their identified records schedule. With the RLO, we'll review each system's identified CMS records schedule. Then, we'll work with the system teams to find out whether the data is within the retention period and what we must do to disposition the data, if needed.

Training & Documentation:

CMS provides annual, mandatory trainings on Records Management and Security and Privacy Awareness to all CMS employees and contractors to make sure that they're aware of their responsibilities to maintain and safeguard data.

CCSQ's Human-Centered Design (HCD) Center of Excellence (CoE) is helping us gather insights into what CMS/CCSQ employees and contractors know about data minimization and how to apply it. This information will help us to create and offer targeted training that's used for onboarding and refresher trainings.

Ongoing Commitment:

Business Owners, CO/CORs, and System Developer Maintainers have a responsibility for ensuring PII/PHI data minimization, per the CMS IS2P2. In CCSQ, we feel that figuring out the least amount of data that is needed is an ongoing effort that includes the support of the ISSO (Now referred to as Security and Privacy Officer), CMS Product Owner, and the Application Development Organization (ADO)/Contractor. These supportive roles are closer to the information and can provide additional insight to the Business Owner, CO/COR and System Developer Maintainer.

For example, an Impact Analysis is to analyze changes to the system to determine potential security and privacy impacts prior to change implementation. The CMS Product Owner, ISSO and ADO can perform this analysis when adding new data to a system. It's also an opportunity to review the purpose of the new data and to consider alternative ways to achieve the same purpose without adding unnecessary PII/PHI. Ultimately, the Business Owner makes the final call.

Conclusion

This Data Minimization Strategy is built on activities already found within CMS. In creating a strategy, we hope to show the relationship between these activities to build a greater understanding of data minimization that helps us to pack light.

For more information on CCSQ's Data Minimization Strategy, reach out to Casey Douglas at: casey.douglas1@cms.hhs.gov.
For questions about data minimization, reach out to the CMS Privacy team at: Privacy@cms.hhs.gov.

Casey Douglas is currently a CMS ISSO in the Center for Clinical Standards and Quality (CCSQ). Past experiences include almost 20 years in the private healthcare industry and various contracting positions in OIT/ISPG and OEDA/DASG.

Information Communications Technology Acquisitions; Avoid Doing Business with Prohibited Sources

Michael Hobert -DSI ISPG SCRM Team

ICT Supply Chain Acquisitions

Information and communications technology *"[i]ncludes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks)."* (Computer Security Resource Center, NIST). Information and communications technology (ICT) is an area of special concern for the US Federal government acquisition for several reasons:

1. **National Security:** ICT products and services are integral to national security, as they are used in critical infrastructure, defense systems, and communication networks. The government must ensure that these technologies are secure and not vulnerable to exploitation or cyberattacks that could compromise national security.
2. **Data Protection and Privacy:** The Federal government collects and manages vast amounts of sensitive information about its citizens, businesses, and operations. Ensuring the privacy and security of this data is paramount to protect against unauthorized access, data breaches, and identity theft.
3. **Supply Chain Security:** The ICT supply chain can be complex and global, with components and services sourced from various countries and vendors. Ensuring the security and integrity of the supply chain is essential to prevent the introduction of counterfeit components, malicious software, or hardware vulnerabilities that could compromise the reliability and security of ICT systems.
4. **Compliance and Regulations:** The Federal government is subject to various laws, regulations, and standards governing the acquisition, use, and management of ICT products and services. These include requirements related to cybersecurity, data protection, accessibility, interoperability, and procurement practices. Ensuring compliance with these regulations is crucial to avoid legal and regulatory risks.
5. **Emerging Technologies**: Rapid advancements in ICT, such as artificial intelligence, Internet of Things (IoT), and quantum computing, present both opportunities and challenges for the Federal government. Acquiring and integrating emerging technologies requires careful evaluation of their capabilities, risks, and potential impacts on government operations and mission objectives.

ICT is a critical enabler for government operations and services, but its acquisition involves unique challenges related to security, privacy, supply chain integrity, compliance, and emerging technologies. Therefore, it requires special attention and expertise to effectively manage these risks and ensure the successful deployment and utilization of ICT resources across the Federal government.

Avoiding Prohibited Sources

Federal government acquisitions are subject to regulations aimed at preventing transactions with **prohibited sources**. One significant regulation in this regard is the **Federal Acquisition Regulation (FAR) Subpart 9.4**, which outlines procedures for determining and dealing with contractors who are debarred, suspended, or proposed for debarment.

FAR Subpart 9.402 Policy

(a) ***Agencies shall solicit offers from, award contracts to, and consent to subcontracts with responsible contractors*** *only. Debarment and suspension are discretionary actions that, taken in accordance with this subpart, are appropriate means to effectuate this policy.*

(b) The serious nature of debarment and suspension requires that these sanctions be imposed only in the public interest for the Government's protection and not for purposes of punishment. Agencies shall impose debarment or suspension to protect the Government's interest and only for the causes and in accordance with the procedures set forth in this subpart.

(c) Agencies are encouraged to establish methods and procedures for coordinating their debarment or suspension actions.

(d) When more than one agency has an interest in the debarment or suspension of a contractor, the Interagency Committee on Debarment and Suspension, established under Executive Order 12549, and authorized by Section 873 of the National Defense Authorization Act for Fiscal Year 2009 (Pub. L. 110-417) (31 U.S.C.6101, note), shall resolve the lead agency issue and coordinate such resolution among all interested agencies prior to the initiation of any suspension, debarment, or related administrative action by any agency.

(e) Agencies shall establish appropriate procedures to implement the policies and procedures of this subpart.

FAR Subpart 9.4 is a good example that can be used as a model to understand the intent and structure of other similar regulations. Here is a summary of its key points:

1. **General**: FAR Subpart 9.4 outlines the procedures for determining whether prospective contractors are responsible and capable of performing a government contract.
2. **Responsibility Determination**: Contracting officers must ensure that prospective contractors possess the necessary financial resources, ability, integrity, and other qualifications to perform the contract satisfactorily.
3. **Pre-award Surveys of Prospective Contractor's Financial Capability**: When necessary, contracting officers may conduct pre-award surveys to assess the financial capability of prospective contractors.
4. **Cooperation with Agency Accounting and Audit Personnel**: Contracting officers may consult with agency accounting and audit personnel to obtain information relevant to determining a prospective contractor's responsibility.
5. **Contractor Team Arrangements**: Subpart 9.4 also addresses contractor team arrangements, emphasizing that the prime contractor is responsible for overall contract performance and may be held accountable for the work of its subcontractors.
6. **Subcontractor Responsibility**: Contracting officers must also consider the responsibility of subcontractors when evaluating a prime contractor's responsibility.
7. **Suspension and Debarment**: The subpart highlights the importance of considering whether a prospective contractor has been suspended or debarred from government contracting, as this would generally indicate a lack of responsibility.

Under FAR Subpart 9.4, contracting officers are required to check the **System for Award Management (SAM) database** to ensure that prospective contractors are not debarred, suspended, or proposed for debarment. [Note: www.SAM.gov requires registration to access the database]. If a contractor is found to be listed, they are prohibited from participating in federal government acquisitions until the debarment or suspension is lifted.

Additionally, the U.S. government has imposed restrictions on doing business with certain entities or individuals due to national security concerns or other reasons. For instance, the **U.S. Department of Commerce's Bureau of Industry and Security (BIS)** maintains lists of entities and individuals subject to export control regulations, including:

- **Denied Persons List.** A list of individuals and entities that have been denied export privileges. Any dealings with a party on this list that would violate the terms of its denial order are prohibited. See Section 764.3(a)(2) of the EAR.
- **Entity List.** These parties present a greater risk of diversion to weapons of mass destruction (WMD) programs, terrorism, or other activities contrary to U.S. national security and/or foreign policy interests.
- **Unverified List**. A list of parties whose bona fides BIS has been unable to verify.
- **Military End User List.** These parties have been determined by the U.S. Government to be 'military end users,' and represent an unacceptable risk of use in or diversion to a 'military end use' or 'military end user' of adversarial nations.
- **Consolidated Screen List.** The Consolidated Screening List (CSL) is a list of parties for which the United States Government maintains restrictions on certain exports, reexports, or transfers of items.

Transactions with entities on these lists may be restricted or prohibited, depending on the specific circumstances. U.S. federal government acquisitions are governed by regulations that aim to ensure compliance with legal and policy requirements, including prohibitions on dealing with sources who are debarred, suspended, or otherwise restricted from participating in government contracts. These regulations help safeguard the integrity of the procurement process and protect national interests.

How to Avoid Doing Business with Prohibited Sources

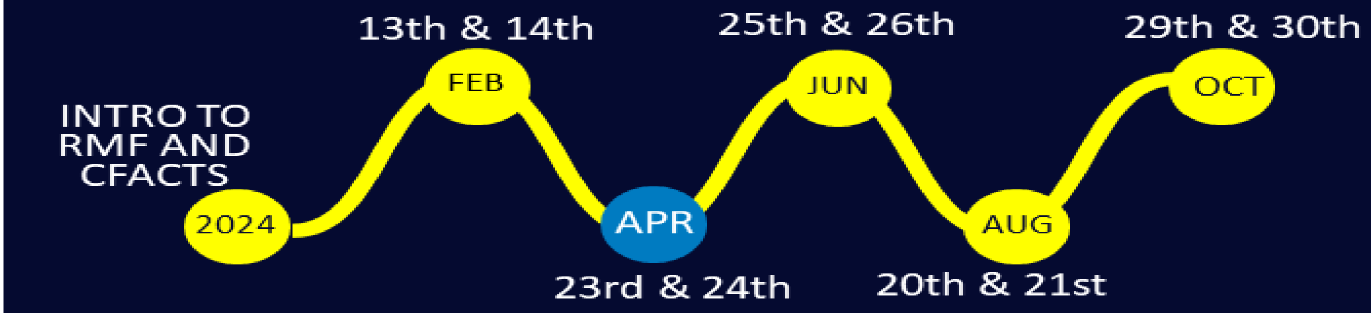
CMS has a team of professionals working to help you and your colleagues avoid doing business with prohibited sources. Working closely with the **Office of Acquisitions & Grant Management (OAGM)**, the **Division of Strategic Information(DSI) Supply Chain Risk Management (SCRM) Team** will help you assess the risks associated with ICT acquisitions. You can reach the DSI SCRM Team by e-mail at **SupplyChainRiskManagement@cms.hhs.gov.**

Michael Hobert is a member of the DSI ISPG SCRM Team where he is focused on Instructional Design/Training, Outreach and Awareness. Michael has worked in tech, finance, and healthcare for top Fortune 500 companies as well as disruptive start-ups.

INTRO TO RMF AND CFACTS

Risk Management Framework & CMS FISMA Continuous Tracking System

2024 TRAINING DATES



INTRO TO RMF AND CFACTS
2024

FEB
13th & 14th

APR
23rd & 24th

JUN
25th & 26th

AUG
20th & 21st

OCT
29th & 30th

Interested?
Please contact:
CMSISPGTrainers@cms.hhs.gov

SaaS-to-SaaS Crosstalk. Knowing When Enough Is Enough.

Daniel Wallace

SaaS-to-SaaS security refers to measures and strategies implemented to ensure the secure exchange of data and services between different SaaS applications. As CMS adopts additional SaaS solutions, the need for these applications to share data and functionality increases. However, each integration point can potentially serve as a vector for security breaches, data leaks, and compliance violations.

SaaS-to-SaaS security is a critical aspect of modern business operations, where organizations increasingly rely on a variety of SaaS applications for their daily activities. This interconnected SaaS ecosystem allows for streamlined workflows and enhanced productivity but also introduces unique security challenges. Ensuring the security integration and interaction between these SaaS applications is paramount to protect sensitive data and maintain operational integrity. Here, we will explore the importance of SaaS-to-SaaS security and outline best practices for organizations, such as CMS, to implement.

Over the past couple of years, we have seen a vested interest by CMS to increase its productivity by interconnecting SaaS applications such as Slack, SalesForce, Grammarly, Box, Snowflake, Jira, the Adobe Suite, Microsoft 365, and more. Although these connections enhance workplace efficiencies, they may expose the organization to unnecessary risk. These connections require rights, such as the right to read, create, update, and/or delete personal or corporate data. This level of access is granted in seconds and is usually far outside the view of the IT and security teams. While they require rights, ISSOs should require insights and control capabilities.

As an example, let us look at a possible SaaS-to-SaaS interconnect using Box and Slack. Integrating Box with Slack allows teams to streamline their workflows by easily sharing and accessing files stored in Box directly within Slack conversations. This connectivity enhances collaboration by ensuring team members have immediate access to the latest versions of documents --enabling quicker review and feedback cycles without the need to switch between applications. This seamless integration supports more efficient communication and project management, making it ideal for teams looking to optimize their productivity and collaboration efforts.

> A full list of integration capabilities, inclusive of actions that may be taken by admin accounts, service accounts, and end-user accounts, may be found here in the Slack app directory.

As you will find (*but not limited to*):

- *Instant permissions* may update the collaboration permissions of a Box file directly from within Slack.
- *Automatic uploads* to Box are possible.
- *Enable/disable content indexing for search in Slack* shows as an option for whether or not the contents of shared Box files are index and surfaced in Slack's native search.

Are you aware that these things could be happening in your environment?

Importantly, all organizations must consider key challenges associated with SaaS-to-SaaS security and take appropriate measures to mitigate the risks. To meet this challenge, CMS has partnered with AppOmni, a SaaS Security Posture Management (SSPM) leader, to help provide insights into SaaS-to-SaaS misconfigurations and interconnects. In fact, CMS' SaaSG team uses this tool regularly to provide visibility and control over SaaS-to-SaaS interconnections. Once visibility is gained, stakeholders immediately know how to reduce their attack surface and protect sensitive data. Use of this tool addresses the complex challenge of securing interconnected SaaS environments where manual monitoring and management are impractical due to the scale and dynamic nature of cloud services.

Key Challenges

Data Protection: Ensuring data remains secure as it moves between SaaS applications is a primary concern. Data in-transit and at-rest needs to be protected against unauthorized access and breaches.

Identity and Access Management (IAM): With multiple SaaS applications, managing who has access to what, and under which circumstances becomes complex but essential.

Compliance: Adhering to regulatory requirements, such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), or System and Organization Controls type 2 (SOC 2), is crucial for businesses operating globally or in regulated industries. Specifically speaking to prescribed CMS requirements, have your SaaS-to-SaaS connections been analyzed for violation?

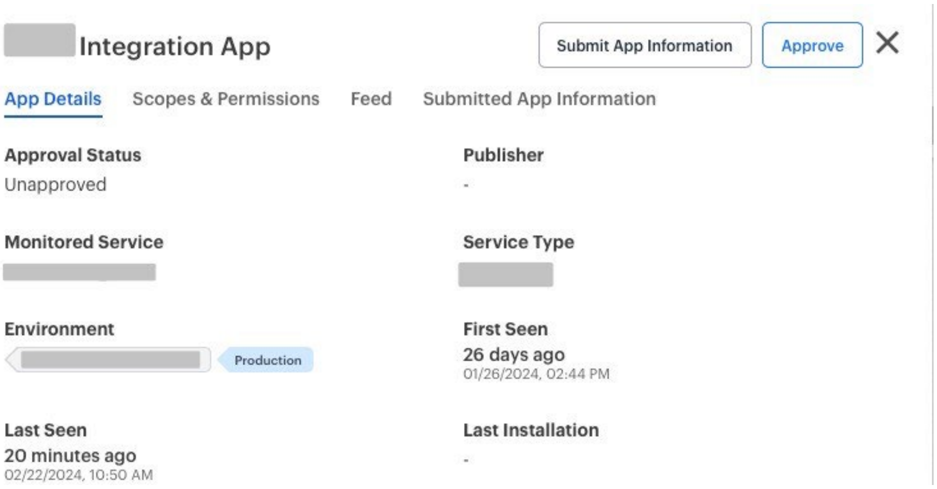
Visibility and Monitoring: Gaining comprehensive visibility into the security posture and real-time monitoring of all SaaS interactions can be challenging but is necessary to detect and respond to potential threats.

Best Practices for SaaS-to-SaaS Security *(but not limited to)*

1. **Conduct Comprehensive Vendor Assessments:** Before integrating with another SaaS application, evaluate its security measures, review, and peruse compliance certifications, and thoroughly review its data protection policies. Only proceed with vendors that meet your organization's security standards. **Specifically, to help CMS stakeholders understand the** risk posture of a SaaS vendor and which controls they are responsible for before implementing a pilot or procuring license, the SaaSG team has developed and implemented a Rapid Cloud Review (RCR) for non-FedRAMP'ed SaaS. You may also supplement (not replace) reviews with continuous Software Bill of Materials ("SBOM") analysis. Analysis should always be continuous and never simply to meet a 'point-in-time' satisfaction level. Security settings, technology, and controls capabilities are always changing- your awareness should remain steadfast and current.
2. **Implement Strong Authentication and Authorization:** Use robust IAM practices, including phishing-resistant multi-factor authentication (MFA) and least privilege access, to ensure that only authorized users may access specific data and functionalities across SaaS applications. Best practice is to integrate with IDM/SSO. An identity and access management solution may provide insights into which users are leveraging access and authentication into SaaS, which may provide new and/or validated intelligence.
3. **Regularly Review and Audit Permissions:** This is paramount! At intervals, and as needed, you should audit who (and what service account(s)) have access to resources across your SaaS ecosystem. Adjust permissions as necessary to ensure that users and service accounts only have access to the data and functionalities required for their/its role.

4. **Monitor and Log Activity:** Implement comprehensive monitoring and logging of all interactions between SaaS applications. Use security information and event management (SIEM) tools to analyze logs for suspicious activity. Strong information security programs fine-tune their SIEMs, leveraging signals to automate controls. At CMS, resources are available via the CMS Cybersecurity Integration Center (CCIC) for this specific purpose. If you are not sure if the SaaS you or your team are leveraging has been integrated with CCIC, the SaaSG team can help. Feel free to message us via our Slack channel so we may initiate this process.
5. **Educate and Train:** Provide ongoing training for your organization's staff on the importance of SaaS-to-SaaS security, recognizing phishing attempts, and safe data handling practices to foster a culture of security awareness.

As previously noted, SSPM tooling, such as AppOmni, are built with capabilities to provide SaaS-to-SaaS insights. This level of information delivery is very useful to security practitioners and managers who want to immediately see the identity of who (i.e., admin, service accounts, or end-user) has authorized respective interconnects, what (and when) permissions have been granted, and which nested environment is connected.



[redacted] Integration App

Approval Status
Unapproved

Publisher
-

Monitored Service
[redacted]

Service Type
[redacted]

Environment
[redacted] Production

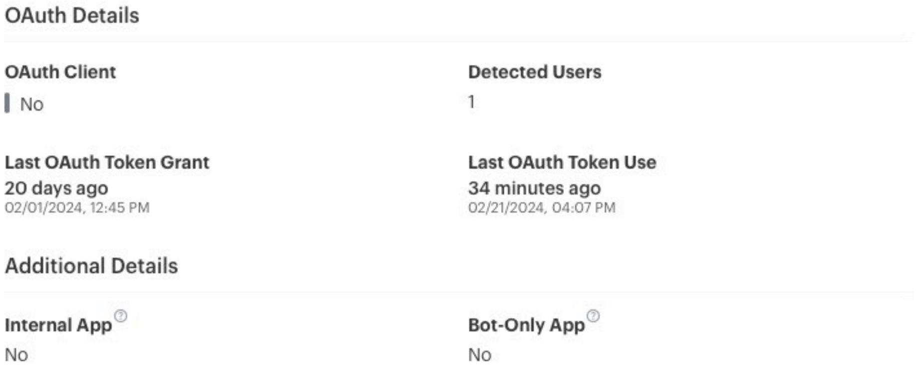
First Seen
26 days ago
01/26/2024, 02:44 PM

Last Seen
20 minutes ago
02/22/2024, 10:50 AM

Last Installation
-

Attribution/sensitive information has been redacted for privacy purposes.

Captured from the AppOmni tool, we are able to clearly identify which attributes tooling can extract from SaaS-to-SaaS interconnects; which App (monitored service) has been authorized, Publisher information, Service Type, Environment, Date and Time First Seen, and Date and Time Last Seen.



OAuth Details

OAuth Client
No

Detected Users
1

Last OAuth Token Grant
20 days ago
02/01/2024, 12:45 PM

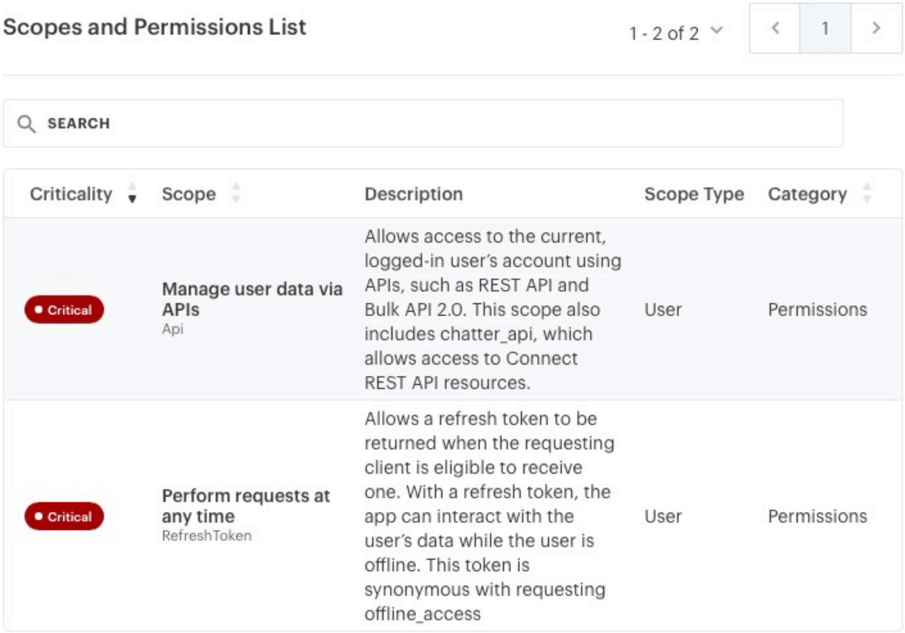
Last OAuth Token Use
34 minutes ago
02/21/2024, 04:07 PM

Additional Details

Internal App
No

Bot-Only App
No

It is important to know who has authorized each interconnect. Here we are able to capture these details along with when tokens were issued.



Criticality	Scope	Description	Scope Type	Category
Critical	**Manage user data via APIs** Api	Allows access to the current, logged-in user's account using APIs, such as REST API and Bulk API 2.0. This scope also includes chatter_api, which allows access to Connect REST API resources.	User	Permissions
Critical	**Perform requests at any time** RefreshToken	Allows a refresh token to be returned when the requesting client is eligible to receive one. With a refresh token, the app can interact with the user's data while the user is offline. This token is synonymous with requesting offline_access	User	Permissions

No longer guess about what might be happening 'behind the scenes.' Insights such as permissions and magnitude of scope should be in your direct view. You should be able to instantly capture what information is being read/written/deleted across an interconnect.

So, What Is Next?

There are a number of key takeaways that may have resonated with you. And for some, there may now be probing questions that you would like to present to your team. Questions such as:

- *Do we actually know when SaaS interconnections are happening in our environments?*
- *How does this affect our upcoming compliance checks and audits?*
- *If we are doing SaaS-to-SaaS interconnections, are we using accounts that are part of CMS' official Identity management platform?*
- *Are we simply overly permissive in our account management practices?*

As a CMS Business Application Owner, it is important to keep these questions in mind as your team adopt, configure, and connect SaaS applications. Additionally, you also want to be mindful of not carelessly bestowing overly permissive rights onto an account so that it can simply work and get the interconnect working. This requires strategic planning, thorough and rigorous implementation of best practices, and sound continuous monitoring. By taking preventative measures to secure your SaaS ecosystem, you are in a better position to protect your data, firm up your regulatory compliance, and optimize the benefits of your SaaS investments. To learn more about SaaS-to-SaaS connections or if you interested in potentially discovering what connections reside in your current environments, we strongly encourage you or a representative from your team to reach out to the CMS SaaSG Team via Slack. #ispg-saas-governance

All trademarks, logos and brand names are the property of their respective owners. All company, product and service names used in this journal are for identification purposes only. Use of these names, trademarks, and brands does not imply endorsement.

Daniel Wallace serves as Senior Security Architect at Aquia and supports the Software-as-a-Service (SaaS) Governance team (SaaSG) and its efforts to discover, manage, and secure SaaS. Within this realm, Daniel supports CMS' efforts to develop and deploy a comprehensive and quantitatively driven Continuous Monitoring program for SaaS.

Letter To Our Partners

Dr. David A. Wheeler

ACT 2023 in Review

The Adaptive Capabilities Testing (ACT) Program has accomplished a lot in 2023. In 2023, the Information Security Acceptable Risk Safeguards (ARS) 5.0 implementation was completed, along with the development and implementation of new templates for all assessment-related artifacts, and control mapping was implemented. We have updated the Core Controls internal processes for the CAAT file and revamped the ACT Handbook, templates, and SOPs. In addition, we worked diligently with the SIGNAL Application Development team to design and develop a scheduling system that would allow stakeholders to have a one-stop shop where they could schedule and track their assessment requests. A testament to our dedication to the mission of ISPG, the ACT Program successfully conducted 126 security assessments, 64 Risk Assessments, and seamlessly integrated 13 new systems into the program. The year 2023 stands out as a landmark year, showcasing the ACT Team's commitment to CMS stakeholders and to help better the Agency's security posture.

2024 The Road Ahead

Although we have had many accomplishments in 2023, we are excited to see what 2024 holds for the program. Starting March 1, 2024, ACT will change its name to Cybersecurity and Risk Assessment Program (CSRAP). Why the change? This change is a move toward a partnership-based methodology to align with ISPG strategies and the strategic goal of risk-based program management. This change is a holistic approach to assessing risk and is the principal methodology of CSRAP. This partnership methodology will help our partners make better data-driven, risk-based decisions by using analytics to help optimize performance, streamline processes, and reduce risk.

The change also takes into consideration the growing cyber threat landscape. Establishing a more flexible and robust assessment program to meet tomorrow's security threats is critical in helping our partners secure the CMS infrastructure. This means increasing security threat awareness, changing internal processes to ensure better compliance and support, and introducing more service lines to give our partners better options to enhance their system's security posture. Rest assured, CSRAP will continue to provide the quality service and customer support our partners deserve during this transition period.

As we embark on this journey of growth and discovery, we are grateful for your partnership and look forward to navigating these exciting changes together. 2024 promises to be a year of transformation, innovation, and strengthened security, and we're thrilled to have you join on in this pivotal journey.

Dr. David A. Wheeler - As the lead program manager for the Cybersecurity and Risk Assessment Program (CSRAP), Dr. Wheeler is committed to supporting our partners through innovation and active customer service.

Integrating Threat Modeling with Change Management: Enhancing Cybersecurity through Strategic Assessments and Documentation

Maril Vernon (Aquia)

The Essence of Threat Modeling

At its core, threat modeling is an analytical framework used to identify, assess, and address potential security threats to a system. Its application can be simplified by drawing parallels to everyday actions, such as locking our doors or being cautious when crossing the street, demonstrating that threat modeling is not just a cybersecurity task but a fundamental part of our daily risk management practices. This approach to understanding threat modeling emphasizes its relevance not only in the digital realm but also in our routine decision-making processes.

Adapting to Changes: Assessments and Documentation

There are a number of critical processes for Change Assessments and Documentation within the context of CMS. Such as ACT (Adaptive Capabilities Testing), SIA (Security Impact Analysis), CM-4 (from NIST 800-53), and Risk Assessments frameworks. Each of these processes serves a unique purpose in evaluating and documenting the potential security and privacy impacts of changes *before* implementation. This structured approach ensures that security considerations are integrated into the system lifecycle, facilitating compliance and mitigating risks proactively.

Integrating Threat Modeling with Change Management

Where is the interconnectivity between threat modeling and CMS change management processes? By asking critical questions such as "What are we working on?", "What can go wrong?", and "How do we address and mitigate these risks?", organizations can create a robust framework that not only identifies and assesses threats but also evaluates the security impacts of system changes. This holistic view enables organizations to implement security measures effectively, ensuring that changes do not introduce new vulnerabilities or compromise the system's former defensive baselines. Additionally, the documentation supports the Change Assessments’ need that these have been taken into consideration and planned for intelligently. So, oftentimes the mitigations and threats documented in a threat model will be a crucial piece of the evidence submitted for SIA and ACT packages.

Conclusion: The Synergy of Theory and Practice

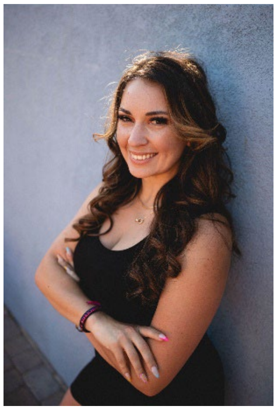
By highlighting the synergy between threat modeling and change management processes, we underscore the importance of a proactive, integrated approach to security. This methodology not only enhances an organization's ability to manage risks but also aligns with regulatory requirements and industry best practices, ultimately strengthening the security posture in the face of evolving threats and challenges.

In essence, the integration of threat modeling with change assessments and documentation exemplifies a comprehensive strategy for managing cybersecurity risks. It is a testament to the evolving landscape of cybersecurity, where adaptability, thorough assessment, and detailed documentation form the cornerstone of effective security and risk management strategies.

Learn more about Threat Modeling at CMS:

1. Check out the CMS Threat Modeling page on ISPG CyberGeek: https://security.cms.gov/learn/threat-modeling
2. Join the #cms-threat-modeling channel on CMS Slack.
3. Email the CASP Threat Modeling Team (ThreatModeling@cms.hhs.gov) to receive information on live interactive training or to engage in a Threat Modeling session.
4. Register for a monthly CASP Threat Modeling Office Hours session: Second Thursdays of the month at 1:00 PM ET https://confluenceent.cms.gov/display/CTM/Threat+Modeling+Office+Hours

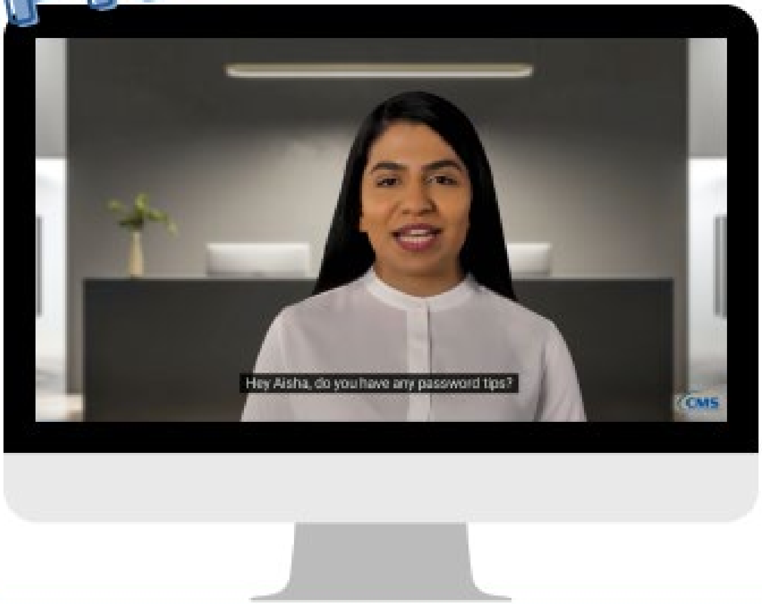
CASP Threat Modeling Team - Robert Hurlbut, Maril Vernon, Eric Rippetoe
CASP Lead - Eric Rippetoe
CMS / ISPG Contacts: Michael Kania, Robert Wood



Marial Vernon (Aquia) is a Principal Application Security Architect on the CMS / CASP Threat Modeling Team

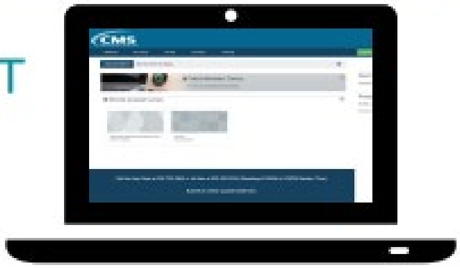
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

NEW AND IMPROVED!



INFORMATION SYSTEMS SECURITY AND PRIVACY AWARENESS (ISSPA) TRAINING

Available now on the CBT
https://www.cms.gov/cbt/



Having technical issues with the course? Email CMS_IT_Service_Desk@cms.hhs.gov
Security and privacy questions? Contact us! CMSISPGTrainers@cms.hhs.gov

Navigating the Digital Frontier: Technology, GRC, and ISSOs in the Age of Innovation

Tim Tipton Jr.

Introduction

In an era marked by relentless technological evolution, the digital frontier is expanding at an unprecedented pace. This rapid digital transformation is not just reshaping the way we live and work but is also setting new paradigms for cybersecurity and compliance. At the heart of this transformation lies a critical nexus between Governance, Risk Management, and Compliance (GRC) and Information Systems Security Officers (ISSOs), whose roles have become more pivotal than ever in safeguarding our digital cosmos.

GRC is an integrated framework that helps organizations ensure they act ethically and in accordance with their risk appetite, internal policies, and external regulations. ISSOs, on the other hand, are the custodians of an organization's information security, tasked with implementing and managing security measures to protect digital assets against unauthorized access, theft, or damage.

As we embark on this journey through the digital age, the interplay between technology, GRC, and ISSOs becomes increasingly complex and intertwined. The advent of advanced technologies such as quantum computing, artificial intelligence (AI), blockchain, and cloud computing has not only introduced new opportunities for innovation but also new vulnerabilities and challenges in cybersecurity and compliance. This article aims to explore the pivotal role of technology in shaping GRC strategies and enhancing the ISSO's efficacy in safeguarding our digital assets. Through this exploration, we will uncover how technology-driven approaches are revolutionizing the GRC landscape and elevating the role of ISSOs in ensuring a secure and compliant digital environment.

The Digital Transformation of GRC

The digital transformation has become a buzzword synonymous with innovation and progress across all sectors. However, beneath the surface of this technological revolution lies a significant impact on GRC frameworks. Traditional GRC models, designed in an era before the introduction of these advancing technologies, are now being challenged to adapt to the complexities of the digital age.

The Impact on Traditional GRC Frameworks

Traditional GRC frameworks, with their manual processes and siloed operations, struggle to keep pace with the rapid scale of digital innovation. The digital era demands agility, flexibility, and integration—qualities that are often lacking in legacy GRC approaches. As organizations migrate to digital platforms, the volume, velocity, and variety of data increase exponentially, complicating compliance and risk management efforts. This digital shift necessitates a transformation in how organizations conceptualize and implement GRC strategies, pushing them towards more dynamic and technology-driven models.

Integration of Advanced Technologies in GRC Practices

To navigate this digital landscape, GRC frameworks are increasingly integrating advanced technologies. Artificial Intelligence (AI) and Machine Learning (ML) are being employed to automate compliance monitoring and risk assessments, enabling real-time insights and predictive analytics. Blockchain technology offers a secure and transparent way to manage contracts, compliance documentation, and transaction records, enhancing trust and simplifying regulatory audits. Cloud computing, with its scalable resources, facilitates the implementation of GRC solutions that can adapt to the evolving needs of the organization, providing both flexibility and resilience.

Case Examples of Digital-First Approaches in GRC Implementation

Several forward-thinking organizations have embraced digital-first approaches to revamp their GRC frameworks. For instance, a global financial services firm implemented a blockchain-based system for real-time fraud detection and regulatory reporting, significantly reducing compliance costs and enhancing transparency. Another example is a healthcare provider that leveraged AI-powered analytics to identify and mitigate privacy risks in patient data management, ensuring compliance with stringent regulations while improving patient trust.

These examples illustrate the profound impact of digital transformation on GRC, highlighting the shift from traditional, reactive approaches to proactive, technology-enabled strategies. By leveraging digital technologies, organizations can enhance their GRC frameworks, making them more agile, integrated, and capable of addressing the complexities of the digital age.

ISSOs at the Helm of Technological Innovation

In the rapidly evolving digital landscape, ISSOs are finding their roles at a crossroads of technological innovation and security. As organizations navigate through the complexities of digital transformation, ISSOs are increasingly recognized not just as guardians of information security but as pivotal figures in steering these entities through the challenges and opportunities presented by new technologies.

The Evolving Role of ISSOs Amidst Rapid Technological Advancements

Gone are the days when ISSOs focused solely on establishing firewalls and enforcing password policies. In the age of digital innovation, their role expands to encompass a broader spectrum of responsibilities, including the strategic integration of cybersecurity measures into the organization's digital transformation initiatives.
ISSOs are now at the forefront of implementing advanced security technologies such as encryption algorithms, blockchain for secure transactions, and AI-driven threat detection systems. Their role involves a delicate balance between enabling technological innovation and safeguarding against the myriad of cybersecurity threats that accompany digital advancements.

Leveraging Technology to Enhance Security Protocols and Compliance Measures

To effectively manage the increased complexity and volume of threats in the digital era, ISSOs are leveraging technology to enhance security protocols and compliance measures. For instance, they employ sophisticated data analytics tools to sift through vast amounts of data for potential security threats and compliance issues, enabling proactive risk management. Machine Learning algorithms are utilized to adapt and improve security measures based on evolving threat patterns. Additionally, cloud security platforms are being adopted to ensure the secure migration and storage of data, facilitating compliance with data protection regulations.

Skills and Knowledge Advancements Required for ISSOs in a Tech-Centric World

The shift towards a more technology-driven approach necessitates ISSOs to possess a robust set of skills and knowledge that extends beyond traditional cybersecurity practices. Understanding the intricacies of cloud computing environments, the potential applications and security implications of blockchain technology, and the capabilities of AI and machine learning for cybersecurity are becoming essential. Moreover, ISSOs must stay abreast of regulatory changes and understand how to integrate compliance into technological solutions seamlessly. Continuous learning and professional development are crucial, as is the ability to communicate complex security concepts to non-technical stakeholders, ensuring organization-wide adherence to security and compliance standards.

- **Cybersecurity Incident Response:** Skills in developing and managing incident response protocols and teams to quickly address security breaches and minimize impacts.
- **Digital Forensics:** Knowledge in digital forensics for investigating and analyzing cyberattacks, understanding attack vectors, and identifying perpetrators.
- **Risk Assessment Methodologies:** Proficiency in advanced risk assessment methodologies and tools to evaluate and prioritize security risks in a dynamic digital environment.
- **Identity and Access Management (IAM):** Advanced knowledge in IAM technologies and strategies to ensure that only authorized individuals can access sensitive information.
- **Regulatory Technology (RegTech):** Familiarity with RegTech solutions for automating compliance tasks and managing regulatory changes efficiently.
- **Internet of Things (IoT) Security:** Skills in securing IoT devices and networks, addressing unique challenges posed by the proliferation of connected devices.
- **Cloud Architecture and Security:** Deep understanding of cloud service models (IaaS, PaaS, SaaS) and strategies for securing cloud environments beyond the basics.
- **Quantitative Risk Analysis:** Skills in quantitative risk analysis to assess and quantify cybersecurity risks, enabling data-driven decision-making.
- **Blockchain for Security Applications:** Understanding the security applications of blockchain beyond transactions, such as for secure identity management and supply chain integrity.
- **Artificial Intelligence Ethics and Security:** Knowledge of the ethical considerations and security implications of using AI in cybersecurity, ensuring responsible and secure AI deployments.

The Synergy between Technology, GRC, and ISSOs

This convergence is not just about leveraging technology for the sake of innovation; it's about creating a cohesive strategy that enhances security, compliance, and governance across all levels of an organization. Understanding and harnessing this synergy are key to navigating the technology-driven GRC landscapes of the future.

Examining How Technology Fosters Seamless Integration Between GRC Frameworks and ISSO Operations

Technology acts as the linchpin that ensures GRC frameworks and ISSO operations are not only aligned but integrated in a manner that enhances the organization's ability to manage risk and comply with regulations. For example, data analytics and AI can provide ISSOs with predictive insights into potential security threats, enabling preemptive action and informed decision-making. Similarly, cloud-based GRC platforms offer a centralized repository for policy management, risk assessment, and compliance reporting, facilitating real-time visibility and control for ISSOs and GRC professionals alike.

Strategies for ISSOs to Navigate Technology-Driven GRC Landscapes

To effectively navigate these landscapes, ISSOs must adopt a strategic approach that includes the following key elements:

1. Collaborative Framework Development: Working closely with GRC professionals to develop frameworks that integrate security and compliance considerations from the outset.
2. Technology Selection and Implementation: Carefully selecting technologies that support the organization's GRC objectives and ensuring their effective implementation and integration.
3. Continuous Monitoring and Adaptation: Implementing continuous monitoring solutions to track compliance and security status, coupled with the agility to adapt strategies as technologies and threats evolve.
4. Education and Advocacy: Educating stakeholders across the organization on the importance of GRC and security, advocating for a culture of compliance and risk awareness.

The Role of Data Analytics and Cybersecurity Tools in Informing GRC Decisions and ISSO Actions

Data analytics and cybersecurity tools are indispensable in informing GRC decisions and guiding ISSO actions. Through the use of sophisticated analytics platforms, ISSOs can identify patterns and anomalies that may indicate potential risks or compliance issues, enabling them to take proactive measures. Cybersecurity tools, including intrusion detection systems, encryption technologies, and vulnerability assessment tools, provide the necessary defenses and insights to protect against threats and ensure compliance with regulatory requirements.

By leveraging these tools and technologies, ISSOs can ensure that GRC practices are not only responsive to the current digital environment but also anticipatory of future challenges and opportunities. The synergy between technology, GRC, and ISSOs thus creates a dynamic ecosystem where security and compliance are not seen as business impediments but as essential components of organizational success.

Challenges and Solutions in Tech-Driven GRC and ISSO Roles

Challenges

The integration of advanced technologies into GRC and ISSO roles, while beneficial, introduces a set of complex challenges. Cybersecurity threats are becoming more sophisticated, leveraging AI and machine learning to bypass traditional security measures. The rapid pace of technological change can outstrip regulatory frameworks, leading to compliance gaps. Additionally, the sheer volume of data generated by digital technologies complicates privacy management and data protection efforts.

Solutions

To address these challenges, organizations must adopt a multifaceted approach. Implementing advanced cybersecurity measures, such as AI-driven threat detection systems, can enhance the ability to preempt and respond to sophisticated cyberattacks. Regularly updating GRC frameworks to align with emerging technologies ensures that compliance gaps are minimized. Furthermore, adopting privacy-by-design principles and utilizing encryption and anonymization techniques can mitigate data protection concerns. Continuous education and training for ISSOs and GRC professionals are essential to keep pace with technological and regulatory changes.

Real-World Success Story: A Healthcare Organization's Triumph

In the realm of healthcare, where the protection of sensitive patient data is paramount, one organization's journey exemplifies the profound impact of integrating technology into GRC and ISSO initiatives. This healthcare provider, faced with the dual challenges of complying with stringent health information privacy regulations and safeguarding against increasing cyber threats, turned to technological innovation to fortify its defenses and streamline compliance processes.

Challenge and Solution

The organization was grappling with the complexities of adhering to the Health Insurance Portability and Accountability Act (HIPAA) across its sprawling network of facilities, each generating vast amounts of confidential patient data. To address this, it implemented a cutting-edge, cloud-based GRC platform tailored to the healthcare industry's unique needs. This platform provided a comprehensive solution for risk assessment, compliance management, and data protection, all within a unified system.

Central to this transformation was the deployment of advanced encryption technologies and access controls to protect patient data across all points of the network. Additionally, the organization leveraged AI-driven analytics to monitor and analyze data flows in real-time, identifying potential privacy breaches or compliance deviations before they could escalate.

Innovative Practices for Enhanced Security

Under the guidance of its ISSOs, the organization adopted a 'security by design' approach in developing new digital health services. This proactive stance ensured that security and compliance were integral to the development process, rather than being retrofitted after deployment. The ISSOs played a crucial role in this process, overseeing the integration of security measures and ensuring that all new technologies adhered to regulatory standards.

Training and Awareness

Recognizing the importance of a security-conscious culture, the organization also invested in comprehensive training programs for its staff. These programs focused on the importance of data protection, the proper handling of patient information, and the recognition of phishing attempts and other cyber threats. This approach not only enhanced the organization's security posture but also fostered a culture of compliance and vigilance across all levels of the organization.

Outcome and Insights

The result of these concerted efforts was a significant reduction in data breaches and compliance violations, alongside improved efficiency in managing regulatory requirements. The organization's success story offers several key insights for other healthcare providers navigating the complexities of digital transformation:

- **Integrated Technology Solutions:** Adopting a holistic, technology-driven approach to GRC and cybersecurity can significantly enhance the ability to manage compliance and mitigate risks.
- **Proactive Security Measures:** Implementing a 'security by design' approach in developing digital health services ensures that security is a foundational element, rather than an afterthought.
- **Culture of Compliance and Security:** Investing in training and awareness programs is essential to building a security-conscious culture within the organization.
- **Role of ISSOs:** ISSOs are pivotal in steering the organization through the digital transformation, ensuring that security and compliance are seamlessly integrated into new technologies and practices.

This healthcare organization's experience underscores the potential of technology to transform GRC and ISSO roles in a highly regulated industry, offering valuable lessons for others in the sector.

Conclusion

The journey through the digital frontier is fraught with challenges, yet it offers unprecedented opportunities for enhancing GRC frameworks and empowering ISSOs. The integration of technology into GRC and ISSO roles is not merely a trend but a necessity in the age of digital innovation. By embracing technological advancements, organizations can navigate the complexities of cybersecurity and compliance with greater agility and effectiveness.

The synergy between technology, GRC, and ISSOs plays a critical role in this endeavor, fostering a dynamic environment where security and compliance are seamlessly integrated into the fabric of organizational operations. As we look to the future, the continuous evolution of this synergy will be paramount in driving forward the agenda of digital security and innovation. Embracing change, fostering continuous learning, and adopting a proactive stance on technology integration will ensure that organizations remain resilient in the face of evolving digital threats and compliance requirements.

This exploration of the intersection between technology, GRC, and ISSOs underscores the importance of a holistic approach to digital security and compliance. As organizations continue to navigate the digital age, the lessons learned, and strategies outlined herein will serve as a valuable guide for enhancing the efficacy of GRC frameworks and the role of ISSOs in safeguarding our digital world.

Tim Tipton Jr. (RevaComm) is one of the newest members of the CMS GRC Team. He is a Cybersecurity Engineer with extensive knowledge in Cyber & Risk Management.

Enhancing Email Vigilance at CMS: Emphasizing the Importance of Reporting Phishing

Nomar Delgado, Premier Enterprise Solutions, Cybersecurity Workforce Support & Training Team

CMS remains committed to cybersecurity and the well-being of our digital environment. An essential part of this commitment is the continuous promotion and utilization of the "Report Phishing" button within Outlook. This feature is pivotal in our ongoing battle against phishing attempts, which pose significant risks to our information security.

The Dual Threat: Spam and Phishing

Spam emails clutter our inboxes, reducing productivity and potentially introducing malware. Phishing, a more insidious threat, involves deceptive emails designed to steal sensitive information or credentials. Both threats require our immediate attention and action.

Your Role in Cybersecurity

Every CMS employee plays a crucial role in identifying these threats. The "Report Phishing" button is your first line of defense. By reporting suspicious emails, you help improve our email filters, reducing future spam and phishing attacks. More importantly, reporting phishing attempts allows our cybersecurity team to analyze and implement measures to prevent similar attacks.

Immediate Benefits of Reporting

- **Security Enhancement:** Each report aids in enhancing our email security measures.
- **Community Protection:** Your actions protect not just your inbox but also the CMS community.
- **Adaptive Security Measures:** Reporting helps in refining our defenses, making our systems smarter.

Continued Vigilance

We urge every member of CMS to remain vigilant and report suspicious emails promptly using the "Report Phishing" button or forwarding the suspicious email to ‘spam@cms.hhs.gov’. Your proactive actions are invaluable in our collective effort to maintain a secure and efficient digital workspace.

For guidance on identifying phishing emails or any other cybersecurity concerns, please contact the IT Help Desk. Together, we can ensure a safer CMS.

Nomar Delgado supports the Cybersecurity Workforce Support & Training Team program, where he is responsible for developing specialized cybersecurity training curricula that align with the NIST framework, ensuring that the workforce is well-prepared to meet current and emerging cybersecurity challenges.

Cybersecurity Community Forum Notes from December 2023, January, and February 2024

Cole Schenck (Assyst)

In December 2023:

- Michael Harris of the ISPG DSI SCRM Team gave a presentation about the implementation of the Federal Acquisition Supply Chain Security Act (FASCSA). All federal agencies will need to adhere to the directions within the interim rule. It will take effect December 4th, 2024. The expected outcome of these procedures is that it will reduce the exploitation of vulnerabilities, in turn making the supply chain more resilient.
- Teresa Proctor, director of DIR, gave a presentation giving an update on the transition over to the Security Data Lake (SDL). The CRM program is transitioning from the "Legacy" Data Warehouse to a Security Data Lake (SDW) to enhance scalability, processing, flexibility, and prepare for future security analytical capabilities. All dashboards will use the SDW as their primary data source as of Nov. 20th, 2023. The Core Legacy dashboards will be removed after the transition period on Feb. 1st, 2024.

In January 2024:

- Melinda Burgess gave an update about the ISPG CyberGeeks website. She began by giving a short tour of the website, showing off the updated homepage, the search function, user-validated menus, and more. Goals for 2024 include expanding content for top security and privacy activities, retiring old duplicative content from other spaces, establish an ISPG blog as a trusted source for security and privacy updates, and more.
- Rob Sheehan of the ISPG DSI SCRM Team gave a presentation about the implementation of the Federal Acquisition Supply Chain Security Act (FASCSA). Like the presentation in December, we were reminded who this affected, what was happening, how it was happening, and when it was happening. He also announced that CISA is proposing the Secure Software Development Framework explaining who is involved, what is happening, when it's happening, and so on.

In February 2024:

- Elizabeth Schweinsberg announced the Zero Trust Ambassador Program. The purpose of this program is to help people stay up to date on Zero Trust. They will be launching a newsletter and officer hours alongside the program!
- Tamara Kravitz announced the new and improved ISSPA training on the CBT website.
- Gita Ollage gave us an update of the Security Data Warehouse (SDW) migration. The SDW is now live in the SDL. Legacy dashboards are now retired. The CRM Dev Team will continue to focus on continuous improvements and updates.

- Chris Hadnagy, CEO of Social Engineering, gave a presentation on Levelized Managed Phishing. His program is designed to educate us at CMS to be aware of phishing attempts and to report them. He showed the different levels of phishing emails that were being sent out. From emails with lots of spelling errors to emails that looked incredibly professional and showed us data plots of those who have been reporting these emails as well as those who haven't.

The C3F PowerPoint slides and recordings can be found on C3F Confluence Page.

Cole Schenck works with Assyst within ISPG on the ISSO Advocacy and Support Program (IASP).

CISAB Notes from January and February 2024

Cole Schenck, (Assyst)

The CMS Information Security Advisory Board (CISAB) was established to provide a mechanism for cybersecurity and privacy concerns between the CISO, the Information Security and Privacy Group (ISPG), and CMS Information System Security Officers (ISSO). CISAB is a conduit for ISPG staff and ISSOs, both federal and contractor, to regularly collaborate and exchange information concerning cybersecurity and privacy related material and knowledge.

In our January meeting, Erica Rebstock gave a presentation about the Rapid Cloud Review policy asking all CMS stakeholders to leverage the RCR process for non-FedRAMPed SaaS. She also went through each step taken during the RCR process. Additionally, she talked about the RCR policy being added to the IS2P2 (CMS-CLD-1.1). Furthermore, she answered commonly asked questions about the RCR process. Those with questions should reach out to the SaaSG team on Slack (#ispg_sassg_team) or email (saasg@cms.hhs.gov). For our second topic, Shawnte Singletary wanted to explain what was happening with Governance, Risk, and Compliance (GRC) with ISPG. She explained that her team is visualizing GRC. What does GRC look like? The governance, the risk, and the compliance aspects at CMS. She explained that the division does a lot of the management and oversight of the risk management framework (RMF), but also helps with developing policies and procedures that need to be adhered to. She wants to visualize all of it.

In our February meeting, Kevin Allen wanted to know the full process when it comes to SaaS products. The provisional ATO process was unclear, and Kevin Allen wondered if it should be the same process as the regular ATO process. He also wondered what happened after you received a provisional ATO. Shawnte explained that once you have a SaaS tool, you go through the RCAR process and then put in for a provisional ATO. Once acquired, the tool can be used. Once a year, the tool will be reevaluated to see if it still wants to be used or if the FedRAMP path wants to be taken. For our second topic, Kevin Allen noted that CMS has five major lines of business: Medicare, Medicaid, Marketplace, Finance, and Management and Quality Oversight. Each have their own requirements in areas like security and privacy. He wanted to see if CyberGeeks can be leveraged to provide more transparency among each line of business as well as the agents and brokers. Melinda Burgess confirmed that if information can't be posted directly to CyberGeeks, it can be used to direct groups in the right direction.

Cole Schenck works with Assyst within ISPG on the ISSO Advocacy and Support Program (IASP). He acts as secretariat for the CISAB group.

Internal and External Resources for ISSOs

Confluence Sites

ISPG ISSO Workforce Resilience Program (Confluence) This Confluence presence is replacing the ISSO SharePoint site.

ISPG Policy Initiative Team (Confluence)

Slack Channels – Slack is the collaboration hub that brings the right people, information, and tools together to get work done. ISPG currently sponsors security Slack channels you may want to join, and we are always open to being invited to channels you finding interesting. you must install the Slack app on your laptop to access Slack and these channels.

Below are just some of the channels available:

#cra_help
#security_community
#vulnerability-digest
#ciso-bookclub
For ADO ISSO's… #cms-cloud-security-forum
For ISSOs… #cms-issos
General topics… #General

Web

ISPG Training Calendar at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/ISPG-Training-Catalog.pdf

CMS Information Security Library at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

NIST Cybersecurity Framework at https://www.nist.gov/cyberframework

NICE Cybersecurity Workforce Framework at https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

US-CERT at https://www.us-cert.gov/

SANS at https://www.sans.org/

OWASP at https://www.owasp.org/index.php/Main_Page

References

Unlocking Career Success for ISSO: The Importance of Communication Skills for Information System Security Officers

1. Indeed (2023, November 9). Mastering Essential Communication Skills (2024 Examples). https://in.indeed.com/career-advice/resumes-cover-letters/communication-skills
2. Beqiri, G. (2022, November 8). List of key communication skills for career progression. VirtualSpeech. https://virtualspeech.com/blog/list-key-communication-skills-career-progression
3. MBA. (2020, July 30). Employers Still Seek Communication Skills in New Hires. https://www.mba.com/information-and-news/research-and-data/employers-seek-communications-skills
4. Beheshti, N. (2018, September 24). Are hard skills or soft skills more important to be an effective leader? Forbes. https://www.forbes.com/sites/nazbeheshti/2018/09/24/are-hard-skills-or-soft-skills-more-important-to-be-an-effective-leader/?sh=6dd3ddb22eb3
5. Monan, E. (2018, July 31). The importance of communication for security. Security Magazine. https://www.securitymagazine.com/articles/89271-the-importance-of-communication-for-security
6. Bradley, T. (2017, November 30). Key to CISO role is effective communication. Forbes. https://www.forbes.com/sites/tonybradley/2017/11/30/key-to-ciso-role-is-effective-communication/
7. Effective communication for leaders. (n.d.). SMZ Health. https://smzhealth.com/26871-effective-communication-for-leaders-46/
8. Bobowski, K. (n.d.). How CISOs & CIOs can collaborate to effectively communicate risk. Evanta. https://www.evanta.com/resources/cxo/peer-practices/how-cisos-and-cios-can-collaborate-to-effectively-communicate-risk