ISSN: 2755-0214

Journal of Economics & Management Research

SCIENTIFIC Research and Community

Review Article

Open Access

Risk Reporting to Management on Federal Offers and How to Navigate the Conundrum?

Pranith Shetty

Information Security & Risk Lead, Cisco, New Jersey, United States of America

ABSTRACT

Technology firms mainly based out of U.S, in and around Silicon valley, in addition to a few firms on the U.S west coast, have products primarily catering to commercial customers across the globe, these are known as Commercial offers but there is another variant catering to the federal agencies and organizations known as Federal offers or Govt offers, the reason to keep this portfolio of products separate is because of the different set of criterias that need to be met and more stringent requirements. Since we are stepping into the government sector, the products in use for this sector have to be rock solid from a risk posture standpoint and in the case of cybersecurity threats hence the need for such criterias and requirements.

Management and Senior leadership of these technology firms are constantly interested in viewing the security and risk posture of all the products designed, developed and marketed to customers, risk reports of commercial offers have no regulatory obstruction or confidentiality requirements hence it's easier to present the risk overview along with the underlying details if requested , however, for federal offers, depending on the level of certification pursued and market access, there are some overarching regulations and confidentiality requirements around personnel viewing the metrics , storage locations.

This article sheds some light on the afore mentioned restrictions and a simple solution or rather an abstraction approach that helps navigate this problem, at the same time, ensuring no impact to the federal product or its customers.

***Corresponding author**

Pranith Shetty, Information Security & Risk Lead, Cisco, New Jersey, United States of America.

Received: December 13, 2023; **Accepted:** December 20, 2023; **Published:** December 27, 2023

Keywords: Federal Product Risk Posture, Federal Offer Risk Report, Risk Reporting, Risk Management

Introduction

Rationale for this Study

Risk reporting for commercial offers meaning the products available to all of us for commercial use has been done or performed for many years now and they go through the standard risk management lifecycle of Identification, Analysis, Response and finally Reporting.

However, it's easier said than done to perform the same process for the federal offers that are meant for government organizations or agencies due to many reasons, for example - it's difficult to obtain exact stakeholder inputs for qualitative analysis, confidentiality of data, Clearances to name a few.

In the light of above problems its very challenging to gather information around the risk posture of the offer, at the same time ensuring confidentiality of data.

The approach prescribed here in the following sections has been tried and tested, this process will help readers understand the background, context, various nuances of this problem along with a credible solution to overcome it. Senior leadership irrespective of the geographical location; they are placed at, will be able to understand the Risk posture of the federal offer due to the simplicity of the approach in abstracting detailed metrics and thereby confidential data.

Literature Review

As per Infusion points, a cybersecurity solutions company, there are many key nuances on the question of requirements of US personnel handling data and offer, as per PMO there is no overall federal requirement about citizenship, however, it may limit the reach of the cloud offers since the need for U.S personnel are key in some federal agencies that are part of critical national infrastructure, for valid reasons [5].

As per Hyperproof, a team vested in FedRamp consulting Continuous Monitoring metrics are key in maintaining the ATO (Authority To Operate) [6].

As per Eptura, a consulting team that guides companies through the FedRamp journey, FedRamp does not explicitly ask for the need of U.S personnel to work with data, meta data but the Federal agencies might bring up these requirements depending on the data classification and the type of project they are vested in, to use these products [7].

Difference between Commercial and Federal Offers and thereby Sales Impact

Commercial offers are products or services meant for consumption of normal individual users or enterprise customers in varied sectors

like Finance, Manufacturing etc.

Regardless, whether the product is commercial or federal space, companies ensure strong security architectural requirements, they run it through various teams for vulnerability checks, exposure and sound design. Stakeholders involved do a demo run of the product internally first and then there is a private preview with selected and trusted consumers, post which its announced publicly.

Additionally, these products do undergo compliance related certifications and checks like SOC2, ISO270001 and many more. As part of these compliance certifications there are a list of controls that a product has to comply with, these control areas ranging from basic access control requirements, to encryption of data at rest and in transit, there are several other requirements of logging and monitoring to ensure the product is not to be tampered with and in the event any such attack happens, then there is sufficient audit related controls to find the attacker.

Every firm does have a risk management process through which the risks are identified, analyzed, and eventually reported with appropriate risk response from Senior management.

Commercial product sales are a straightforward process as compared to Federal due to the absence of stringent regulations, hence the Sales staff can have an edge in the ability to penetrate more markets. The process is not easy however it is easier to understand it overall from a client perspective. Modifications and configuration changes can be achieved based on client's request which makes it more convenient for both the firm and customers, which drives the revenue, profits etc [4].

Federal offers on the other hand are products or services that are meant for the use of various federal agencies like FTC (Federal Trade Commission), FCC (Federal Communications Commission). The product security requirements and control obligations are stringent here due to the overarching regulatory obligations of handling confidential government data. As a result, the products developed for federal clients are on a separate instance of government clouds for data segregation reasons, furthermore, there are various regulation like FedRamp, StateRamp that govern the compliance obligations of these products, a multitude of audits and continuous monitoring controls are to be adhered to. The federal agencies still can exercise their option to opt out of contractual obligations, if they are not comfortable with the security provisions.

Risk reporting for federal offers currently is included as part of compliance related certifications namely FedRAMP, a few control statements are aligned around Risk management, there is no exclusive process or provision to report risks on the federal offers.

Federal product sales on the other hand are more difficult due to many parameters starting with Ethics rules, contracting related obligations, certification requirements, Budget etc. Sales staff have very little room to work with, Federal organizations have a final say here which is also fair given the confidentiality of data and the magnitude of the reputational impact of the breach.

Methods

Fedramp & ConMon (Continuous Monitoring)

It's important to understand FEDRAMP (Federal Risk and Authorization Management Program) for background on the risk report and its connection to the federal offers.

FedRamp is a government wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies [3].

To get to understand the Risk report a little better, let's try to get context on Continuous Monitoring requirements that forms the foundation of this report. After engaging with the Federal organization and satisfying some of the initial set of requirements, which involves a whole process around (P-ATO), Provisional Authority to Operate ,the firm that intends to provide the service or product satisfies a set of requirements as per the (P-ATO), they receive a letter from the Federal organization that's sponsoring this effort, in that letter there is a listing of minimum requirements that the firm should adhere to. These requirements are deliverables with evidence on a monthly and annual cadence. The deliverables are mainly around vulnerability scans, annual security assessments, incident reports, change requests.

FedRamp requires the organizations or in this case CSPs (Cloud Service providers) to collect evidence throughout the year on these areas, this maintaining the compliance requirements with the ConMon program. There are steps to build this program successfully

- Define a Strategy
- Establish metrics needed
- Initiate the program
- Analyze the findings and remediate it with the accountable parties
- Improve the overall program

The above steps are a continuous process as the name itself suggests and the metrics from this program feed into the Risk report that makes it palatable for the Senior Management in the firm to absorb and understand the Risk posture.

ConMon or Continuous Monitoring is mainly focused on three major areas of Operational Visibility, Incident Management and Change Management.

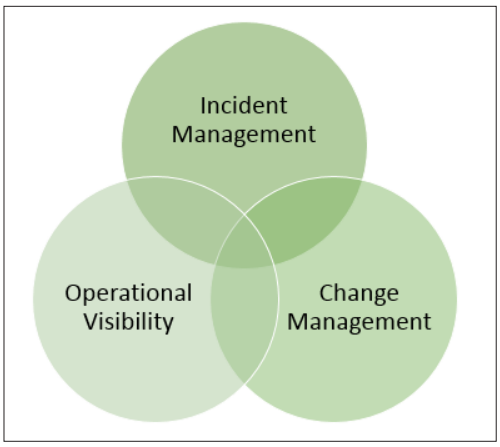

Figure 1: Continuous Monitoring Areas

CitVal

Most firms that work on FedRamp and with Federal agencies have personnel validated through various clearances either through third parties outside the firm or internally there are teams that vet people working on these projects. The core idea behind this approach is to protect the confidentiality of information and ensure minimal impact in the event of a breach or insider attack. This process is sometimes called as "CitVal" short for Citizen Validation process.

In today's world, firms expand across locations to support "round the sun" or 24/7 model, they employ teams that focus on development, testing and implementation across time zones to ensure seamless coverage and productivity at scale. This is also due to the amount of competition in this space. When we have employees spanning across borders due to strategic dependencies, there needs to be an administrative program that can control access provisions along with technical controls. This overarching program also ensures accesses are granted on "need to know" basis and whether employees requesting access are U.S personnel.

Below is how a "Risk report format" if presented or circulated to management, would help leadership understand the key tenets behind evaluating the risk posture of the federal offer

Preface: This section should give context on participating teams and content creation points, we are making it clear in this section on the participating teams and use of ConMon requirements.

To identify and measure the overall health and risk posture of the offer, Risk team based on the inputs from materials resulted out of ongoing assessments, FedRamp members, involved stakeholders from Umbrella engineering, SBG Prod Sec

"As a result of the information sensitivity and CitVal requirements around Federal environment space, the Risk team in partnership with stakeholders involved in the FedRamp program have opted to use ConMon requirements also known as Risk Management Deficiency triggers as a way to measure the operational effectiveness of controls in the following FedRamp environment and draft the Federal SRP."

Scope: Products consistently have major releases so it's important to scope products and their releases in, as part of the risk reporting exercise.

Content: ConMon requirements are classified under the following 3 sections to ensure consistent expectations and enforcement, FedRamp defines these requirements as risk management deficiency triggers. When a provider's performance exceeds one or more of the thresholds as defined in the following areas.

- **Operational Visibility:** Example could be "Late remediation of High Impact vulnerabilities (How many etc.)
- **Change Control:** Example could be "Late notice of Emergency changes (How may and days etc.)
- **Incident Management:** Example could be "no of incidents with recurring theme".

In the following section, risks has been classified in Tiers ensuring that importance is levied appropriately meaning Tier 1 risks are the risks to be focused on or thought through from a management perspective since that could have impact to the product 'Go to Market' strategy and thereby impacting sales.

Tier 2 risks are more on a routine check basis and need not be escalated to management level, Tier 2 risks first are moved up to Tier 1 for more attention and work, only then are escalated to Senior Management level.

"The risks have been classified as Tier 1 and Tier 2
Tier 1 risks are risks in the federal environment running overdue and which could hinder or pose a roadblock to ATO (Authority to Operate)
Tier 2 risks identified through the FedRamp program on an ongoing basis, resourcing constraints or minor operational risks resulting from other challenges".

Metrics from the three ConMon sections mentioned earlier, should be analyzed by the Risk manager and accordingly verbalized, Following areas can be looked into, Assuming there are no findings across these areas, below is how they would appear in the report.

- **Operational Risk:** There are no operational risks realized across the FedRamp program impacting the offer.
- **Vulnerability Mgmt.:** There are no high impacting vulnerabilities, current risk posture is low
- **Change Control:** There are no emergency changes, current risk posture is low.
- **Incident mgmt.:** There are no incidents, current risk posture is low.
- **Pentest:** Pen Test findings identified during the course of 3PAO (3rd party auditors) assessment were remediated and/or risk adjusted, current risk posture is low.
- **Annual Assessments:** Al identified findings during the 3PAO assessments have been remediate or in progress.

Overall health of the product is Green/Amber/Red and there is no impact to the ATO Green, Amber and Red statuses similar to Project management definitions where Red meaning "at risk" and Green indicating "all good".

Discussion

This risk report is first of its kind since not many firms have figured out the metrics needed to generate this report, at the same time to ensure confidentiality of the data in the report has also been a challenge for many firms. As we have observed, the report does not delve into the details but ensures the key areas of Continuous Monitoring are covered. This report helps senior stakeholders and especially senior management present outside U.S understand the risk posture of the products that they are vested in. It gives a good perspective on where things are with the federal offer and if more resources should be invested and which areas.

The risk report generated through this approach is flexible and can be adapted based on organizations portfolio of federal products, irrespective of the FedRamp journey they are in, the risk team only has to work with the selected set of stakeholders.

Conclusion

Now that we have understood and got a little context on the Risk report, details used, practical significance, it's important to understand why the need for abstraction and not include the whole set of metrics obtained from ConMon, the rationale behind tailoring the metrics.

At the same time Risk reports are Internal only meaning they can and in most cases should be circulated across the firm to ensure transparency, thus the need to intake ConMon metrics and format it in a way that does not conflict with the CitVal program but at the same time ensure Risk report transparency across borders and at the same time maintaining the confidentiality of the underlying metrics data. This format of report is palatable across senior stakeholders globally and can be saved in commercial instances where we don't have to worry about Gov cloud storage, the simple reason being there is no confidential data and all the actual metrics and details are still governed by the FedRamp within those boundaries. Thus ensuring information is communicated between the Compliance and Risk arm of the organization and making sure there is no overall impact to the ATO or sales because of this approach.

References

1. Lazarus Alliance (2023) Revising FedRAMP Continuous Monitoring with the New OMB Memo. Available: https://lazarusalliance.com/revising-fedramp-continuous-monitoring-with-the-new-omb-memo/
2. FedRAMP Training -Continuous Monitoring (ConMon) Overview 1 (2015) FedRAMP_Training_ConMon_v3_508. Available: https://www.fedramp.gov/assets/resources/training/200-D-FedRAMP-Training-Continuous-Monitoring-ConMon-Overview.pdf
3. Program Basics/ FedRAMP.gov. Available: https://www.fedramp.gov/program-basics/.
4. Ashely Neu (2023) 10 Differences Between Selling To Federal And Commercial Markets. Available: https://sanctumfederal.com/federal-sales-articles/10-differences-between-selling-products-to-the-federal-and-commercial-markets.
5. Shropshire J (2018) Demystifying FedRAMP - Part 4 - Who is allowed to work on the system or access SSP documentation? What about non-US Persons / non-US Citizens? | InfusionPoints. Available: https://infusionpoints.com/blogs/demystifying-fedramp-part-4-who-allowed-work-system-or-access-ssp-documentation-what-about.
6. Team H (2023) Maintaining FedRAMP Authorization: What to Know About Continuous Monitoring, Hyperproof. Available: https://hyperproof.io/resource/fedramp-authorization-continuous-monitoring/.
7. Davis J (2023) Demystifying FedRAMP compliance and authorization, Eptura. Available: https://eptura.com/discover-more/blog/demystifying-fedramp-compliance-and-authorization/.