Accreditation Models for Secure Cloud Adoption

June 2020

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

This paper provides best practices with respect to cloud accreditation to help organizations capitalize on the security benefits of commercial cloud computing, while maximizing efficiency, scalability, and cost reduction. It includes a comparative analysis relating to different accreditation models in use today to help decision makers considering and undergoing cloud adoption. While highlighting examples from public sector models, the best practices described apply to organizations considering cloud adoption from both the public and private sector.

Overview

Both public and private sector organizations are looking to modernize their IT and move quickly to the cloud. Understanding best practices and the organizational models of first adopters can educate decision makers about best practices for their enterprise.

Organizations, particularly governments, can find accreditation of cloud service offerings (CSOs) a challenge. This is because accreditation can initially delay cloud usage if the organizational model is too laborious or is seen as an onerous obstacle to cloud adoption and cloud first policies.

> An **organizational model** refers to the institutional and bureaucratic structures developed to support and implement programs of accreditation. Governments must develop their organizational models within the context of larger governmental bodies and traditions. The models presented in this paper include: centralized, decentralized, and hybrid.
>
> **Accreditation programs** refer to the set of international standards, certifications, and accreditations used independently of the organizational model chosen.

When considering accreditation, there are multiple options to consider including leveraging existing standards, establishing accreditation reciprocity, and creating a new accreditation program. Tailoring organizational models, the institutional structures developed to support accreditation, to the unique aspects of a government or company and employing internationally accepted accreditations can balance ease of adoption with security, risk management, and compliance requirements. Internationally recognized and widely used certifications and attestations, such as ISO 27001[1], SOC[2], and PCI[3] provide a robust set of security domain coverage for cloud services.[4] In fact, there is considerable overlap (around 80%) in the security objectives across these certifications. Regardless of geography, or where it is accredited, a hyperscale cloud provider addresses these common security practices and controls across its respective enterprise. These controls are validated through independent assessments of the same standards/certifications referenced in the NIST Cybersecurity Framework.

This provides commonality and global applicability of security objectives, offers predictability, efficiency, and easy and economical scaling options.

Public sector first movers in establishing cloud accreditation programs such as the UK, United States, Singapore, and others have chosen different organizational models to

facilitate cloud adoption. (See Appendix: First Movers in Cloud Accreditation for details about the implementation of these countries' cloud accreditation programs.) The national bodies in these governments who are charged with cloud adoption policies have considered the range of security risks and are using their initial experiences to improve their models continuously. In doing so, examples of best practices and lessons learned emerge which should be considered as organizations develop their own organizational models for cloud adoption. Each model has benefits and risks as differences between countries have naturally led countries to structure their program to meet the requirements of their government. However, regardless of the organizational model used, there are principles that are broadly applicable to minimize risk, avoid redundancy of requirements and processes, and keep costs down.

This paper covers examples of public sector organizational models in practice today, best practices for cloud accreditation, and an analysis of first movers' approaches to cloud accreditation.

Governments should develop an accreditation program that allows their organizational model to capitalize on structural efficiencies and effectiveness. This can be done if governments do the following:

- **Facilitate the speed of cloud adoption.** Streamlining procedures and accreditation to reduce unnecessary redundancy can decrease the time to accreditation.
- **Maintain reasonable and manageable cost for both the organization (government and private sector) and the CSP.** Ultimately, higher costs cascade down to customers. However, efficient processes can keep costs down, promote access, and drive value for CSP customers.
- **Balance availability of third-party auditors and growth of talent.** Use of third-party auditors can create the bandwidth to increase speed of cloud accreditation by allowing organizations to focus resources on other aspects of accreditation. However, it is also important for organizations to maintain enough in-house expertise for oversight and to make critical risk decisions.

In choosing an organizational model, organizations should choose a model that they can tailor to highlight these attributes.

Cloud Accreditation in Practice Today: Decentralized, Centralized and Hybrid Models

Accreditation is essentially a risk management decision that the authorizing government or company will have to make based on the results of the assessments performed on the cloud service provider. An accreditation program is the set of international standards, certifications, and accreditations used, independent of the organizational model chosen. Private industry can leverage the accreditation programs developed by governments. Accepting CSOs authorized through a government accreditation process creates efficiencies in a company's internal processes, reducing cost and time to adopt new services. An organizational model consists of the institutional and bureaucratic structures that organizations develop to support and implement programs of accreditation.

Three general organizational models to cloud accreditation have emerged differentiated by who determines and approves the risk profile. Determinations of risk occur when organizations prioritize the acceptance and implementation of some controls over others. Organizational objectives are usually the key factor of these determinations.

These models correlate loosely with varying levels of speed and flexibility in the accreditation process. However, the unique characteristics of the country, government, or environment in which these models are implemented also have an impact.

Responsibilities for Risk Management in the Cloud

As governments recognize the benefits of cloud computing and establish policies to improve, transform, and/or deliver new government services to the public leveraging technology, it is important to ensure due diligence in reviewing and assessing cloud service providers' (CSP) ability to meet resiliency, security, and compliance objectives. A key aspect of due diligence is achieving a thorough understanding of the shared responsibility model between the CSP and the consumer to create a more secure, robust, and transparent environment for agency consumers from day one.

In the decentralized model, there is no central entity or agency established to make risk decisions on behalf of the government or company, but rather, each individual entity within the organization adopts and accredits the cloud service. This is the key distinction from the centralized model, where a single, central entity is responsible for determining

risk. In the third model, a hybrid model, both a central entity and individual agencies play a role in risk calculations and authorization decision.

Regardless of the model chosen, clear understanding of the shared responsibility model, which identifies customer and CSP responsibilities, will assist organizations to define and meet their specific security, risk, and compliance requirements.

See Appendix: First Movers in Cloud Accreditation for a detailed description of how public sector first movers apply these models.

Decentralized Model

A decentralized model, such as the one used by the UK (see appendix for details on UK model), allows for a tailored approach, allowing each public sector agency or department the flexibility to adopt the risk profile required by its mission or organizational requirements. By delegating risk ownership down to each entity, they can choose international accreditations based on their priorities, accounting for specific organizational objectives. Generally, this approach facilitates speed of adoption. If necessary, enterprise requirements not already addressed by existing standards and accreditations can be met by developing additional tailored requirements. However, achieving such flexibility may increase overall overhead by requiring specialized IT expertise in each agency or department within the enterprise that makes authorization decisions.

Centralized Model

A centralized authorization model standardizes security accreditation across the enterprise. Risk decisions are largely determined in a central office according to an agreed upon set of criteria often designed to incorporate the requirements of a variety of departments or agencies at the highest level of security. Although, in some circumstances, this may add time to initial accreditation, it can also set the foundation for efficiency gains in the long term as agencies across the enterprise can use CSOs that gain accreditation in such a model with minimal additional effort. However, agencies with narrowly tailored missions may find it unnecessary and challenging to adhere to the broad set of requirements usually found in a centralized model. This model may not be a good fit for agencies who only require either a narrower set of controls or compensating controls to meet their objectives.

There are different ways to implement the centralized model in the public sector. Two examples are:

1. A central organization publishes or maintains the accepted standards and the CSP attests to the relevant controls. The CSP publishes the result but there is no requirement for a formal government review or authorization. This is the approach used in Singapore and Germany.
2. A central organization both publishes standards and runs a formal review process for CSPs to gain authorization for their service. The United States' Federal Risk and Authorization Management Program's (FedRAMP) Joint Authorization Board (JAB) pathway uses this model.

Hybrid Model

A hybrid model integrates both the centralized and decentralized models, taking attributes from both. For example, the U.S. FedRAMP model is a hybrid model that contains two pathways: a decentralized path (agency authorization) and a centralized path (the JAB). Moving from Provisional-Authority to Operate (P-ATO) to Authority to Operate (ATO) can also be considered decentralized as it also allows agencies to add considerations for mission unique requirements.

Two key differences in the models are:

- who makes decisions about risk
- how to determine standardization around security criteria

In a hybrid model, the resources required to reach consensus among multiple decision makers also adds an additional burden. In a decentralized model, even if there is national centralized guidance provided, decisions about risk tolerance occur in a decentralized, delegated manner to account for unique mission requirements. A centralized model manages risk decisions collectively. This does not imply that organizations are not relying on internationally accepted standards, certifications, or accreditations. Rather, risk acceptance decisions are made by the organization and/or individual who hold(s) the ultimate responsibility for system risk.

Regardless of the organizational model employed, outlined below are recommended best practices when instituting a program of accreditation.

Best Practices for Cloud Accreditation

In examining early adopters' models, we identified best practices, which maximize efficiency, scalability, and cost reduction while maintaining the benefits of security gained by cloud adoption. It is imperative that departments and agencies gain a clear

understanding of their own security responsibilities compared to those of the CSPs in a shared responsibility model.

To balance security and speed of adoption, start with internationally recognized accreditations and determine any new requirements based on additional needs. It is critical to add requirements only if they provide value beyond what existing auditing schemes already achieve. For example, in the case of national security systems (NSS) and national security information. NSS authorizations should fully leverage existing authorizations and provide a risk-based justification for additional or stricter requirements supported by data or specific use cases. Therefore, new requirements and certifications, which are unique to a government, country, or sector, should be added only if they provide additional insight into current practices beyond what is already achieved by existing accreditations.

Government Participation in Standard Setting

If national governments uncover requirements not already addressed by international standards, they should consider working with international certification organizations (for example, the International Organization of Standards) to have their requirements added to international standards. This has the potential to make technology available to local consumers, both in the public and private sectors, more quickly than creating local certifications.

Another way to balance security and speed is through reciprocity between countries, sectors, and companies with comparable risk profiles. These risk profiles can occur at the organizational, system, or information level. Both public and private sectors use data classification schemes as a means to inventory, categorize, and prioritize cloud-ready workloads based on risk profiles. Through impact assessments that take into consideration the sensitivity, including confidentiality, integrity, and availability of data, cloud adoption can begin with non-sensitive or public data. This approach will also enable organizations to learn and experience commercial cloud services at lower risk while preparing to migrate additional data in the future.[5]

Additionally, organizations should consider relying on third-party auditors by verifying their reports, rather than duplicating their assessments, as it enables speed of adoption without sacrificing security.

As programs mature, practices will evolve but the current best practices are detailed in the following sections.

Understand Shared Responsibility

There are specific and oftentimes distinct roles, responsibilities, and obligations of the customer in the context of cloud computing risk management and shared responsibility. The CSP and the customer have responsibilities for different aspects of the cloud system. Therefore, both parties must implement a set of practices to secure sufficiently their respective environments. More specifically, CSPs operate, manage, and control the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating systems and other associated application software. For instance, it is incumbent upon the agency to appropriately classify their data (i.e., low, moderate, high) or enforce policies managing user account access because a CSP would not have access to customer data to perform these functions. This is important to help ensure the execution of cloud users' responsibilities rather than assume the CSP has undertaken them. Even in the centralized organizational model, where accreditation decisions are made in a central office, each implementing entity must understand their role and responsibility with respect to the shared responsibility model.

Roles and Responsibilities for Secure Cloud Adoption

A secure and transparent environment for customers requires shared responsibility between the CSP and customers from day one. When accrediting a CSP to host government workloads, it is important to perform the accreditation from the perspective of the government agencies. However, agencies must recognize that the scope of the accreditation only covers the responsibilities of the CSP, not those of the cloud users, (that is, the government departments and agencies). Agencies also need to be held to a high security bar for the cloud environments they manage and accountable for the effective implementation of customer security activities.

Recognize and Accept International Certifications

To optimize for trustworthiness, consistency, and repeatability, a cloud accreditation program should leverage international standards to the extent possible. If there are security challenges that require country or sector-specific certifications not included in internationally-recognized standards and regimes, the additional certifications should focus only on requirements that are unique from, rather than redundant to, current international certifications. In the event of additional requirements, governments and

industries should consider working with international organizations to incorporate the additional requirements into international standards rather than developing unique or domestic standards. Doing so will reduce the cost of implementation and accelerate cloud adoption without compromising security. As stated earlier in the background section, internationally recognized certifications and attestations, such as ISO 27001, SOC, and PCI offer a considerable overlap (i.e. ~80%) in their security objectives and domain area coverage. One-off security accreditation programs can introduce risks (known and unknown) as their processes can be unpredictable, less mature, and the security value limited. Governments such as Germany and Singapore have all adopted the ISO/IEC 27001, ISO/IEC 27017, and ISO 27018 as the baseline requirements in their respective accreditation schemes.

Imposing security requirements above what existing accreditations cover can lead to redundancy, focus on documentation, and increases in compliance costs, while not improving security outcomes. Therefore, adding new country or sector unique requirements and certifications should only occur when they provide additional insight into current practices beyond what existing audit regimes achieve. Continuous improvement requires remaining aware that international standards evolve over time, and it may be necessary to incorporate changes into an organization's existing accreditation program.

International standards provide an important trusted baseline for interoperability, allowing for international cooperation as well as cooperation between sectors, across agencies, and among levels of government (national, state, local). In particular, cooperation between different law enforcement agencies or militaries requires common standards to facilitate interoperability and joint mission execution. Without such a baseline, operational cooperation is a challenge.

Leverage Third-Party Auditor Assessments

Relying on a qualified third-party assessor to perform the security assessment and attest that the CSO conforms to the agreed upon standards allows a program to scale. Rather than duplicating their work by "auditing the auditor," leveraging the audit and associated artifacts of accredited third-party auditors to the extent practicable increases efficiency and reduces redundancy. This enables an organization to scale their program and keep pace with CSPs that are regularly innovating new services and features. In many instances, public sector entities cannot take advantage of services readily available to the commercial sector unless offerings are government-accredited- a process that can often take over six months. However, it's possible to shorten this timeline by identifying and improving process inefficiencies and leveraging audit work

already performed by accredited third-party assessors. Even in a decentralized model, this helps alleviate the requirement of having specialized expertise in multiple areas of an organization. By recognizing third-party auditors as the primary certifier for assessing whether a CSO is meeting international standards, the burden on an individual organization is oversight rather than reassessment, a responsibility that requires significantly less resources.

Establish Reciprocity

Regardless of the model used, employing widely accepted accreditations allows a company or government to reuse (establish reciprocity), instead of "redo." If a CSO is accredited using a widely accepted standard, this allows other organizations to accept previous certifications or re-use assessments, adding only their unique mission requirements, if necessary. The potential effects of widespread accreditation reciprocity across a government or company are increased efficiency, decreased costs, and ability to scale quickly.

Example of Cooperation

An example of current bilateral accreditation cooperation is New Zealand and Australia. New Zealand uses AWS's Asia Pacific (Sydney) Region and recognizes Australia's Information Security Registered Assessors Program (IRAP) accreditations. This allows New Zealand to bring new services online more quickly and at less expense if they have already been through Australia's IRAP accreditation.

As countries fully leverage the potential of the cloud by utilizing centralized infrastructure outside their geographic boundaries, they should consider partnering with countries who host AWS infrastructure and neighboring countries or industries with similar privacy, data protection and cybersecurity laws and requirements. This can be done through bilateral or multilateral accreditation reciprocity agreements. When based on international standards, such reciprocity can be a force multiplier of resources, efficiency and cost savings without degrading security. Bilateral or multilateral cloud accreditation reciprocity agreements can decrease an organization's time to onboard new CSOs while increasing their capacity to do so. Kuwait's MOU with Bahrain on cloud cooperation is a good example of a vehicle to codify such an agreement.[6]

Conclusion

Ultimately, the model chosen by an organization depends on a multitude of factors unique to that country, sector, or company. However, examining the range of options available is helpful to understanding that, regardless of the model chosen, there are key elements that can facilitate the success of a program without compromising security or unnecessarily increasing costs. These elements include integrating international standards which allows for reciprocity between organizations, focusing on an outcome-based approach and leveraging the work of third-party assessors to the extent possible, and understanding the responsibilities of each actor for security.

Appendix: First Movers in Cloud Accreditation

The approaches described in this appendix represent different models with guidance provided by the national government. Each model has benefits and challenges that are instructive for organizations preparing for cloud adoption. For example, FedRAMP is very resource-intensive which makes it cost prohibitive for many governments considering replicating it.

Decentralized Model

United Kingdom's 14 Principles

The United Kingdom, a first mover in cloud adoption, has an organizational model based on the Cloud Security Guidance published by the UK's National Cyber Security Centre (NCSC). The Cloud Security Guidance lists 14 principles for public sector and enterprise organizations to consider when evaluating cloud services.[7] Organizations then determine which of the principles are important, and how much (if any) assurance the users require in the implementation of these principles.

These 14 principles are a risk management approach that includes the major factors to consider when evaluating a cloud offering. The defining element of this decentralized model is the delegation of decisions about which principles are most important. Organizations then make decisions based on their risk tolerance and mission.

The NCSC provides recommended guidance for implementing the 14 principles. The guidance includes eight steps to identify cloud services, which are suitably secure for an organization's intended use. The initial steps, which allow users to determine the most relevant of the 14 Cloud Security Principles, are:

- **Know your business requirements** and identify acceptable and unacceptable organizational risks.
- **Understand your information** including identifying the information that will be in the cloud and the legal and regulatory implications.
- **Determine relevant security principles** based on analysis from the first two steps and the planned use of the service.

The five remaining steps include understanding how the Cloud Security Offering (CSO) implements the pertinent principles and the level of assurance the CSO offers for their implementation. NCSC also recommends identifying additional mitigations, which the organization can take to reduce risk and determining whether any outstanding risks are acceptable to the risk profile the organization is seeking. Finally, the NCSC concludes that periodic reviews are necessary to determine whether the CSO still meets the business and security needs of an organization.

Best Practice

- **Understand shared responsibility.** NCSC implementation guidance emphasizes agency responsibility to securely configure as a service user.

Centralized Model

Singapore's Multi-Tier Cloud Security Singapore Standard (MTCS)

Singapore's Information Technology Standards Committee (ITSC) for CSPs developed the Singapore Multi-Tier Cloud Security (MTCS) Singapore standard (SS584). CSPs can apply SS584 to meet differing cloud user needs for data sensitivity and business criticality. MTCS seeks to drive cloud adoption across industries by providing clarity around the security provisions of CSPs, while also increasing the level of accountability and transparency from CSPs.

MTCS certification adopts the ISO standards accreditation approach, whereby the accreditation body is Enterprise Singapore (ESG), (previously known as SPRING Singapore), and the Conformance Assessment Body (CAB) (also known as Certification Body), are companies accredited by ESG to validate CSP compliance with MTCS standards. Alongside certification, CSPs must produce a standardized self-disclosure document. This document creates a consistent disclosure format on services offered and enables users to discern services uniformly across various CSPs. The disclosure areas include, but are not limited to:

- data retention

- data sovereignty
- data portability
- liability
- availability
- business continuity plans and disaster recovery
- incident and problem management

Best Practices

- **Recognize and accept international certifications**, including ISO 27001.
- **Leverage third-party auditor assessments** by accepting independent audit reports completed by accredited third-party assessor and using the SOC report as a tool for verification.

Germany's C5 Cloud Security Standard

Since 1996, the German Federal Office for Information Security (BSI) has issued IT security standards. Based on ISO 27001, BSI developed the Cloud Computing Compliance Controls Catalog (C5), which defines a cloud-focused baseline security standard that looks at both the design and effectiveness of a CSO.

C5 approval is mandatory for the public sector offerings. The commercial sector has also adopted C5, as it previously did with the German IT-Grundschutz, another baseline security approach. Having C5 certification is a requirement for a CSP to sell in Germany.

C5 requires an attestation report from an independent third-party assessor. By using an independent third party, the report implicitly contains the accountability and reliability of the third-party assessors mandate as professional accountants.

Best practices

- **Recognize and accept international certifications** by basing its standard on ISO 27001.
- **Leverage third-party auditor assessments** by requiring an attestation report from independent third-party assessor.

Hybrid Model

United States' Federal Risk and Authorization Management Program

The Federal Risk and Authorization Management Program (FedRAMP) is the United States Government model. FedRAMP aspires to provide federal U.S. agencies with "a cost effective, risk-based approach for the adoption and use of cloud services" based on the motto, "do once, use many times."[8] In this model, significant upfront investments enable future efficiencies.[9]

FedRAMP provides a pool of trusted cloud services. Third-party assessment organizations (3PAOs) have assessed and verified these services, which have been accredited, or authorized, by the adopting agency. Based on NIST Special Publication 800-53 Rev. 4 security controls, FedRAMP provides CSPs two paths to accreditation: JAB provisional authority to operate (P-ATO) or via individual agencies' full ATO.

Path 1: JAB

The JAB is headed by the Chief Information Officers (CIOs) from the Department of Defense (DoD), Department of Homeland Security (DHS), and U.S. General Services Administration (GSA). It has limited capacity each year to authorize new CSOs. Therefore, CSPs must show broad demand for their services for the JAB to consider accreditation.

The JAB pathway involves CSPs working with a 3PAO who attests to the CSO's readiness for the authorization process and subsequently working with the JAB technical reviewers (TR) to introduce them to new services and infrastructure and/or changes to the current infrastructure. The JAB process involves extensive security assessments developed by the 3PAO and CSP, plans to manage residual security risks, a deep dive into the service offering, system offering, architecture, capabilities and risk posture. Once the CSP has satisfactorily addressed and remediated all JAB TR comments, a provisional authorization to operate (P-ATO) is issued. However, to receive final authorization, each agency is responsible for CSOs used within their environment so each must still review and issue an ATO prior to use.

Path 2: Individual Agencies

Alternatively, CSPs can pursue authorization by entering into a formal partnership with an Agency. The Agency approves, and a 3PAO tests, a security blueprint of their system developed by the CSP. The process is similar to the JAB process with two key

distinctions: (1) The individual agency reviews the security plans versus the JAB board and (2) there is no P-ATO.

If the Agency accepts the risk associated with the use of the system, they provide the ATO. The FedRAMP program management office then reviews the CSO's package in collaboration with the Agency, CSP, and 3PAO and makes a decision about FedRAMP authorization.

Regardless of the path, CSPs must provide monthly continuous monitoring deliverables to the authorizing body and engage a 3PAO to complete an annual security assessment to maintain an acceptable risk posture. FedRamp uploads this annual assessment to a secure FedRAMP repository.

However, in 2016, five years after the start of the FedRAMP program, FedRAMP reported four requests from 85 stakeholders:

1. Greater certainty of success
2. More transparency in the process
3. Faster speed to authorization
4. Predictability in timeframes for authorization.[10]

Best Practices

- **Leverage third-party auditor assessments** by accepting independent audit reports completed by accredited third-party assessor.
- **Establish reciprocity** among public sector and industry accreditation programs by implementing a system recognizing FedRAMP and the Cloud Security Alliance STAR Program to reduce the audit burden for CSPs.[11]

Document Revisions

Date	Description
June 2020	First publication

Notes

1 ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments appropriate to ever-changing threat scenarios.

2 Service Organization Controls reports (SOC 1, 2, 3) are intended to meet a broad range of financial auditing requirements for U.S. and international auditing bodies. The audit for this report is conducted in accordance with the International Standards for Assurance Engagements No. 3402 (ISAE 3402) and the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly SSAE 16).

3 The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council (https://www.pcisecuritystandards.org/), which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. PCI DSS applies to all entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers.

4 AWS compliance programs can be found at: https://aws.amazon.com/compliance/programs/

5 For more information on data classification, please see AWS's data classification whitepaper at: https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf

6 https://www.kuna.net.kw/ArticleDetails.aspx?id=2749760&language=en

7 https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

8 2011 U.S. Office of Management and Budget Memo.

9 Approximately six months to receive an accreditation through the Joint Authorization Board (JAB) and often times less for agencies with costs ranging from $350,000 to $865,000 based on a study from one of the largest 3rd party assessment organizations: https://federalnewsnetwork.com/cloud-computing/2017/05/new-report-tries-to-bust-fedramp-myths-about-cost-usage/9

10 https://csrc.nist.gov/CSRC/media//Projects/Forum/documents/aug-2016/wed130_fedramp-lessons-learned_belloli.pdf

11 https://cloudsecurityalliance.org/press-releases/2018/05/14/cloud-security-alliance-announces-fedstar-a-new-joint-certification-system-with-fedramp/