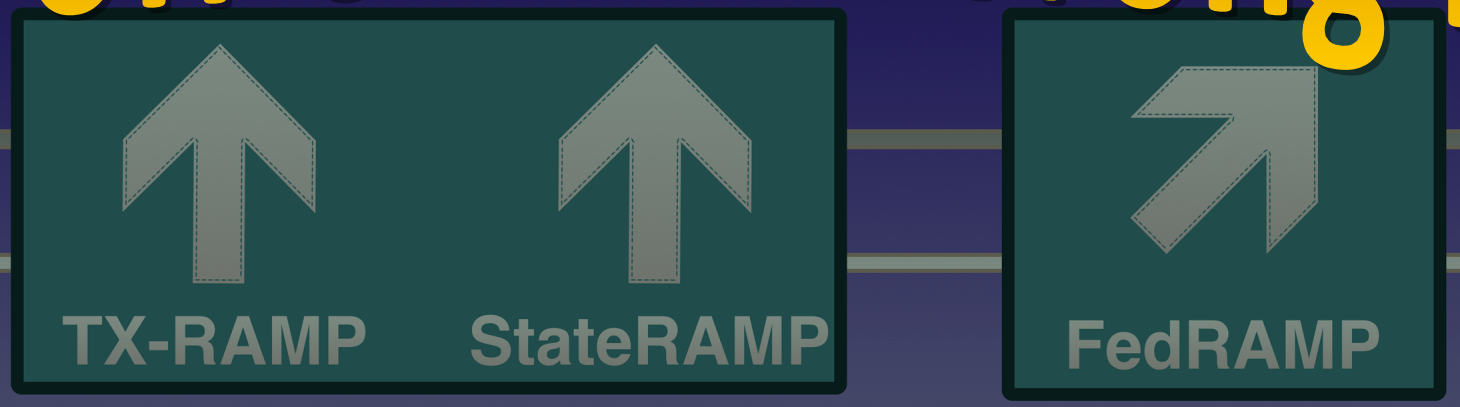
Getting off on the Wrong RAMP



Deconflicting Emerging Compliance Regulations

Jeremy B. Blevins, CISSP, CEH

- Veteran (Alabama Army National Guard) Radio/COMSEC Repair
- Defense Contractor 20+ Years
- College Instructor 4 Years

SENTAR

CALHOUN COMMUNITY COLLEGE

U.S.ARMY SOLDIER FOR LIFE


CALHOUN
COMMUNITY COLLEGE


FAULKNER
UNIVERSITY

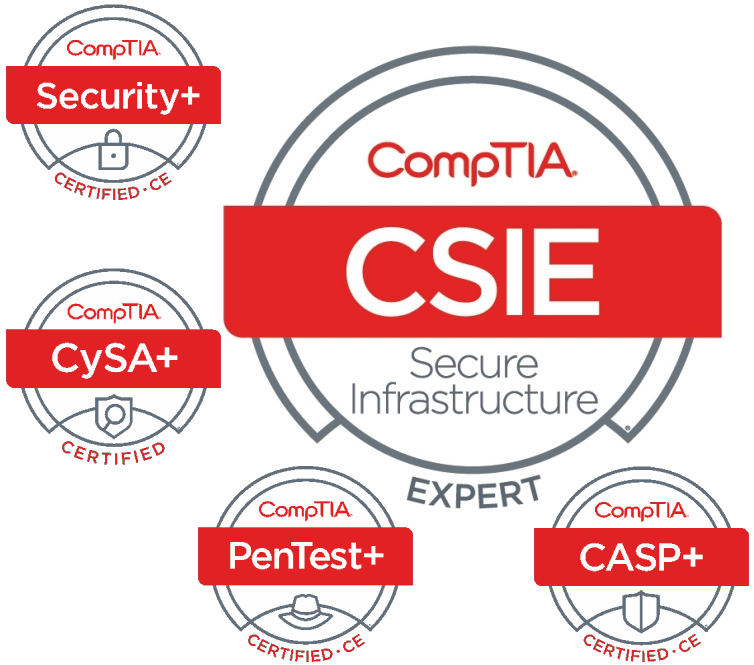

EMBRY-RIDDLE
1926
AERONAUTICAL UNIVERSITY


UTICA
PIONEERS
TM


CompTIA
Linux+
CERTIFIED · CE


CompTIA
Project+
CERTIFIED


CISSP®

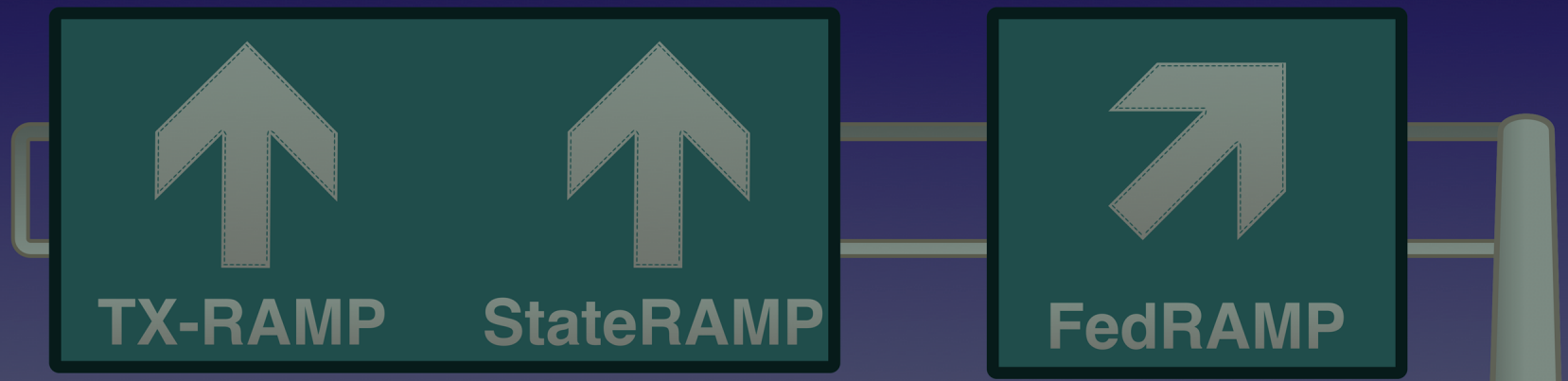

CompTIA
Security+
CERTIFIED · CE
CompTIA
CySA+
CERTIFIED
CompTIA
CSIE
Secure
Infrastructure
EXPERT
CompTIA
PenTest+
CERTIFIED · CE
CompTIA
CASP+
CERTIFIED · CE


CompTIA
Cloud
Essentials+
CERTIFIED


™
C|EH
Certified Ethical Hacker

- **Quick history of Cloud Computing**
- FedRAMP Overview
- StateRAMP Overview
- TX-RAMP Overview
- Reciprocity
- Summary

Bottom Line Up Front



There are several Risk and Authorization Programs (RAMP) that an organization may need to comply with and ascertaining the correct one can be challenging initially. Changes to various state and Federal regulations require organizations to either dedicate resources to stay on top of the changes or to hire outside consultants to perform the task.

Image Source: https://www.ibm.com/cloud/blog/cloud-computing-history

There is no cloud

it's just someone else's computer

Image Source: https://www.awsforbusiness.com/aws-planning-new-east-coast-campus-northern-virginia/


FedRAMP
StateRAMP
DIR
Texas Department of
Information Resources

Top 3 Security Breaches of 2021

1. **Cognyte**
   Database of 5 billion records exposed on the Internet without any password or authentication required to access it – contained aggregated breach data that Cognyte was researching

2. **LinkedIn**
   700 million users' personal data was for sale online – no login credentials, but names, physical addresses and email addresses

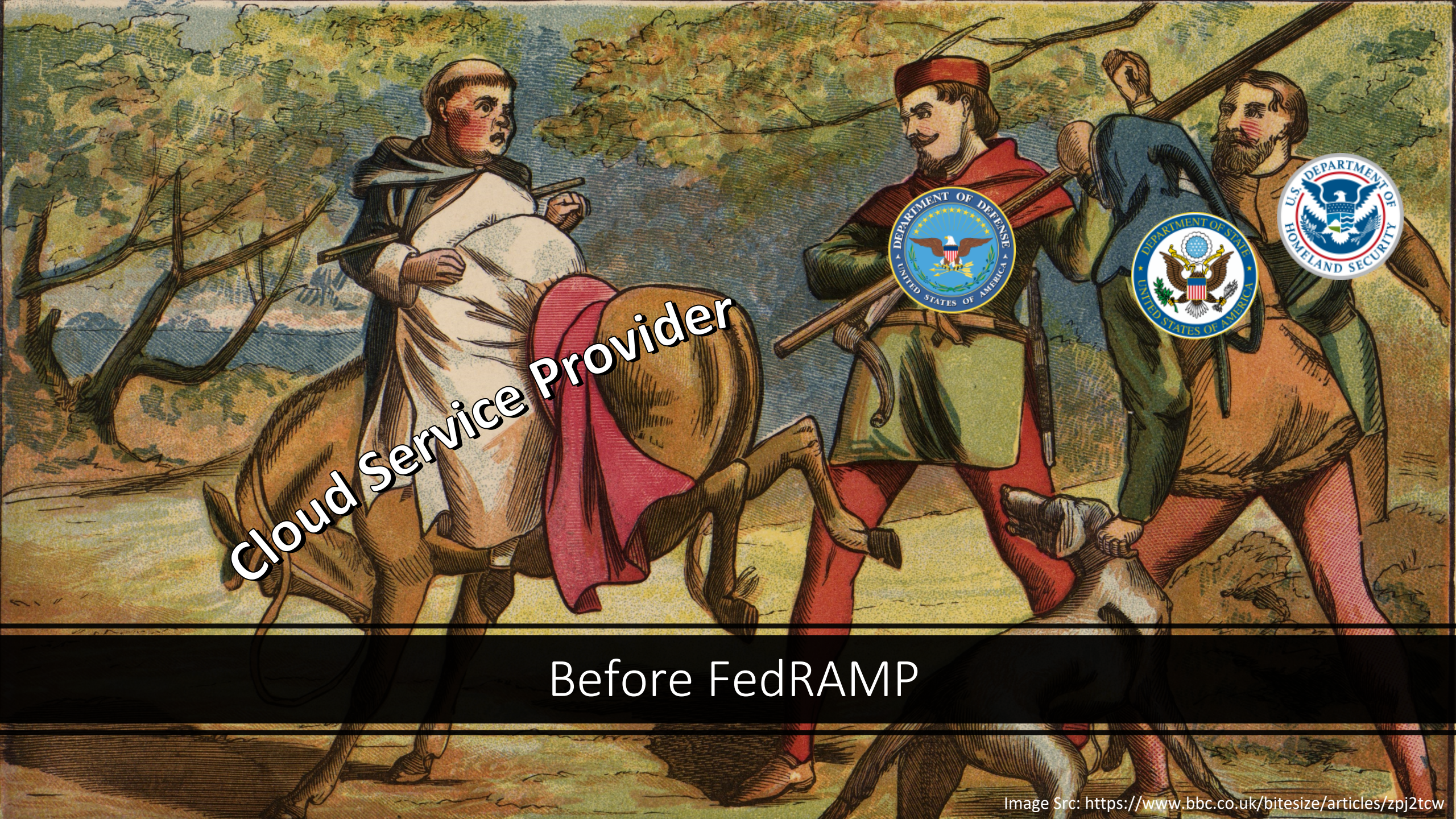
3. **Facebook**
   553 million accounts (106 countries, 32m records from US) including phone numbers

Source: https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021

- Quick history of Cloud Computing
- **FedRAMP Overview**
- StateRAMP Overview
- TX-RAMP Overview
- Reciprocity
- Summary

- Established 2011 to “provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government”

- Cloud Service Providers contract 3rd Party Assessment Organizations (3PAOs) to either Consult in preparation for an assessment or to perform the actual assessment

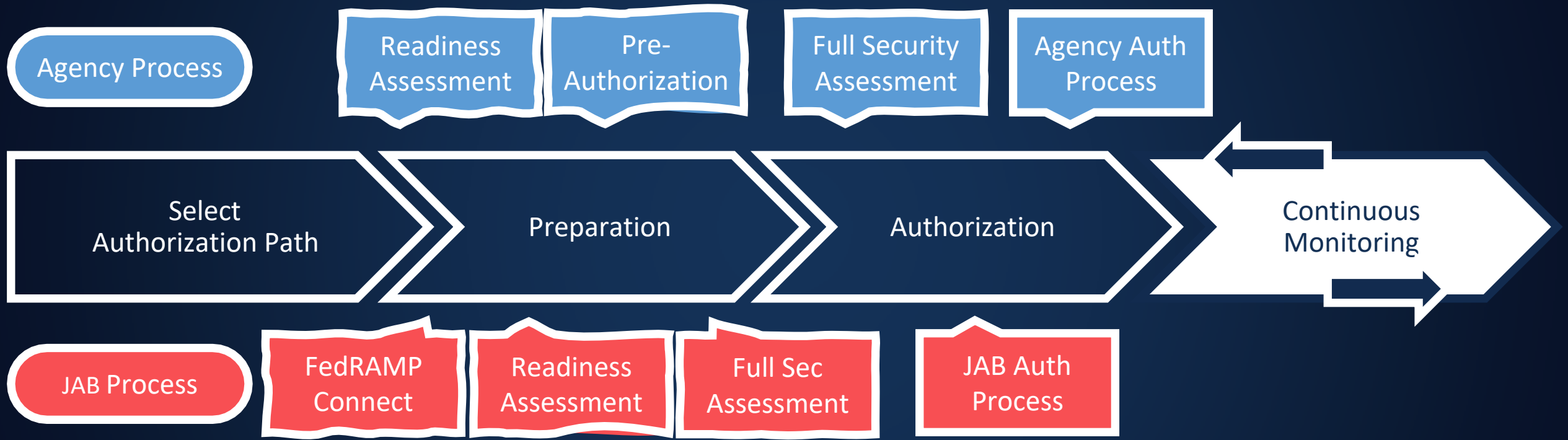


Before FedRAMP

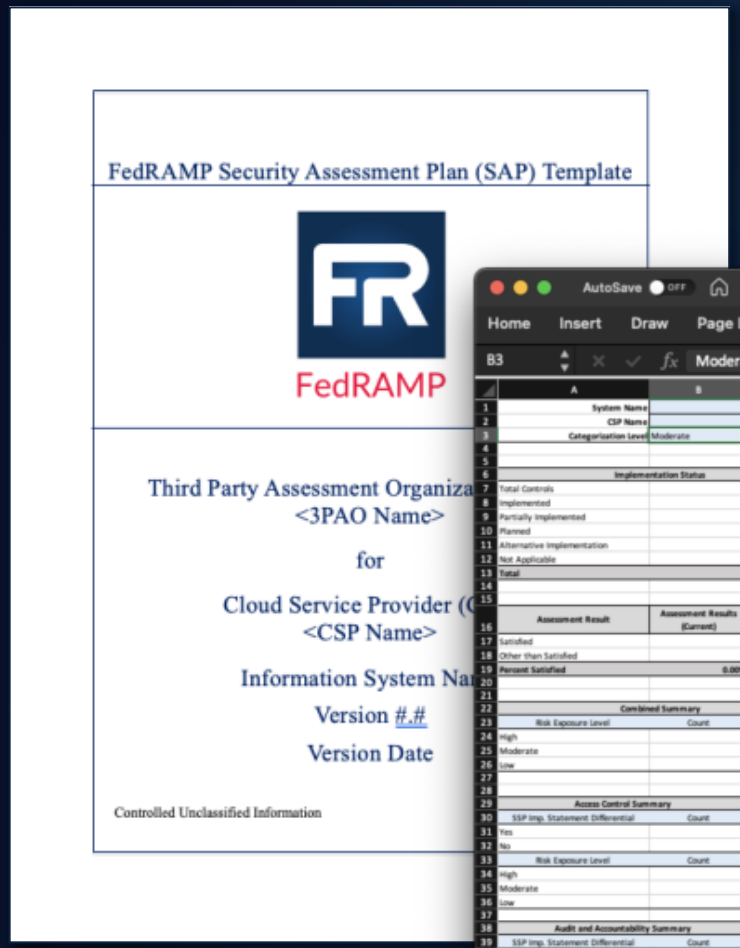
Image Src: https://www.bbc.co.uk/bitesize/articles/zpj2tcw

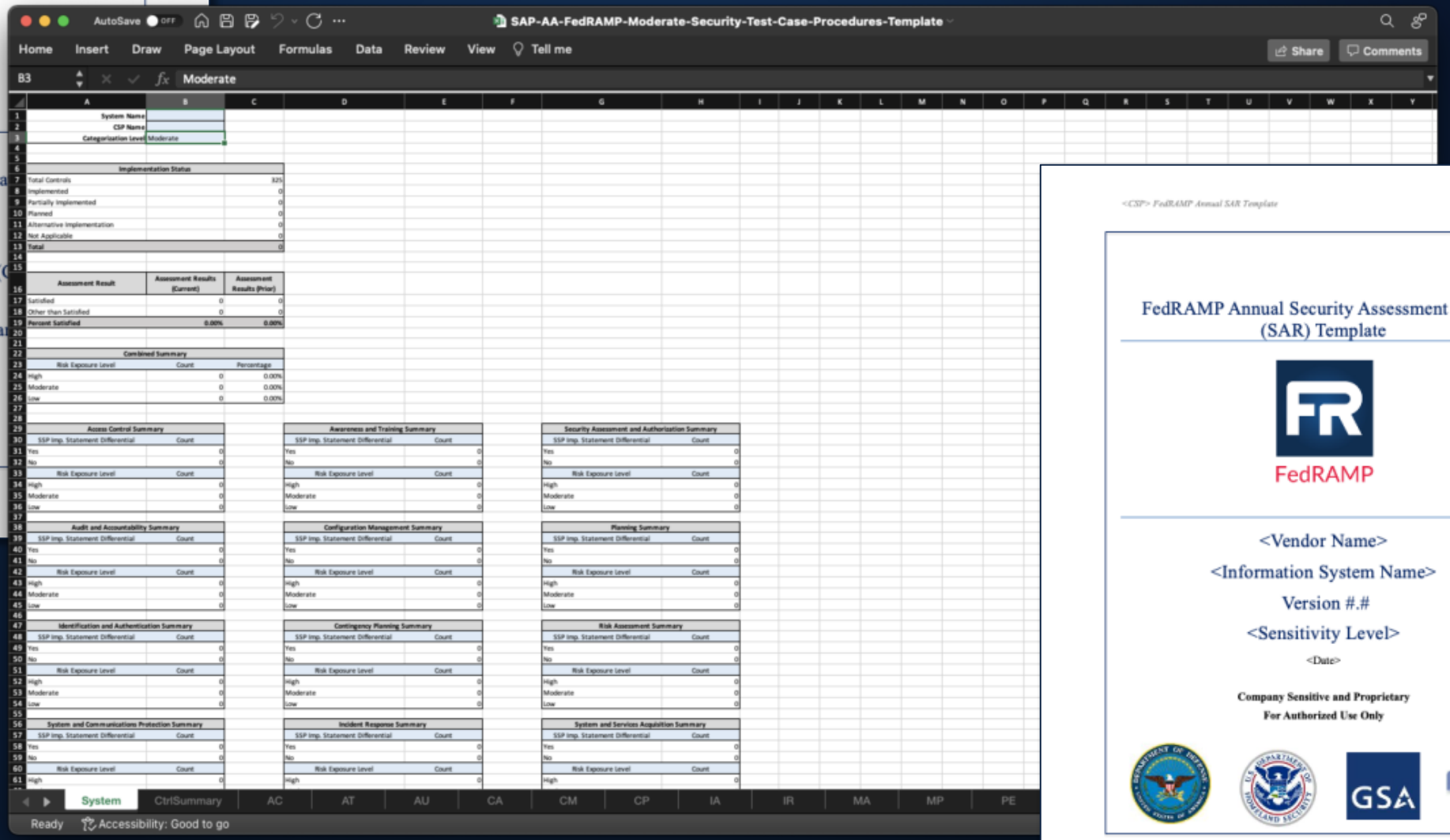
FedRAMP’s guiding principle is reuse:
do once, use many times.

Source: https://www.fedramp.gov/assets/resources/documents/Transcript-FedRAMP-Overview.pdf



Source: https://www.fedramp.gov

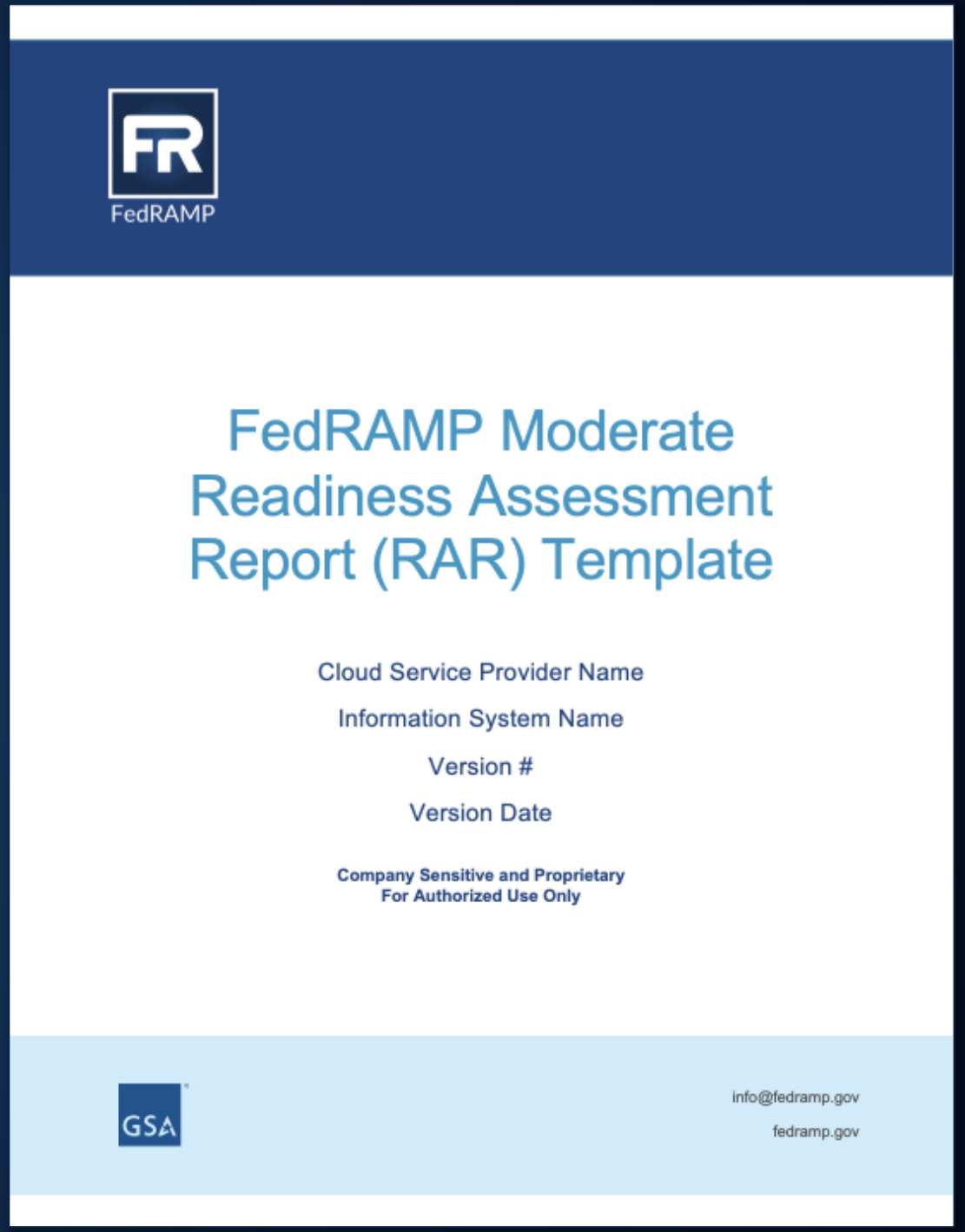

FedRAMP Security Assessment Plan (SAP) Template
FedRAMP
Third Party Assessment Organiza
<3PAO Name>
for
Cloud Service Provider (
<CSP Name>
Information System Na
Version #.#
Version Date
Controlled Unclassified Information


AutoSave
SAP-AA-FedRAMP-Moderate-Security-Test-Case-Procedures-Template
Home
Insert
Draw
Page Layout
Formulas
Data
Review
View
Tell me
Share
Comments
B3
Moderate
System Name
CSP Name
Categorization Level
Moderate
Implementation Status
Total Controls
Implemented
Partially Implemented
Planned
Alternative Implementation
Not Applicable
Total
Assessment Result
Assessment Results (Current)
Assessment Results (Prior)
Satisfied
Other than Satisfied
Percent Satisfied
Combined Summary
Risk Exposure Level
Count
Percentage
High
Moderate
Low
Access Control Summary
Awareness and Training Summary
Security Assessment and Authorization Summary
Audit and Accountability Summary
Configuration Management Summary
Planning Summary
Identification and Authentication Summary
Contingency Planning Summary
Risk Assessment Summary
System and Communications Protection Summary
Incident Response Summary
System and Services Acquisition Summary
SSP Imp. Statement Differential
Yes
No
System
CtrlSummary
AC
AT
AU
CA
CM
CP
IA
IR
MA
MP
PE
Ready
Accessibility: Good to go

<CSP> FedRAMP Annual SAR Template
Date of modification
FedRAMP Annual Security Assessment Report (SAR) Template
FedRAMP
<Vendor Name>
<Information System Name>
Version #.#
<Sensitivity Level>
<Date>
Company Sensitive and Proprietary
For Authorized Use Only
GSA
NIST
Company Sensitive and Proprietary
Page 1

FedRAMP Ready

- Not selected by JAB and not sponsored by an agency
- Optional for Agency authorization, but recommended
- Still gets you listed on the marketplace as ”Ready”



Baseline Security Controls

126	Tailored Low Impact SaaS (LI-SaaS)
125	Low
325	Moderate
421	High

NOTE: FedRAMP Ready requires at least a Moderate Baseline

3rd Party Risk Assessment Organizations (3PAOs)

- Accredited by American Association for Laboratory Accreditation (A2LA)

- Two Modes of Operation
  - Consultant
  - Assessor

Image Source: https://darkknightnews.com/2017/07/29/concept-art-reveals-different-batsuit-designs-batman-v-superman/

Image Source: https://inspirationfeed.com/wp-content/uploads/2015/09/Steampunk-c3p0-by-Anjics.jpg

In the Marketplace!

- CSP products
  - Ready
  - In Process
  - Authorized
- Federal Agencies
- 3PAOs
  - Only 41 in the Marketplace
  - # offerings assessed

- Quick history of Cloud Computing
- FedRAMP Overview
- **StateRAMP Overview**
- TX-RAMP Overview
- Compare and Contrast
- Summary

StateRAMP

- 501(c)6 non-profit organization designed to assist State and local governments in managing 3rd party risk
- Board of Directors comprised primarily of state and local government officials
- Patterned after FedRAMP
- Leverages FedRAMP authorized 3PAOs

StateRAMP

- Three security statuses
  - Ready
  - Authorized
  - Provisional

- Three progress statuses
  - Active
  - In Process
  - Pending

- Quick history of Cloud Computing
- FedRAMP Overview
- StateRAMP Overview
- **TX-RAMP Overview**
- Reciprocity
- Summary

Tx-RAMP DIR Texas Department of Information Resources

- Created in May 2021 by the Texas Legislature; effective January 1, 2022
- Implementation occurs in phases depending on an organization's certification level
- TX-RAMP Certified Cloud Products list similar to FedRAMP Marketplace
- Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM) for TX-RAMP submissions
- TX DIR directly works with CSPs – no 3PAO assessments – you can still consult with a 3PAO, but they aren't involved in the authorization process
- TX DIR takes a holistic approach to certification – remediation plans may be allowed

- Quick history of Cloud Computing
- FedRAMP Overview
- StateRAMP Overview
- TX-RAMP Overview
- **Reciprocity**
- Summary

Reciprocity

- FedRAMP does not accept StateRAMP or TX-RAMP authorizations
- StateRAMP accepts FedRAMP authorizations but not TX-RAMP authorizations
- TX-RAMP accepts all FedRAMP authorizations, but only accepts full StateRAMP authorizations (e.g. TX DIR will will grant a TX-RAMP Provisional authorization for a FedRAMP Ready authorization but not a StateRAMP Ready authorization)

What's the right choice? (Jeremy's Opinion)

- If you have Federal customers – go FedRAMP
- If you don't have Federal customers and are seeking a full authorization – go StateRAMP
- If you don't have Federal customers and are seeking a Ready authorization – and don't do business with Texas – go StateRAMP
- If you only do business with Texas – go TX-RAMP
- If you're fishing in multiple states and are only ready for Ready – do StateRAMP Ready – you still have to have an agency sponsor for TX-RAMP Provisional

- Quick history of Cloud Computing
- FedRAMP Overview
- StateRAMP Overview
- TX-RAMP Overview
- Reciprocity
- **Summary**

Summary

- There is no one-size-fits all solution, but FedRAMP – if you can – provides the reciprocity and the most flexibility
- 3PAOs are required for FedRAMP and StateRAMP – a consulting 3PAO can’t turn around and then perform your assessment, though
- 3PAOs are not part of the TX-RAMP certification process, but they can help you prepare
- The process isn’t going to be cheap, but its cheaper than not doing it right

Thank you!

Jeremy.Blevins@Sentar.com

References

- FedRAMP PMO
- FedRAMP PMO. (2018, November 6). FedRAMP Updates 3PAO Requirements. Retrieved from FedRAMP
- FedRAMP PMO. (2020, March 26). JAB Prioritization Criteria and FedRAMP Connect Guidance, Version 3.0
- FedRAMP PMO. (2022, January 4). FedRAMP Moderate Readiness Assessment Report (RAR)
- FedRAMP. (n.d.). Program Basics. Retrieved from FedRAMP
- Henriquez, M. (2021, December 9). The top data breaches of 2021
- IBM Cloud Team. (2017, January 6). A Brief History of Cloud Computing
- Kelly, M. (2022, May 5). Email Conversation. (J. B. Blevins, Interviewer)
- Kelly, M. (2021, December 16). Tx-RAMP SPECTRIM Overview
- Miller, B. (2021, March 17). How the New StateRAMP Process Will Work for Gov Tech Vendors
- StateRAMP. (2021, May 12). StateRAMP Readiness Assessment Report
- StateRAMP. (n.d.). Frequently Asked Questions
- StateRAMP. (n.d.). Who We Are
- Texas DIR. (n.d.). Texas Risk and Authorizatio Management Program (TX-RAMP)
- VanRoekel, S. (2011, 12 08). Security Authorization of Information Systems in Cloud Computing