Cybersecurity Risk Assessment in the State and Local Government

How Cloud can be an enabler

Maria Thompson
AWS - SLG Cybersecurity Lead

The responsibilities of the CISO

Influence and enable the business

Align security strategy with business strategy

Draft, implement and enforce policies and procedures

Manage security operations

Achieve and maintain compliance

Hire, develop and maintain competent security staff

Oversee organizational risk management

Manage security procurement and engineering

aws

Common challenges

Organizational

1. **Competing priorities** with Business Managers, CIO, IT Program Managers, and others
2. **Inadequate authority** due to position in org chart or lack of executive sponsorship
3. **Insufficient** budget and resources

Common challenges

Security Mission

1. Difficulty in mapping organizational policies to technical and procedural controls
2. Implementing and maintaining security controls in numerous technology platforms
3. Gaps in technical capabilities
4. Lack of visibility, resiliency, and automation
5. Lack of resources to implement defense-in-depth
6. Difficulty in keeping up with emerging technologies, new threats and responding quickly

aws

What State CISOs are saying are the top barriers to security challenges

Source: 2020 Deloitte – NASCIO Cybersecurity Report

Federal Audit challenges

Table 2: Extent to Which Selected Federal Agencies' Cybersecurity Requirements for State Agencies Varied with Each Other and Federal Guidance

	CMS	FBI's CJIS	IRS	SSA
Total number of requirements included in each agency's policy[a]	**281**	**118**	**220**	**61**
Type of variance				
Unique requirements	54	24	5	3
Requirements included in agency policy that other agencies did not include	(19%)	(20%)	(2%)	(5%)
Conflicting parameters	139	72	131	48
Requirements with differences in technical thresholds from at least one of the other selected agencies for a related control	(49%)	(61%)	(60%)	(79%)
Did not fully address guidelines from National Institute of Standards and Technology (NIST) guidance	26	63	22	30
Agency requirements that did not fully address the guidelines from NIST for associated controls and control enhancements	(9%)	(53%)	(10%)	(49%)

Source: GAO analysis of selected federal agencies' data. | GAO-20-123

Note: CMS = Centers for Medicaid and Medicare Services, FBI/CJIS = Federal Bureau of Investigation, Criminal Justice Information Services, IRS = Internal Revenue Service, SSA = Social Security Administration.

[a]We examined a nonprobability sample of 616 cybersecurity controls and control enhancements from NIST Special Publication 800-53. Of the 616 controls, each agency selected a number of these controls to include in its cybersecurity requirements policy. For example, for the control related to unsuccessful logon attempts, an agency is to define the number of consecutive invalid logon attempts by a user during a given time period before a user's account is automatically locked (NIST control AC-7).

"Twenty-four states estimated that the four selected federal agencies conducted at least 188 assessments between calendar years 2016 and 2018 and that the states' best estimates of the total expenditures associated with those assessments ranged from $43.8 million to $67 million" – **May 2020 GAO Report:** *CYBERSECURITY Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States*

aws

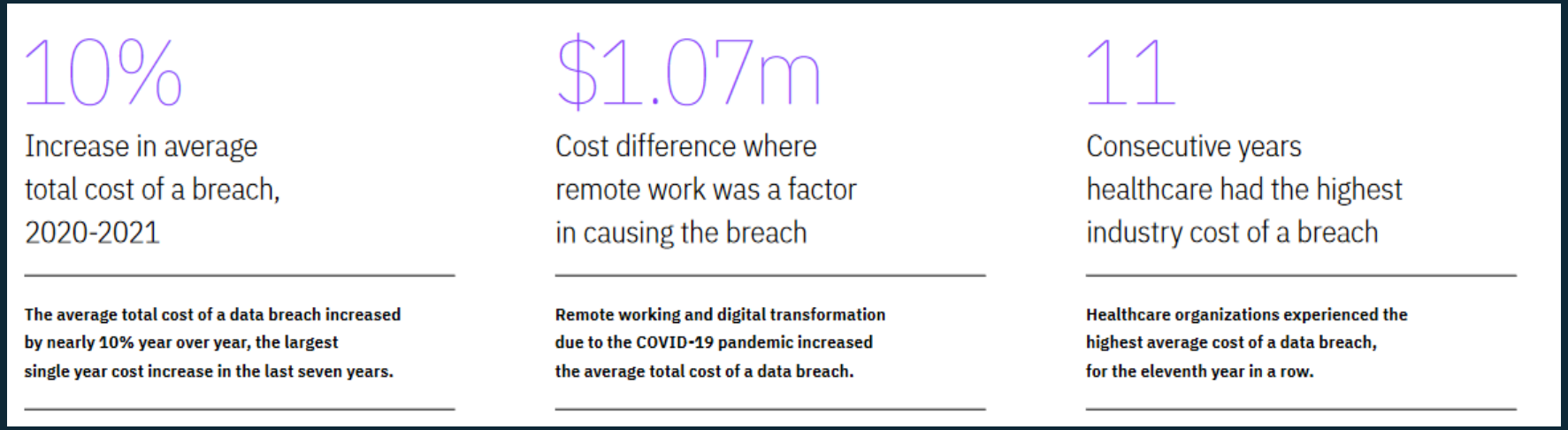
Federal Data Retention challenges

Table 4: Examples of Conflicting Parameters in Selected Federal Agencies' Cybersecurity Requirements for State Agencies

Requirements	CMS	FBI's CJIS	IRS	SSA
Amount of time state agencies should retain audit records,[a] which are individual entries in an audit log related to an audited event	10 years	1 year	7 years	3 years, preferably 7 years
Frequency of assessments of security controls in the information system environment	Annually	Every 3 years	Annually	Did not define a frequency
Frequency of providing basic security awareness training to information system users	Annually	Within 6 months of assignment and biennially thereafter	Annually	Annually
Frequency of reviews and updates to access control policies	Annually	Not applicable[b]	Every 3 years	Not applicable[b]
Number of consecutive login attempts before user is locked out	3 attempts within 15 minutes	No more than five	No more than three within 120 minutes	No fewer than three and no more than five
Frequency of scans for vulnerabilities in the information system	Monthly	Did not specify a frequency	Monthly	Did not specify a frequency
Frequency of review and updates to agency risk assessment policies	Annually	Not applicable[b]	Every 3 years	Did not specify a frequency

Source: GAO analysis of agency data. | GAO-20-123

Cost of a Data Breach Statistics



Source: IBM 2021 Cost of a Data Breach

aws

What Security Assessments look like today

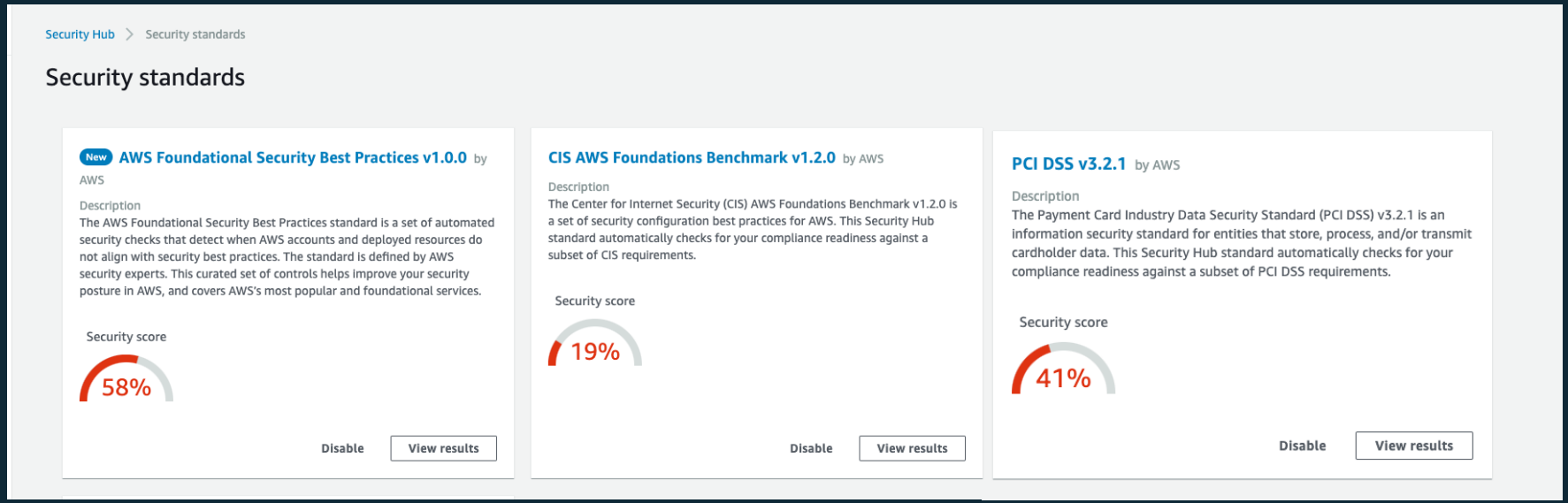
- Ad Hoc or Annually
- Paper based / Manual questionnaires
- Subjective vs. Objective – hard to measure
- Interview style aka resource intensive
- Static vs. Continuous Monitoring
- Costly depending on scope

My CISO 5 Stages of Cloud Journey

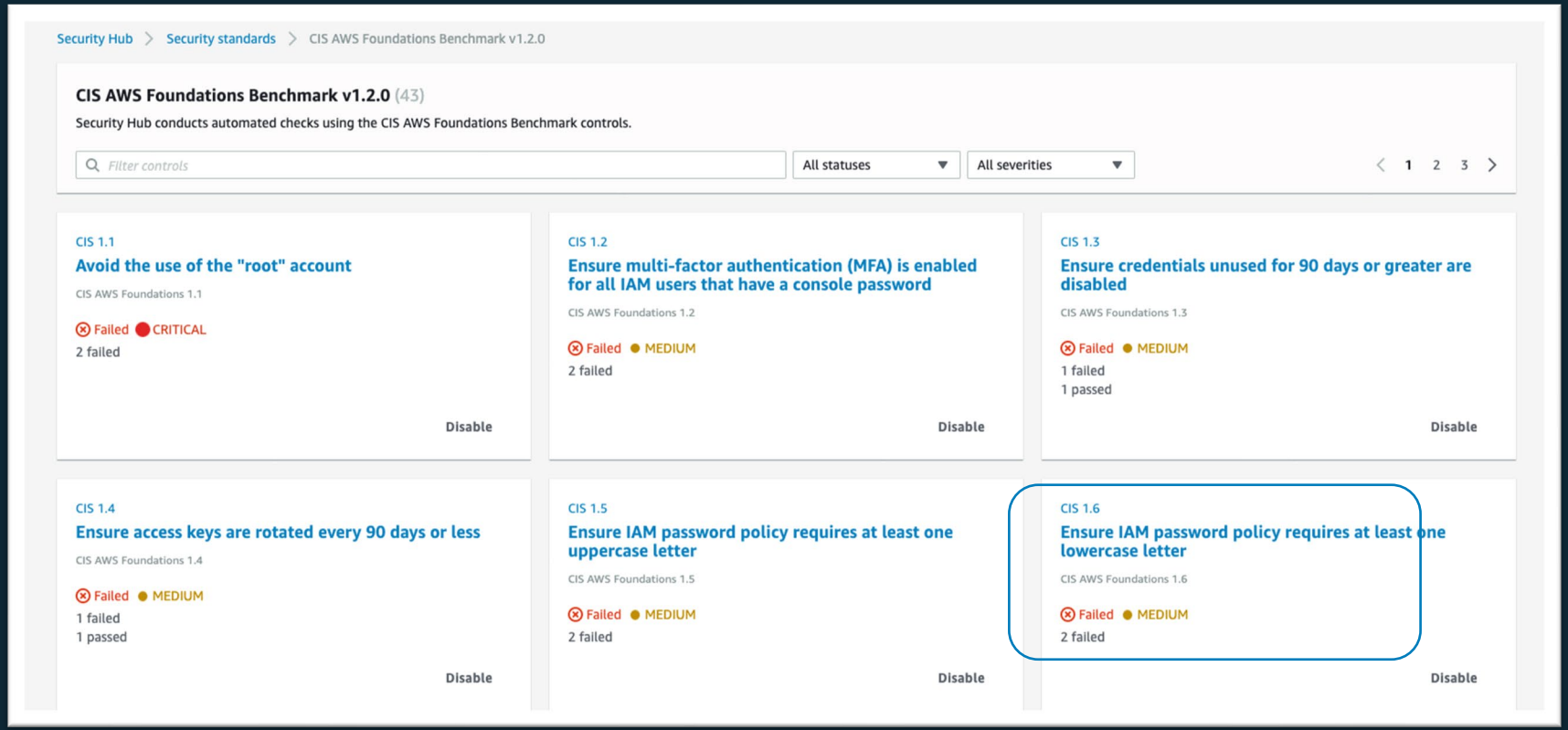
Start with a foundation

Question: How does your organisation's strategy, people, governance and capability define how your security organisation delivers value to the business?

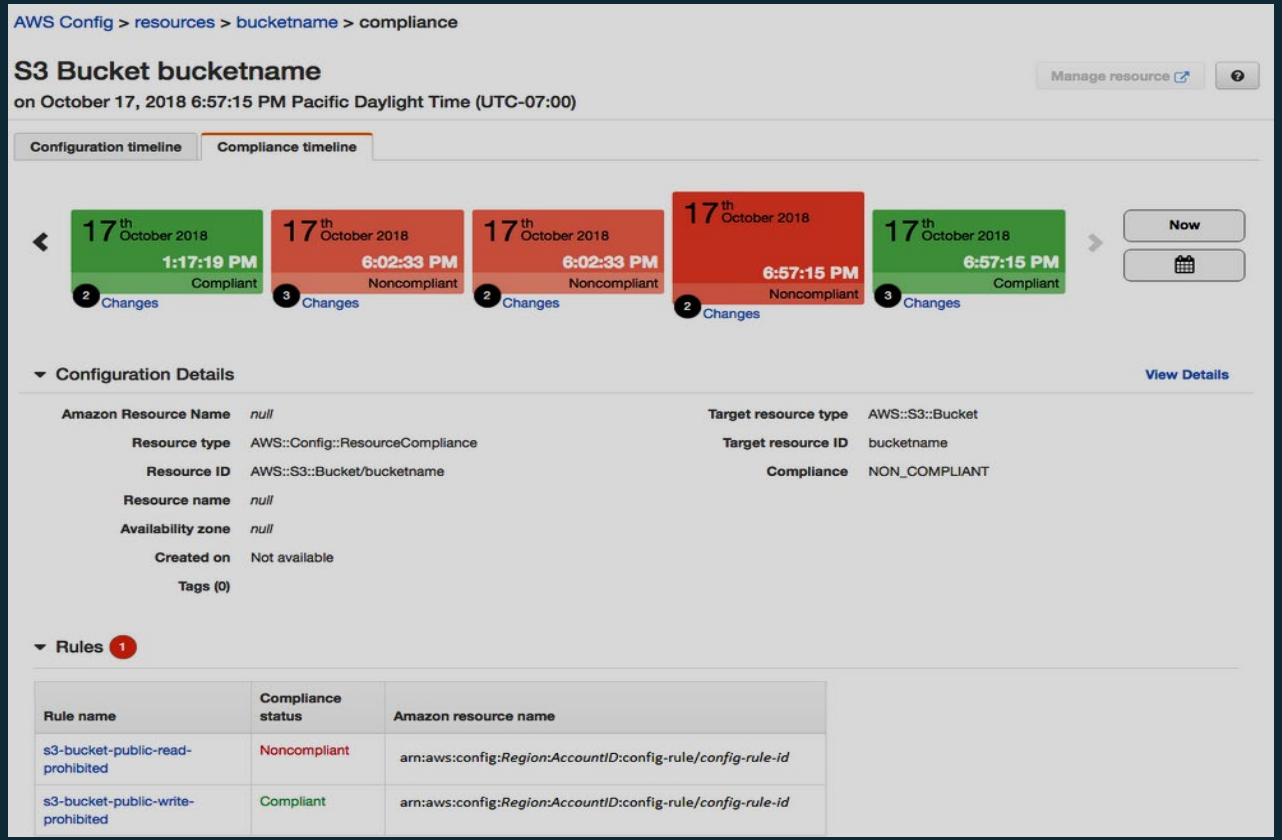
Automated security checks



Compliance standards



Compliance history timeline



Conformance Templates

Operational Best Practices for ABS CCIG 2.0 Material Workloads

PDF | Kindle

Conformance packs provide a general-purpose compliance framework designed to enable you to create se optimization governance checks using managed or custom AWS Config rules and AWS Config remediation Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or com responsible for making your own assessment of whether your use of the Services meets applicable legal ar

The following provides a sample mapping between the ABS Cloud Computing Implementation Guide 2.0 - AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more Implementation Guide controls. An ABS Cloud Computing Implementation Guide control can be related to Refer to the table below for more detail and guidance related to these mappings.

AWS Region: All supported AWS Regions except Asia Pacific (Hong Kong), Europe (Stockholm), and Middle

Operational Best Practices for MAS TRMG June 2013

PDF | Kindle

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Monetary Authority of Singapore (MAS) Technology Risk Managment Guidelines (TRMG) June 2013 and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more Title 21 CFR Part 11 controls. A MAS TRMG June 2013 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable you to align to a subset of MAS TRMG June 2013 design principles.

AWS Region: All supported AWS Regions except Middle East (Bahrain)

Operational Best Practices for Data Lakes and Analytics Services

PDF | Kindle

This pack contains AWS Config rules for Data Lakes and Analytics Services. For more information, see Data Lakes and Analytics on AWS. This Conformance Pack has been designed for compatibility with the majority of AWS regions and to not require setting of any Parameters. Additional managed rules that require parameters to be set for your environment and/or for your specific region can be found at: List of AWS Config Managed Rules.

AWS Region: All supported AWS Regions except Middle East (Bahrain)

See Parameters section for names and descriptions of required parameters.

The template is available on GitHub: Operational Best Practices for Data Lakes and Analytics Services.

https://docs.aws.amazon.com/config/latest/developerguide/conformancepack-sample-templates.html

aws

Open Discussion

a.k.a. the fun part