CSA CONTINUOUS 2021
APAC › EMEA › AMERICAS

Continuous Audit Metrics WG

Metric Catalog

Max Pritikin

Principal Engineer @ Cisco

CSA working group co-chair

Context

Open Certification Framework

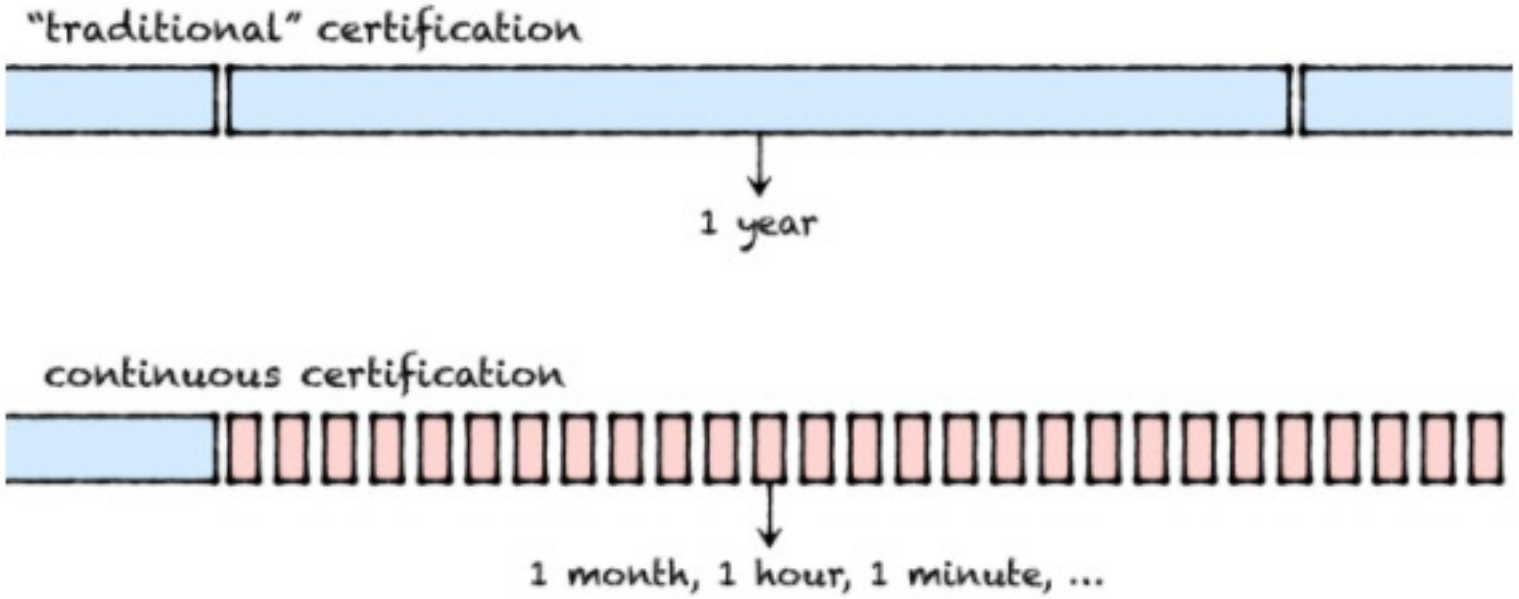
Table 1: STAR Audit Frequency

Level 3 phase2:"develop automated and manual testing of controls to be performed at the expected testing frequency"

STAR Continuous Technical Guidance: https://cloudsecurityalliance.org/artifacts/star-continuous-technical-guidance/

Context

Traditional certification reflects where we were at some time ago. How are we doing now?



Continuous Audit Metrics:

- Improve the quality of audit
- Ensure audit results are relevant and current
- leverage industry strengths

https://cloudsecurityalliance.org/blog/2020/03/20/continuous-auditing-and-continuous-certification/

SMART metrics:

Specific, measurable, achievable, relevant, and time bound

Returns on Investment

- Increase quality & speed of traditional audit
- Improve governance and risk management
- Improve information security management systems
- Improve the information system security

Metrics need to be valuable to the teams operating the systems being measured

Metrics need to be valuable to the teams using them for risk assessment

Operational Privacy: Metrics enable transparency and privacy

"The CSA at no time receives any specific evidence directly generated by the CSP" & STAR Registry posts only a "summary of validated continuous audit results" for the Cloud Service Provider and Customer

Metrics can also provide operational privacy:

CSP's policy is integral:

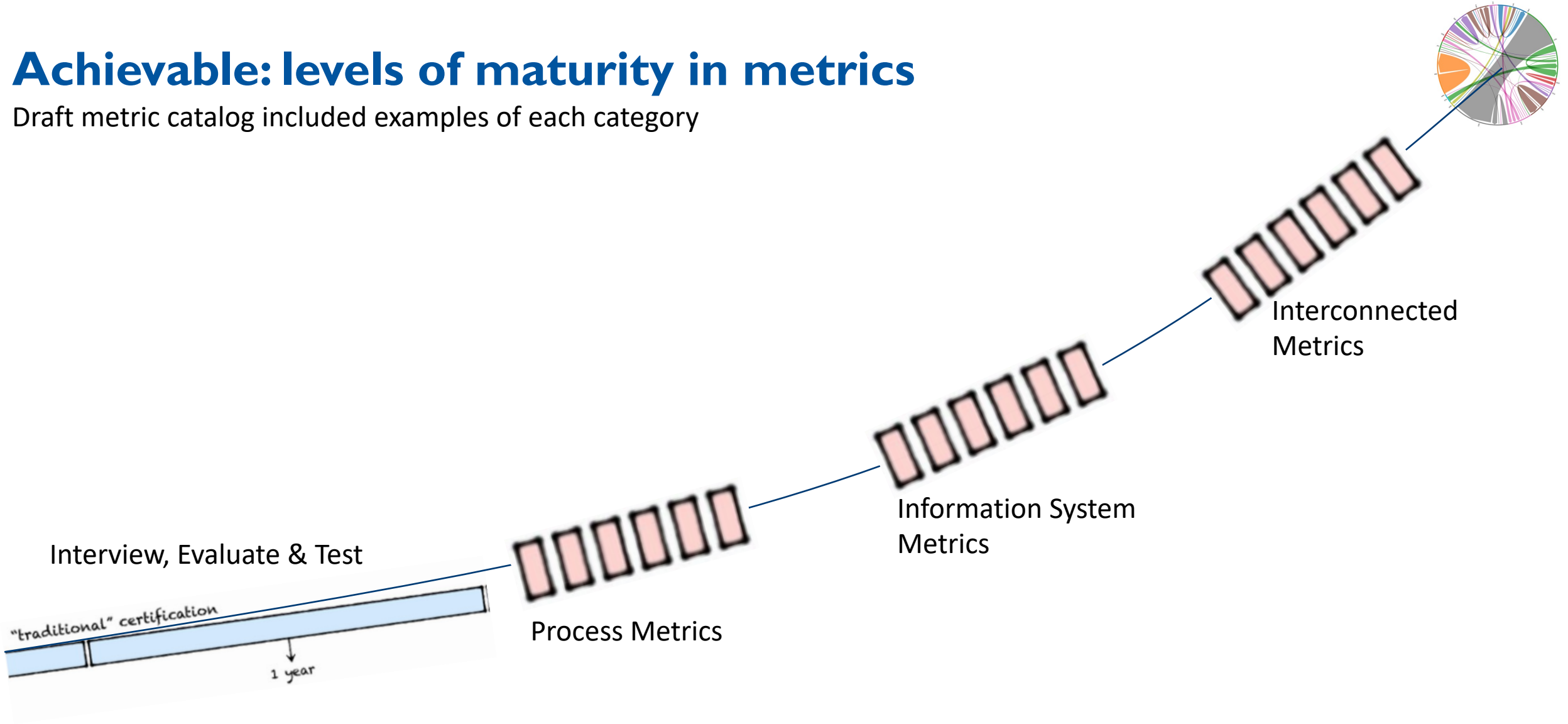
Expression	Percentage: 100 * A/B Where: A = Number of high and critical vulnerabilities identified during the sampling period and remediated within policy timeframes B = Total Number of High and Critical Vulnerabilities identified during the sampling period

CSP's could set their own ISO/IEC 19086 Service Level Objectives which may or may not be the same as recommendations

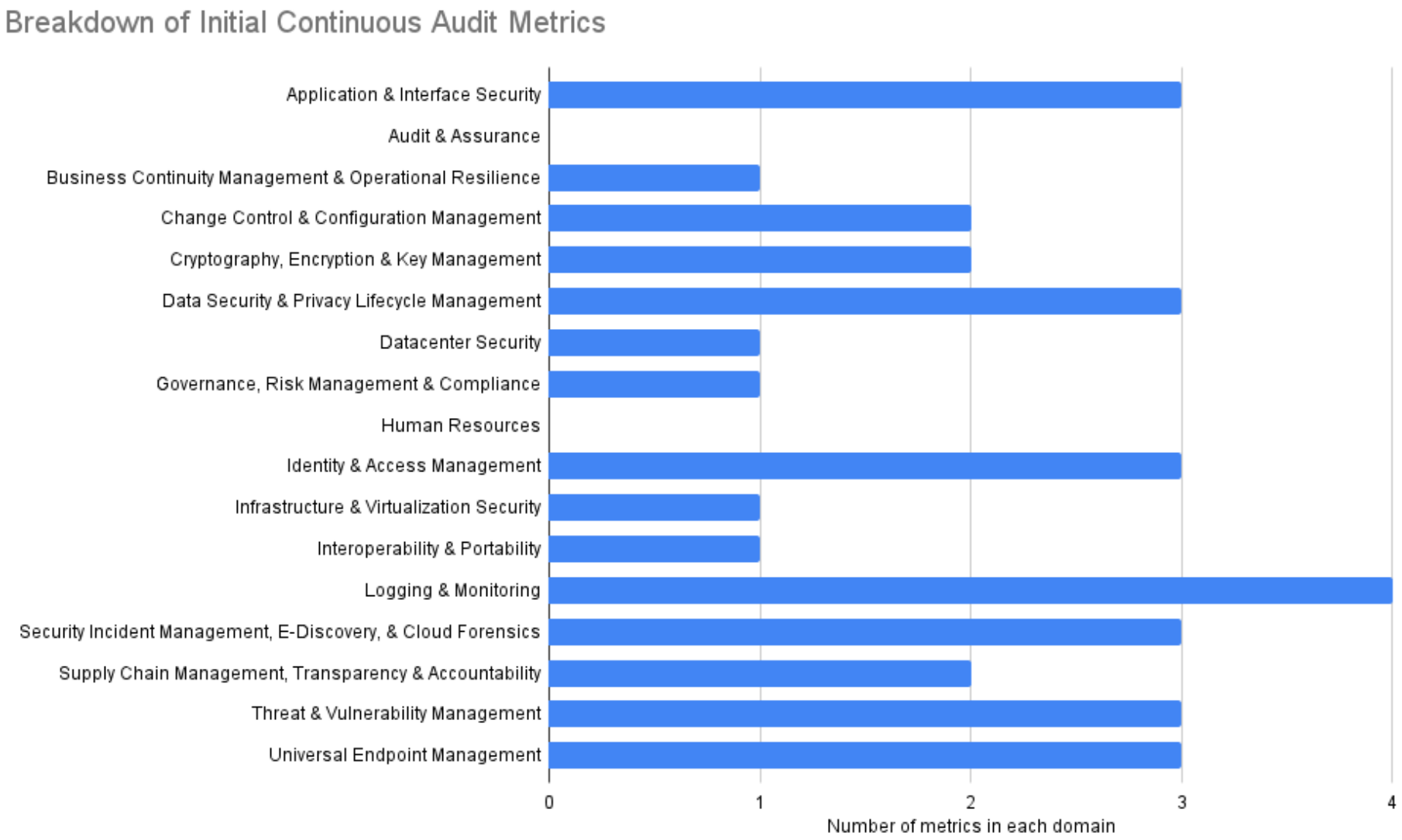
SLO recommendations	99%

Achievable: levels of maturity in metrics

Draft metric catalog included examples of each category



Initial Metric Set: ~33 metrics and growing



Threat and Vulnerability Management TVM-03-M1

Assumes ‘technical measures’ are a ticketing system

Service Level Objective:
“99% of high and critical vulnerabilities will be remediated within [policy timeframes]” …

… where traditional audit verified the policy (e.g. w/in 10days)

Primary CCMv4 Control ID	TVM-03
Primary Control Description	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.
Related CCMv4 Control IDs	TVM-08 (“Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.”)
Metric ID	TVM-03-M1
Metric Description	This metric measures the percentage of high and critical vulnerabilities that are remediated within the organization's policy timeframes. This reflects the time between when a vulnerability is identified on an organization's assets and when remediation is complete.
Expression	Percentage: 100 * A/B Where: A = Number of high and critical vulnerabilities identified during the sampling period and remediated within policy timeframes B = Total Number of High and Critical Vulnerabilities identified during the sampling period
Rules	High and critical Vulnerabilities are defined consistent with the implementation of TVM-08. If a vulnerability is identified but not remediated yet when the measurement is made, the measurement date is used as the remediation date in order to evaluate if the vulnerability has been mitigated within the defined policy timeframe, as expected for the calculation of A.
SLO recommendations	99%

Identity and Access Management IAM-09-M1

Assumes ‘technical measures’ is a database of users and roles that can be queried.

The metric is built from measures of this database

Primary CCMv4 Control ID	IAM-09
Primary Control Description	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.
Related CCMv4 Control IDs	IAM-03, IAM-05, IAM-10
Metric ID	IAM-09-M1
Metric Description	This metric measures the segregation of duties of non-production staff having access to production roles and vice-versa.
Expression	Percentage of users with segregation of privileged access roles: 100*(1-(A/B)) Where A = Number of users with admin access to more than one of the following capabilities: production data management, encryption and key management, or logging B = Number of users with access to production data management, encryption and key management, or logging capabilities
Rules	Capabilities are privileged roles or functions.
SLO recommendations	99%

Threat and Vulnerability Management
TVM-07-M1

Assumes “technical measures” results in system for scanning assets and that datacenter security objectives are met.

Combining data from multiple information systems in different domains.

Primary CCMv4 Control ID	TVM-07
Primary Control Description	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.
Related CCMv4 Control IDs	TVM-07, UEM-14, DCS-06
Metric ID	TVM-07-M1
Metric Description	This metric measures the percentage of managed assets scanned monthly
Expression	Percentage: 100 * A/B Where: A = Number of assets from the organization's asset catalog that have been scanned during the sampling period B = Total number of assets in the organization's asset catalog
Rules	The "asset catalog" refers to the cataloging requirements of CCMv4 DCS-06, which requires to "catalog and track all relevant physical and logical assets located at all of the CSP's sites within a secured system."
SLO recommendations	99%

Datacenter Security DCS-06-M1

Control is to track all relevant assets.

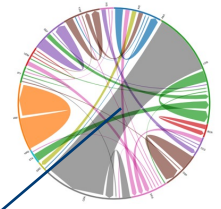
The metric is a “ratio of managed assets to detected assets”. This informs how well we’re doing at tracking.

Interconnects DCS-06 with LOG-05 (“Monitor security audit logs to detect… “)

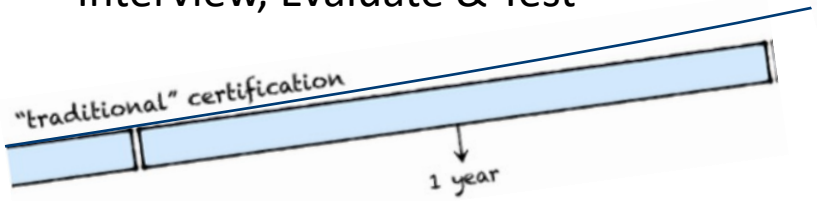
Primary CCMv4 Control ID	DCS-06
Primary Control Description	Catalog and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.
Related CCMv4 Control IDs	LOG-05
Metric ID	DCS-06-M1
Metric Description	This metric measures the ratio of managed assets (i.e. cataloged and tracked) to detected assets. The goal is to provide a signal if the asset cataloging and tracking system stops working.
Expression	Percentage: 100 * A/B Where: A = Number of distinct assets seen in security audit logs during the sampling period that are in an asset catalog. B = Number of distinct assets seen in security audit logs during the sampling period.
Rules	The assumption is that the design of the DCS-06 control process(es) was found to be effective by internal or external audits.
SLO recommendations	95%

Achievable: levels of maturity in metrics

Draft metric catalog included examples of each category



Interview, Evaluate & Test



Process Metrics

TVM-03-M1 is a measure of ticketing queue management

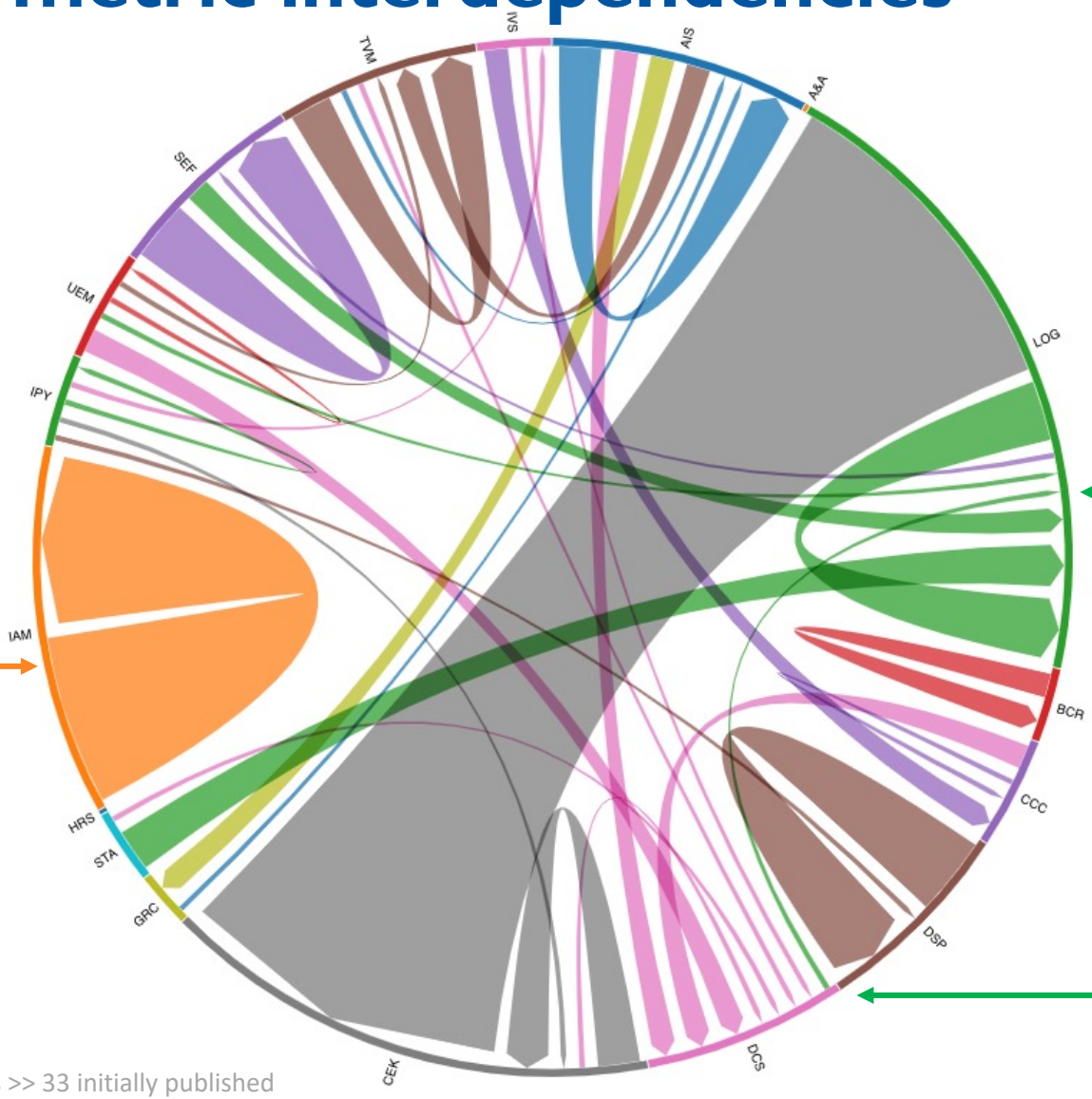
Information System Metrics

IAM-08-M1 measures if an information system is internally consistent.

Interconnected Metrics

TVM-07-M1 -> DCS-06 -> LOG-05 shows how data from multiple information systems informs holistic security state

Visualization of metric interdependencies

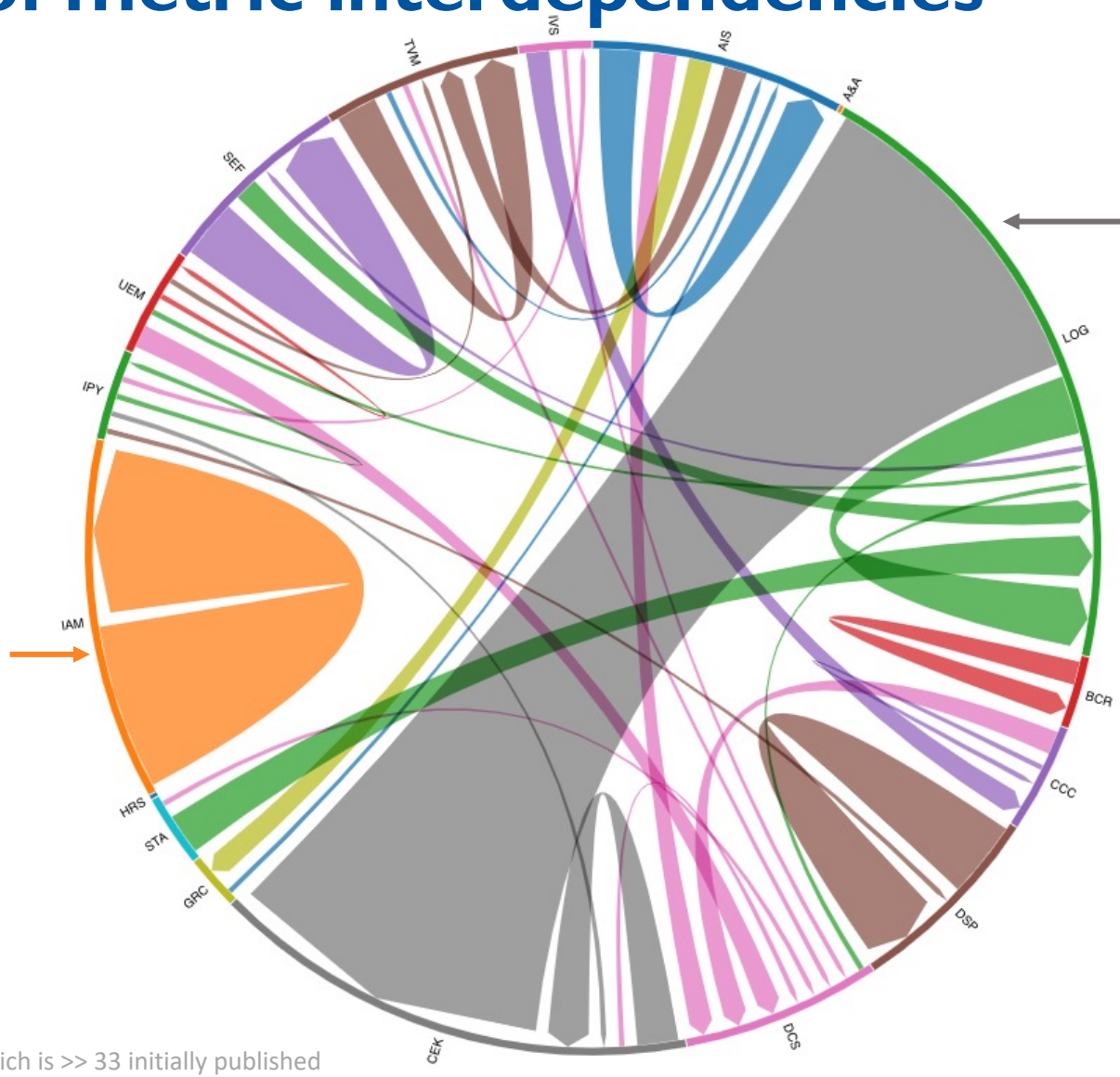


The initial IAM metrics look to their own information system

This this green line shows DCS-06-M1 leveraging LOG-05

Visualization includes all proposed metrics which is >> 33 initially published
https://observablehq.com/@pritikin/visualization-of-ccmv4-metrics-catalog

Visualization of metric interdependencies



LOG-10 “Establish and maintain a monitoring … of cryptographic, encryption and key management “ (e.g. CEK)

Visualization includes all proposed metrics which is >> 33 initially published
https://observablehq.com/@pritikin/visualization-of-ccmv4-metrics-catalog

Draft metric catalog status

As of July 24th, 2021, we no longer accept new comments in this document. If you want to contribute to this work, please join our community at circle.cloudsecurityalliance.org.

THANK YOU for all comments!

We're updating accordingly

Feedback we received

Both editorial and scope

On “operational privacy”

- “This metric is subjective”
- "90%, or an appropriate percentage as determined by the organization’s risk profile”

A mix of comments for easier and harder to meet metrics

- “Large number of organisations may not have such tools”
- “this SLO must be 100% to maintain compliance with [regulation]”

Interconnected metrics were accepted w/o comment

Many suggestions for additional metrics or alternate metrics

Call to action

Use metrics internally to validate the concepts in real life

- Integrate a metrics time series graph in your CISO dashboard.
  e.g., trend line for TVM-03-M1 to indicate vulnerability remediation efficiency
- Scope your metrics as narrow or as broad as you want
  e.g., measure IAM-09-M1 to be scoped for a specific application
- Ask your tool vendors to provide APIs to collect evidences and metrics automatically

Metrics during audit

- guide the way a continuous metrics audit would be evaluated and presented
- interactions between cloud vendors, providers and customers and auditors

Join the working group help us improve the catalog

Work on protocols for sharing metric results as continuous attestations

Conclusion + Contact

Metrics are a set of common indicators that we can share with each other while respecting operational privacy

pritikin@cisco.com

Or contact co-chair: Alain Pannetrat, apannetrat@cloudsecurityalliance.org

Join the "Continuous Audit Metrics" working group

https://circle.cloudsecurityalliance.org