ORACLE

CC in the Cloud
CCDB Joint Session Update
March 2023

Joshua Brickman & Brandon Harvey
Oracle Security Evaluations

Who we are:

- ***The team is comprised of 70 members including about 15 active members***

ORACLE

DISA DEFENSE INFORMATION SYSTEMS AGENCY A COMBAT SUPPORT AGENCY

Lightship Security

Trellix

NIAP

aws

cisco

JOHNS HOPKINS UNIVERSITY

Government of Canada / Gouvernement du Canada
Canadian Centre for Cyber Security

TERON LABS

Australian Government Australian Signals Directorate
ACSC Australian Cyber Security Centre

leidos

DELL Technologies

McAfee

Microsoft

NetApp

intertek ewa canada

intertek acumen security

UL

Project Timeline

March 2020
Project Kicks Off

Sept 2020
NWI Submitted to ISO

Mar 2022
ESR Published

May 2022
NIAP, ACA and CCCS Position Statements

Feb 2023
In-Person Workshop

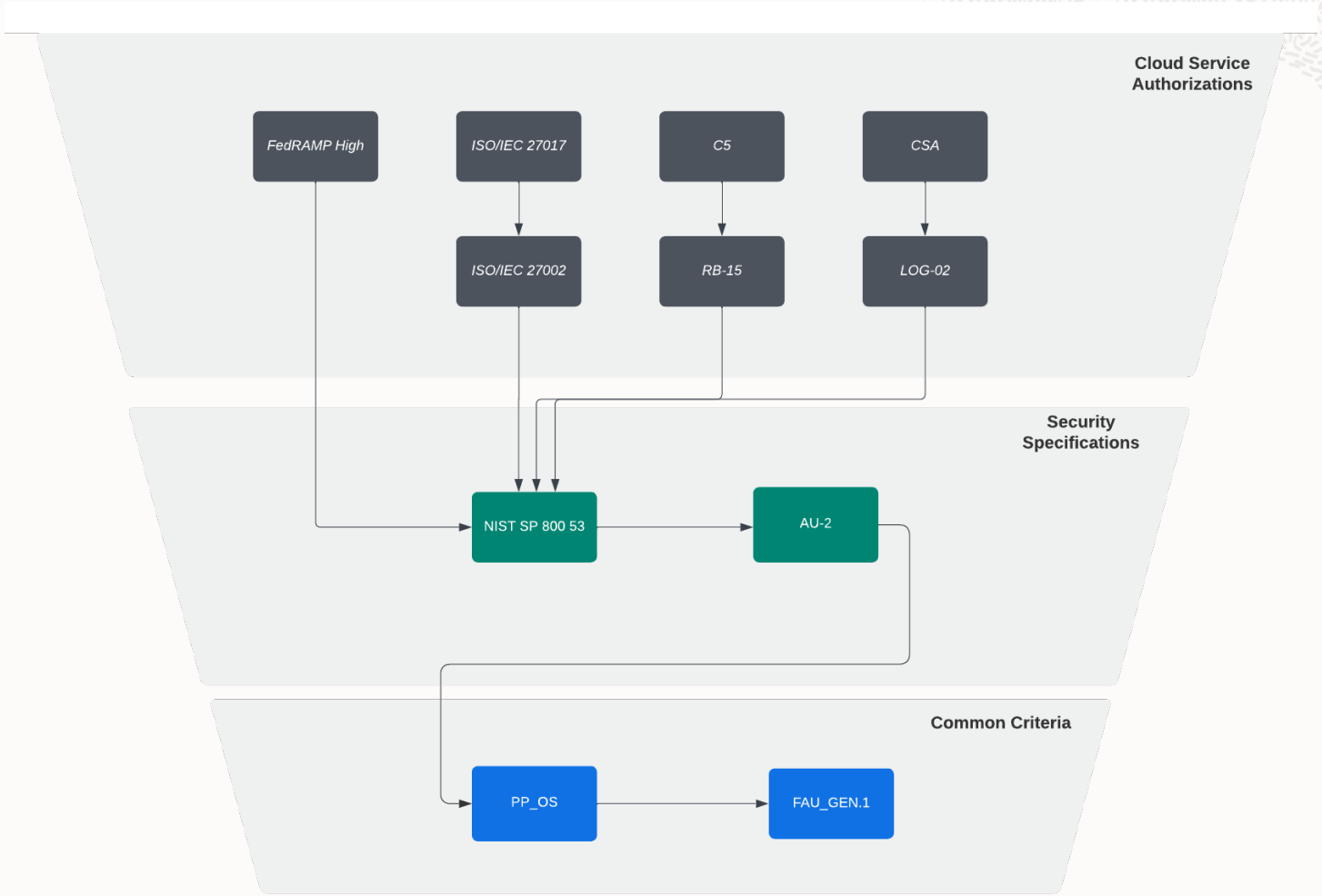
2H 2023
Draft Guidance Publication

Workshop Accomplishments

1. Main Guidance went from 11 to 23 pages in 3 days
2. Mapped 1st PP to FedRamp (MDM)
3. Closed ~50% of Open Issues
4. First Publication in 2023?

Mapping Evaluation Frameworks

- There is a bilateral relationship between Cloud authorization providers (FedRAMP, C5, CSA, etc) and CCiTC
- Controls can be mapped from the Cloud Service Provider down to the TOE.



MdM Mapping Report

- The Mobility Chief (Greg Youst) at Defense Information Systems Agency (DISA) is a key participant in the CCiTC project.
- Providing end-user guidance and an adoption use case
- We are developing this use case for Mobile Device Management (MDM) to provide a reference implementation for other PP TCs/iTCs
- The essential work for this foundation is in making sure that the assumptions and objectives in the MDM PP can be transferred to a Cloud Operating Environment
  - Can existing FedRAMP collateral satisfy these?

Figure 1: MDM System Operating Environment

MdM Mapping- Example

Assumption	Text	Affected by Cloud Deployment?	Assurance Needed in Cloud Deployment	Applicable Controls (800-53)	FedRAMP Level	Applicable Controls (C5)	How to Obtain Assurance in Cloud Deployment
A.MDM_SERVER_PLATFORM	The MDM Server relies upon a trustworthy platform and local network from which it provides administrative capabilities. The MDM Server relies on this platform to provide a range of security-related services including reliable timestamps, user and group account management, logon and logout services via a local or network directory service, remote access control, and audit log management services to include offloading of audit logs to other servers. The platform is expected to be configured specifically to provide MDM services, employing features such as a host-based firewall, which limits its network role to providing MDM functionality.	Y	logon and logout services	IA-5	Low	IDM-08 (confidentiality of authentication information) IDM-09 (authentication mechanisms)	Review documentation to ensure that the available platform authentication mechanisms are described Ensure through testing that authentication to the platform is enforced through these mechanisms
			remote access control	AC-3, AC-17	Low	COS-01 (technical safeguards) PSS-09 (authorisation mechanisms)	Review documentation to identify the mechanisms that can be used to control remote access to the platform Ensure through testing that the documented restrictions to remote access are enforced
			audit log management services	AU-9, AU-9(2)	AU-9 Low AU-9(2) Moderate	OPS-10 (logging and monitoring - concept) OPS-14 (logging and monitoring - storage of the logging data)	Review documentation to identify the mechanisms that can be used to offload stored audit records to an external system Ensure through testing that the documented mechanisms can be configured and used for any platform audit facility to which the TOE writes audit data
			limitation of non-MDM services through e.g. host-based firewall	SC-7(12)	Moderate	OPS-23 (managing vulnerabilities, malfunctions, and errors - system hardening)	Identify through documentation what platform or infrastructure mechanisms can be deployed to limit the external services that can be accessed on the platform to only those necessary for the TOE to function Ensure through testing that configuration of these mechanisms will enforce access control to the platform host
			protection of data in transit	SC-8	Moderate	CRY-02 (encryption of data for transmission (transport encryption))	Identify through documentation what trusted communications protocols are used to protected data in transit. Ensure through testing that the interface for these protocols can be invoked and that the use of insecure or unauthorized protocols can be restricted.
			protection of stored data at rest (specifically private keys)	SC-28, SC-28(3)	SC-28 Moderate SC-28(3) N/A	CRY-04 (secure key management)	Identify the protection mechanism used to ensure the confidentiality and integrity of data at rest. Ensure through testing that this mechanism can be used to store the desired data

Strategic Hurdles Prior to Workshop

What were the main gating factors for the project?

- Education about Cloud
- Policies around testing and equivalence
- Policies around assurance maintenance
- Could crypto be validated without low-level access to hardware?

Hurdles left to clear

- Developed guidance for Labs to incorporate cloud testing infrastructure (Labgram)
- Develop guidelines for pinning cloud testing infrastructure to hardware (VM Shapes / Bare Metal) for equivalence.
- Mapping cloud scope expansion across all PPs and more bidirectional analysis

Long term or Aspirational Goal-a Reminder

- CC for ICT products running in cloud (not CC for services or cloud providers)
- Have the CCRA formerly accept solutions to evaluate IT products in the cloud via position statements
- Provide guidance to evaluate a product/service in a cloud environment:
  - iTCs and TCs take guidance and update PPs
  - Schemes issue policies on CC testing in the cloud
  - ~5 years--Next version of Common Criteria ISO standard (15408)

Questions?

https://cc-in-the-cloud.github.io/