4th HPC Security Workshop

May 20-21, 2025

Wichita, KS

Erik Deumens

Building a Compliance Program for HPC

UF Information Technology
UNIVERSITY of FLORIDA

Overview

- Preparation
  - HPC system
  - Compliance and audits
  - Vendor selection
- Compliance frameworks
- Assessment process
  - Scoping
  - Readiness assessment
  - Remediation
  - Validation assessment
- Benefit for research

HiPerGator

Specs:

- 70,320 CPU cores
- 1,800 NVIDIA GPUs
- 30 petabytes of fast storage
- 51st fastest supercomputer in the world (Nov 2023 top500)

Preparation: HPC system

- High-performance computing (HPC) system
- Designed to handle large-scale, data-intensive computing workloads that require substantial processing power, memory and storage
- Used by researchers and students for development and production
- Clustered environment consisting of hundreds of interconnected compute nodes, switches, and PetaByte storage systems
- Software used: newly developed, open source, and commercially licensed

Preparation: HPC system

- 2013
  - Data center constructed in 2012 – 1.6 MW
  - HiPerGator 1.0 was built – 16,000 cores
- 2015
  - HiPerGator 2.0 – added 30,000 cores
- 2021
  - HiPerGator 1.0 – decommissioned
  - HiPerGator 3.0 – add 40,000 cores, now total 70,000 cores
  - Data center – power & cooling upgrade to 3.2 MW
  - HiPerGator AI in 2021 – added 1,120 A100 GPUs by donation from Chris Malachowsky and NVIDIA

Preparation: Compliance

- 2015 – need for NIST 800-53 moderate compliant system for one big contract
- We built an enclave on premise – it was too expensive to scale to small grants and projects
- But we learned about compliance
  - It is not just IT and technical controls
  - Policies, procedures, documentation
  - Communication with other offices: Research, Privacy, IT Security, Internal Audit
- 2017 – DFARS calls for NIST 800-171 for CUI
- We build a second enclave – cheaper to operate
  - Compliant with both 800-53 moderate and 800-171
  - with a lot more self service and automation to meet demands of complex research scenarios

Preparation: Audits

- Annual audits of 800-53-moderate enclave
  - Done by Internal Audit
- External 3rd party assessment of 800-171 enclave
  - We did two
  - We are about to do another this year for CMMC

Preparation: Beyond enclave

- Researchers wanted to use the full HPC system
  - With Protected Health Information (PHI) using AI tools
  - Going beyond the enclave
- To avoid any doubts about compliance, the administration decided to go with HITRUST Alliance certification
  - It is considered the gold standard in healthcare (hospitals, health insurance, pharma)
  - HITRUST has “certified assessors” (like CMMC)
- UF did a purchase process called “invitation to negotiate (ITN)”
  - Vendors submit a proposal
  - A committee reviews, interviews, negotiates, and selects the vendor

Compliance Frameworks

- NIST – National Institute for Science and Technology
  - Risk Management Framework (RMF)
    - Special Publication 800-53 is the catalog of all controls
    - Many other NIST documents describe how to use the catalog
    - SP 800-171 was created for non-federal organization to safeguard Controlled Unclassified Information (CUI) – DFARS requires compliance with 800-171 for DoD contacts with CUI
  - Cybersecurity Framework (CSF)
    - Similar but easier to follow and implement, especially for large organizations
- ISO – International Standards Organization
  - Maps to NIST frameworks
- HITRUST CSF – Originated to meet HIPAA (Next slide)

HITRUST

- Founded in 2007, HITRUST is a nonprofit responsible for frameworks, standards and methodologies. HITRUST champions programs that safeguard sensitive information and manage information risk for organizations across all industries.

- A certifiable controls framework built upon other frameworks and authoritative sources
- Originally built on ISO 27001 and ISO 27002
- Managed and maintained by HITRUST
- Designed by security professionals to address:
- Risk management requirements
- Security requirements
- Compliance needs

HITRUST CSF® is a comprehensive, prescriptive and certifiable framework that's built upon other standards and authoritative sources. It's one of the most widely adopted frameworks that covers over 40 authoritative sources.

Assessment process with certified assessor

2. READINESS ASSESSMENT

The likelihood of HITRUST Certification is directly dependent of how well an organization prepares

4. HITRUST VALIDATION

Assessment that tests the design and effectiveness of implemented controls; often results in CSF Certification

1. WORKSHOP

Proper planning, scoping, training and organizational alignment is a critical success factor

3. REMEDIATION

Implementation of remediated controls is necessary to boost scores to a “certifiable” level

5. INTERIM

Year two HITRUST assessment requirement that ensures CAP fulfillment and no erosion of control maturity

Assessment process: Workshop

Purpose

- Prepare control owners
- Solidify scoping parameters
- Evaluate existing policies and procedures
- Introduce HITRUST key stakeholders
- Understand control responsibilities between UF Research Computing and UFIT
- Identify inheritance opportunities
- Understand the nuances of the HiPerGator environment
- Perform MyCSF scoping
- Establish timeline, investment estimate and success factors

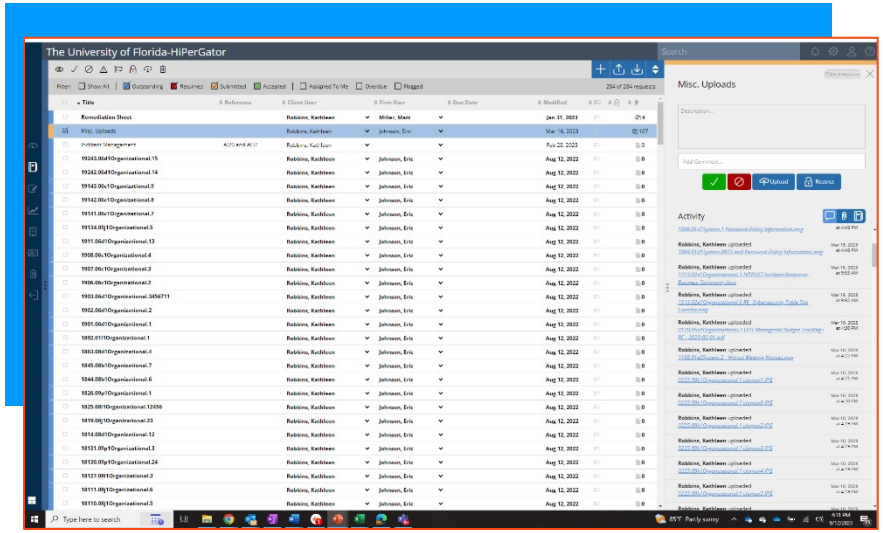
Process

- Two-day virtual exercise
- Representation from UF Research Computing, HITRUST and FD
- Review of:
- Network design
  - In-scope systems
  - Implemented controls
  - Policies and procedures
  - HITRUST scoping factors
  - Post-workshop meeting with HITRUST
- Evaluate one requirement from each domain

Payoff

- Three-way agreement on scope
- Confirmation from HITRUST that HiPerGator was “certifiable”
- Control owners were prepared for the process ahead; executive buy-in
- Solidified scope; 266 requirements, 8 N/A’s
- Communication of expected remediation
- Treatment plans defined for areas of non-conformance

Assessment process: Readiness assessment



- Performed “facilitated walkthroughs” onsite at UF
- FD provided policy and procedure templates and guidance
- UF established a central point of contact for evidence collection
- Remediation was performed collaboratively between UF and FD
- Visibility was given to HITRUST QA as needed throughout

Assessment process: Remediation considerations

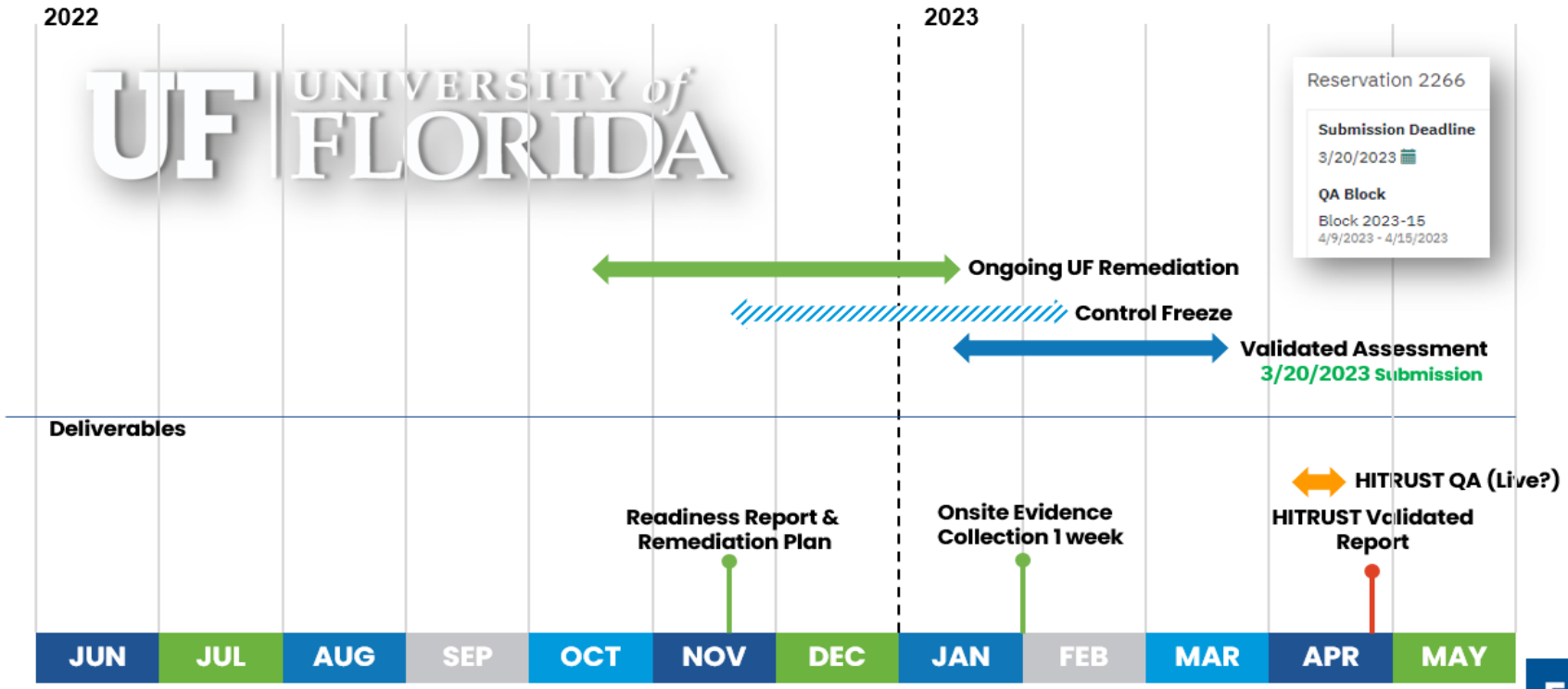
- Policies and procedures did not conform to the prescriptive nature of HITRUST
- Removal of laptops/desktops from scope
- AV scanning negated the high-performance design of HiPerGator
- “Copy/paste/print” functionality could not be restricted
- Hundreds of end-user deployed software applications
- Management of privileged access
- Encryption of data within the HiPerGator environment

Assessment process: Remediation

- Because of our experience with compliance and audits
  - We were able to address the 87 findings in 6 weeks (Oct 1st through Nov 15th)
- Because of the close relation of the assessor with HITRUST
  - We could discuss the troublesome controls with the HITRUS quality assessment (QA) team during remediation
  - We could ensure that compensating controls were satisfactory
  - Thus we would not run into unexpected obstacles after validated assessment in Feb-Mar 2023

Assessment process: Full timeline

UPDATED HITRUST ASSESSMENT TIMELINE PROPOSAL 11/15/2022



Benefit for research

- Our faculty are very grateful
- They can write proposals that process PHI data with the most advanced computing system available to them
- Many projects are running now
- Many more are being reviewed for award this year and next.

Questions?