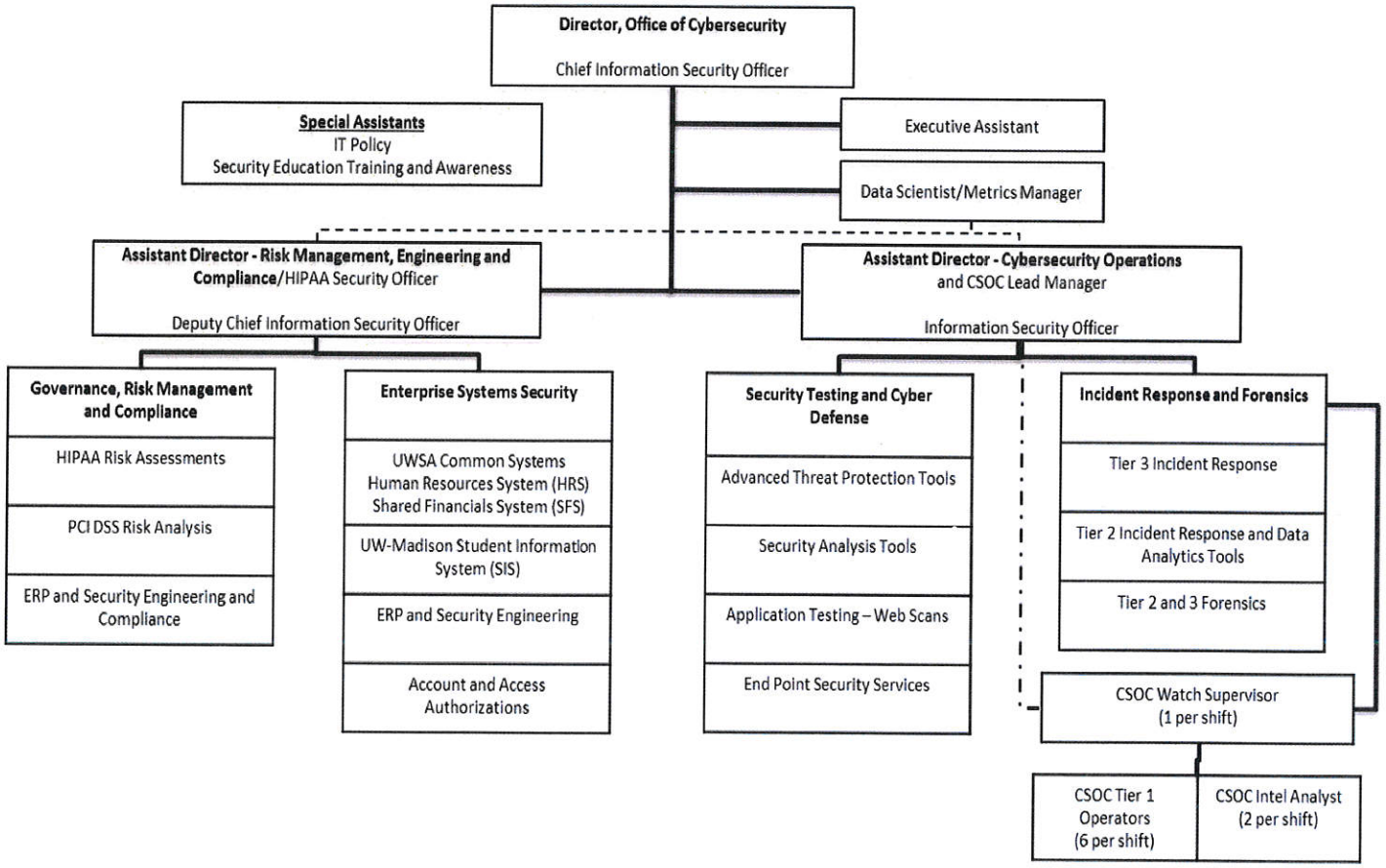
UC, MAR 26, 2018

Office of Cybersecurity Overview

Office of Cybersecurity is situated in the Office of the CIO. The Chief Information Security Officer reports to the campus Chief Information Officer. Cybersecurity is funded by ~$1M in GPR money (fund 101), ~$1M in cost recovery money (fund 128) and has 27 FTE and 19 student hourly employees.



2018-2023 Cybersecurity Strategy

The Office of Cybersecurity is working with many task groups comprised of Cybsecurity staff members and staff in the distributed IT community to formulate a 2018-2023 Cybersecurity strategy for UW-Madison, an update to the 2015-2019 Cybersecurity strategy. A final version of the strategy will be posted by July 1, 2018.

- The task groups have identified several challenges including coordination, communication, and consistency of cybersecurity standards, practices, and guidelines across distributed units; diverse and changing technology, business processes, use cases, and cybersecurity skill levels; competing priorities compounded by ever-changing security laws, policies, and procedures.

- These task groups have also worked to identify goals and metrics across seven elements of the Cybersecurity strategy: community, service alignment, measuring metrics, data, trust, operational risk, and research & outreach.

Risk Management Policy

Likely familiar to the UC, this policy was reviewed, and endorsement was advised by the technical advisory groups to the ITC. The ITC voted to endorse the policy during their meeting on 3/16.

The basic concept of the policy is that cybersecurity risk will be managed such that the likelihood and impact of threats and vulnerabilities are minimized. The implementation plan describes the mandatory process to follow, the Risk Management Framework, which is based upon (and very similar to) NIST Special Publication 800-37. There are six steps, positioned in a circular manner (Step 1 is followed by Step 6), and the Risk Management Policy focuses on the last three steps:

- Step 1 – Categorize system
- Step 2 – Select security controls
- Step 3 – Implement and verify controls
- Step 4 – Perform Risk assessment (Cybersecurity asses risk, and CISO provides Risk Assessment to certify the represented risk is accurate)
- Step 5 – Authorize system (Level of risk presented in Step 4 is then accepted or mitigated by the Risk Executive on behalf of the University. The CIO has affirmed there is one Risk Executive per division which is the Dean, Director, or their appointee)
- Step 6 – Monitor and Mitigate (The unit and the Office of Cybersecurity will continually monitor the given system to assure the level of risk remains at or below the level accepted in Step 5)

This is a system-by-system approach which is intended to be phased in. Prioritization of how systems will be onboarded into compliance with the policy is based on data classifications of each system (restricted data systems first, then sensitive/internal data systems, then public data systems).

Controlled Unclassified Information (CUI)

CUI is information that requires safeguarding or dissemination controls but is **not** classified. Executive Order 13556 from November 2010 established the CUI program to create common definitions and standardized procedures to handle the 100+ different ways of characterizing such data. This is an open and uniform program to manage all CUI within the *executive branch* and *agencies* of the federal government, those that sponsor our research (DoD, USDA, DoE, etc.). We are required to safeguard CUI in accordance to guidance issued by NIST, by complying with NIST Special Publication 800-171.

One agency (DoD) is enforcing compliance as of December 31, 2017. Other agencies will be following in 2018 and beyond, though there currently are no determinations on specific dates.

OVCRGE and RSP are interested in provisioning a campus service to introduce efficiencies for researchers who need to work with or create CUI. DoIT is in the planning stages of creating this service.