Michigan
Auditors in Glass Houses

Dodi E. Smith

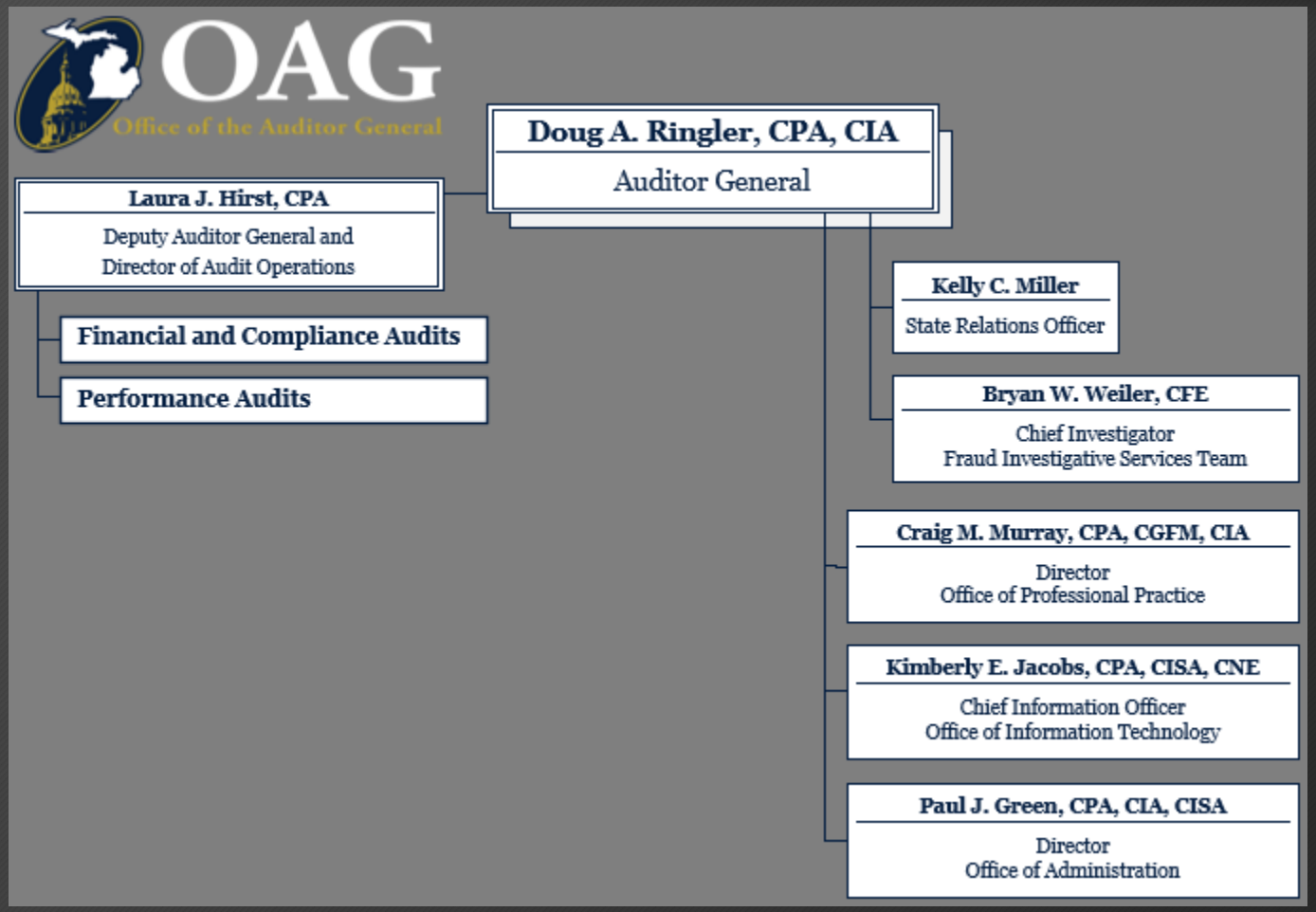
Information Security Manager

A Little About the Michigan Office of the Auditor General (OAG)

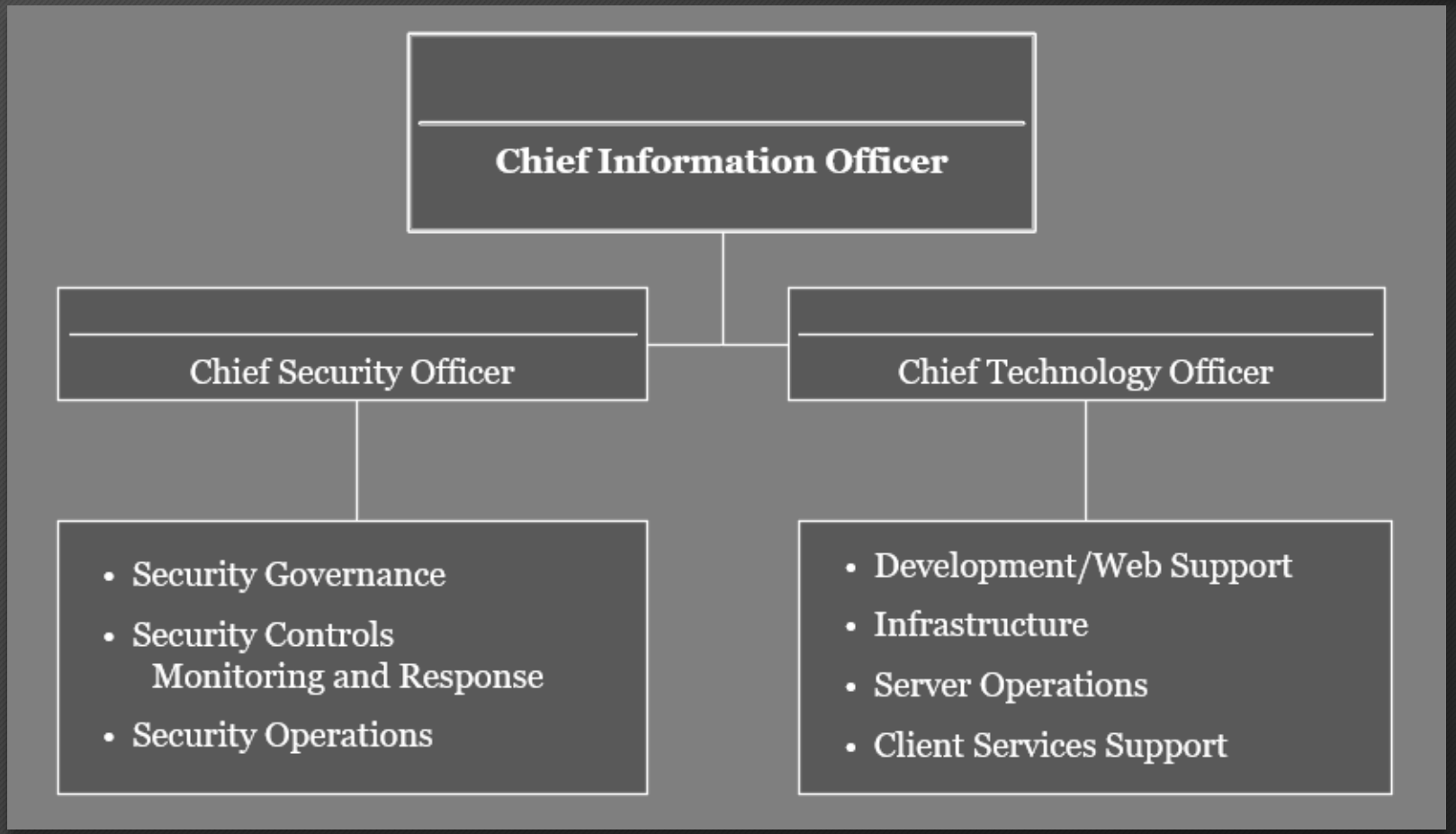
Auditor General - Appointed by Legislature

- 154 employees
- $26 million budget
- Fiscal Year 2020 Audits
  - 18 financial/single audit
  - 32 performance audits and follow-ups
  - 10 other projects
  - 15 contract audits

OAG Organizational Chart (July 2021)



Office of Information Technology



A Little About Michigan Government…

State of Michigan

- 17 Executive Branch Departments
- 48,000+ State Employees
- $62.7 billion budget
- 1.2 million recipients of government food assistance
- 1.7 million residents in the Medicaid program
- 13,000 foster care children
- 1.4 million pupils
- 5 million individual income taxpayers
- 92,000+ prisoners

Our Authority

The State Constitution and State law provide the OAG with authority to access all State department records upon demand.

Clarifying points in the law that have helped us:

- The auditor general is subject to the same duty of confidentiality imposed by law on the entity providing the confidential information.
- The auditor general is subject to any civil or criminal penalties imposed by law for unlawfully disclosing that confidential information.

Security Assessment

Security Assessment of the OAG IT Environment

- Policy, Process and Procedure Assessment and Maturity Review
- Framework Recommendation
- Vulnerability Scan
- Organizational Structure Review
- Remediation Plan

What We Learned From the Security Assessment

- Summarized the OAG's security posture
- Identified the gaps in our security posture
- Prioritized our to-do list

To-Do List

Framework/Security Governance

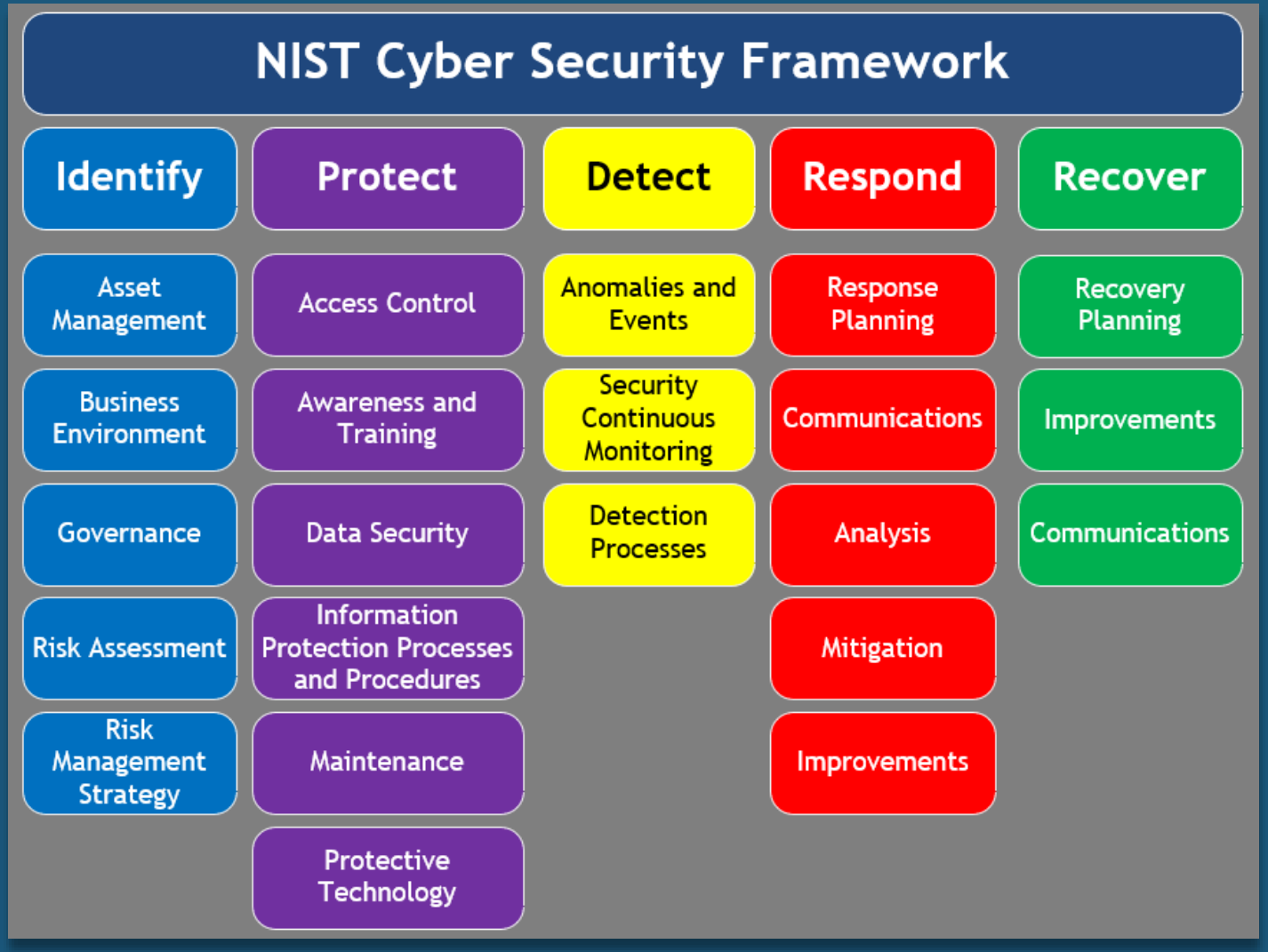
Staff Augmentation

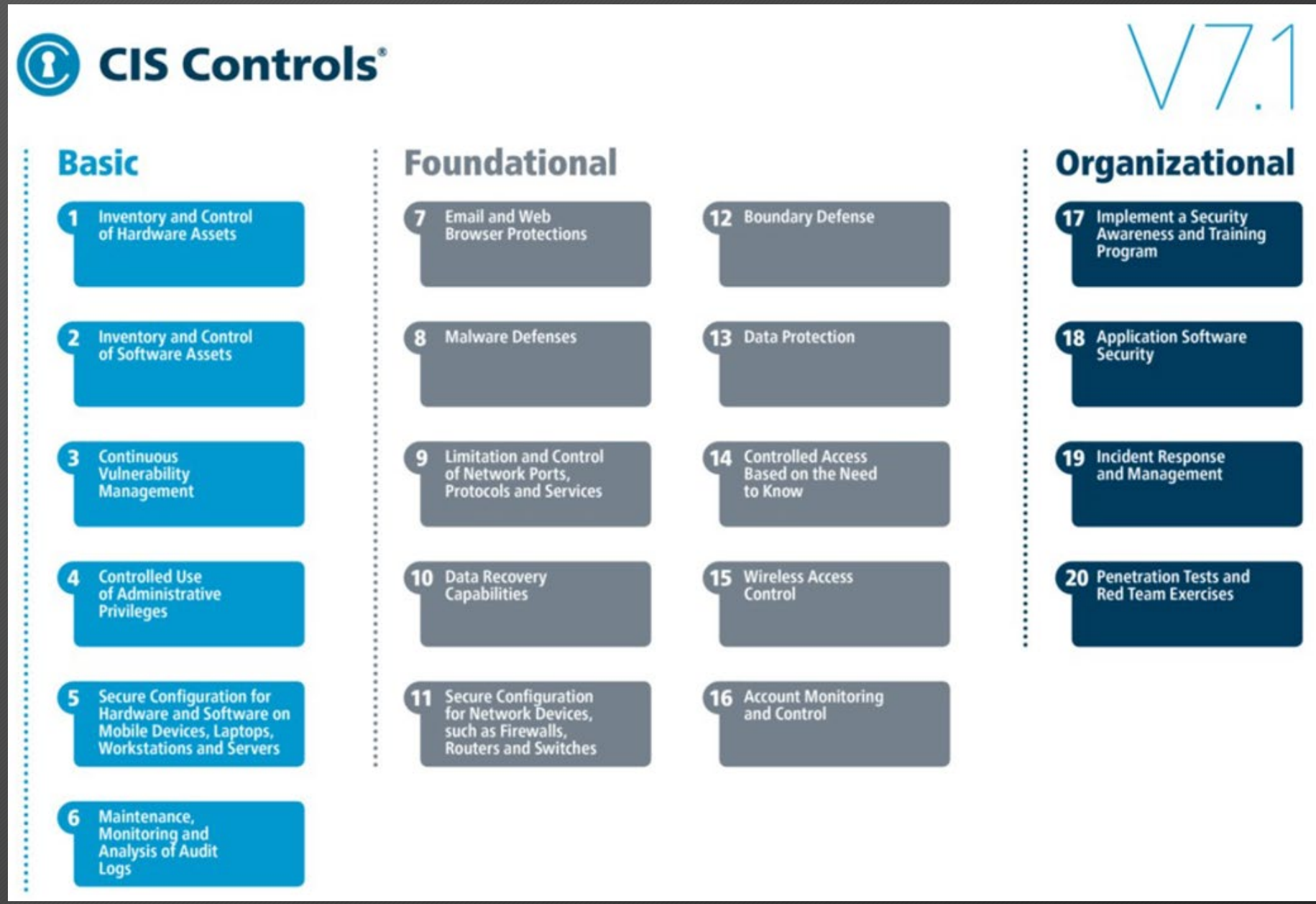
Hardware and Software Considerations

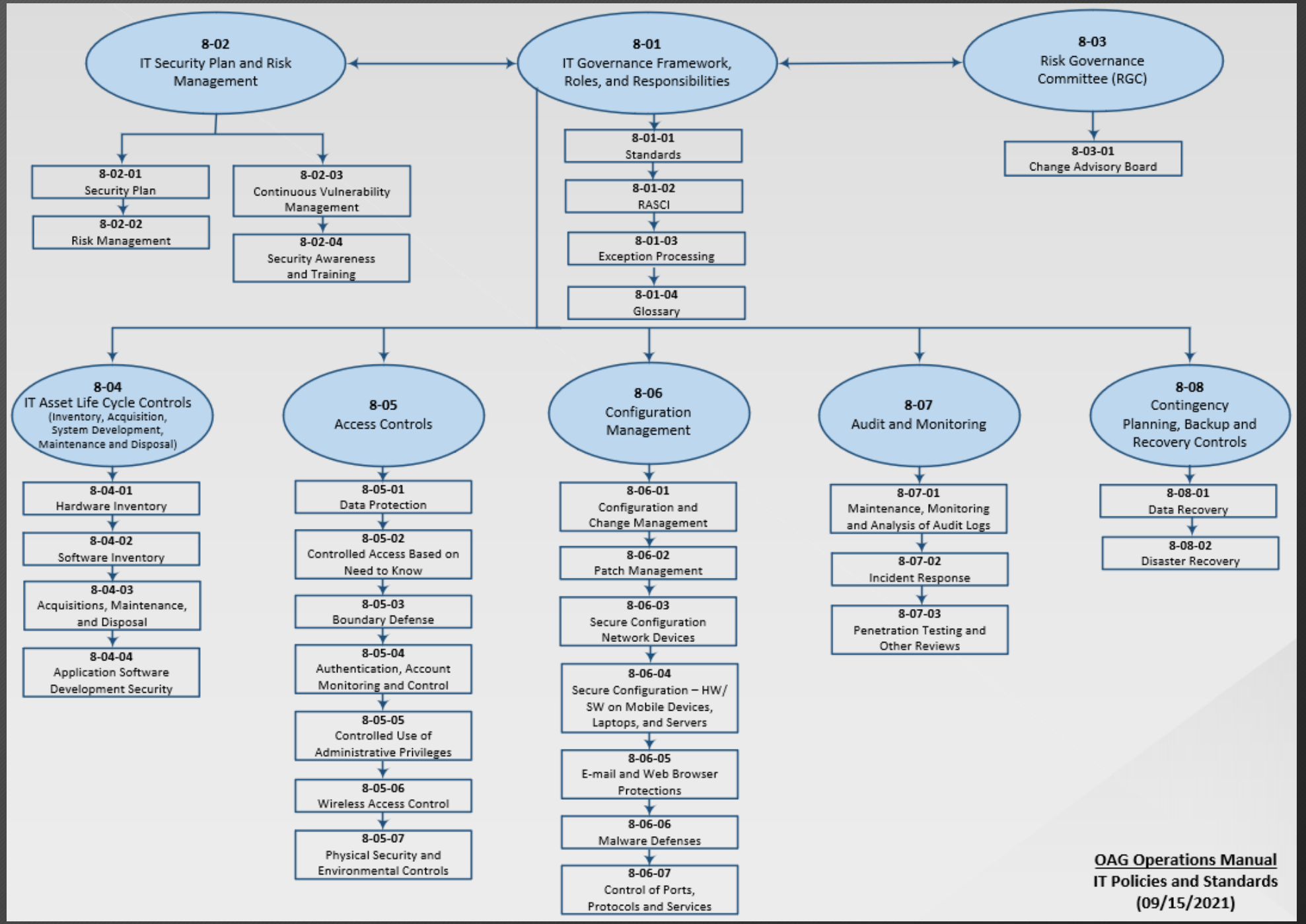
- Centralized Logging
- Security Information and Event Management
- Segregated Production & Non-Production
- Vulnerability Scanning
- Multi-Factor Authentication
- Enhanced Asset Inventory Tracking
- Network Monitoring

Adopt a Security Framework

The Framework is a helpful tool in managing cybersecurity risks.




CIS Controls®
V7.1
Basic
1 Inventory and Control of Hardware Assets
2 Inventory and Control of Software Assets
3 Continuous Vulnerability Management
4 Controlled Use of Administrative Privileges
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6 Maintenance, Monitoring and Analysis of Audit Logs
Foundational
7 Email and Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports, Protocols and Services
10 Data Recovery Capabilities
11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring and Control
Organizational
17 Implement a Security Awareness and Training Program
18 Application Software Security
19 Incident Response and Management
20 Penetration Tests and Red Team Exercises


8-02
IT Security Plan and Risk Management
8-01
IT Governance Framework, Roles, and Responsibilities
8-03
Risk Governance Committee (RGC)
8-02-01
Security Plan
8-02-02
Risk Management
8-02-03
Continuous Vulnerability Management
8-02-04
Security Awareness and Training
8-01-01
Standards
8-01-02
RASCI
8-01-03
Exception Processing
8-01-04
Glossary
8-03-01
Change Advisory Board
8-04
IT Asset Life Cycle Controls
(Inventory, Acquisition, System Development, Maintenance and Disposal)
8-05
Access Controls
8-06
Configuration Management
8-07
Audit and Monitoring
8-08
Contingency Planning, Backup and Recovery Controls
8-04-01
Hardware Inventory
8-04-02
Software Inventory
8-04-03
Acquisitions, Maintenance, and Disposal
8-04-04
Application Software Development Security
8-05-01
Data Protection
8-05-02
Controlled Access Based on Need to Know
8-05-03
Boundary Defense
8-05-04
Authentication, Account Monitoring and Control
8-05-05
Controlled Use of Administrative Privileges
8-05-06
Wireless Access Control
8-05-07
Physical Security and Environmental Controls
8-06-01
Configuration and Change Management
8-06-02
Patch Management
8-06-03
Secure Configuration Network Devices
8-06-04
Secure Configuration – HW/ SW on Mobile Devices, Laptops, and Servers
8-06-05
E-mail and Web Browser Protections
8-06-06
Malware Defenses
8-06-07
Control of Ports, Protocols and Services
8-07-01
Maintenance, Monitoring and Analysis of Audit Logs
8-07-02
Incident Response
8-07-03
Penetration Testing and Other Reviews
8-08-01
Data Recovery
8-08-02
Disaster Recovery
OAG Operations Manual
IT Policies and Standards
(09/15/2021)

IT Governance

- Risk Governance Committee
- Change Advisory Board

- ROUND-THE-CLOCK MONITORING
- VULNERABILITY SCANNING
- ACCESS TO SPECIALIST EXPERTISE

Managed Security Service Provider (MSSP)

Center for Internet Security (CIS)

- CIS Benchmarks
- CIS-Configuration Assessment Tool (CAT)
- CIS Controls Self-Assessment Tool (CIS CSAT)

Multi-Factor Authentication (MFA)

The OAG is implementing MFA to increase our security to authentication.

- DUO is currently required for access to:
  - Office 365
- Within 2 months, DUO will be required for:
  - Cisco AnyConnect VPN
  - Microsoft Login and RDP (terminal services)

Challenges

- Managing Change
- Balancing security and end user usability
- Keeping the momentum

Next Steps:

STRENGTHEN SECURITY POSTURE

ASSESS RISK

AUDIT

Questions

- **Dodi E. Smith, CPA, CISA**
- **Information Security Manager**
- **E-mail:** desmith@audgen.michigan.gov
- **Phone:** 517-481-4382