

Treasury IT Overview



OREGON
STATE
TREASURY

February 14, 2019

Joint Legislative Committee on Information
Management and Technology

Our Way is Forward

Vision Statement

Leading the way for Oregonians to achieve long-term financial security

Mission Statement

Improving Oregon governments' and citizens' financial capabilities

Our IT Mission

Improving Oregon governments' and citizens' financial capabilities *through collaborative, resilient, innovative, and secure technology solutions.*

IT Director: Chris Molin

- 21 Years with Military (Active Duty Air Force, DoD Contractor)
- 7 Years State Government
- Background:
 - Systems, Network, and Database Administration
 - Cybersecurity
 - IT Service Management
 - Program Management (Command and Control and IT Operations)
 - Strategy, Project Portfolio Management, and Process
- CompTIA (Computing Technology Industry Association), ITIL (Information Technology Infrastructure Library), Oracle, and Microsoft Certifications

Information Technology and Cybersecurity

- Bottom line: Millions of annual transactions, hundreds of billions of dollars
- Provide the computing infrastructure and expertise needed to conduct business securely and reliably.
- Three connected locations (Salem, Capitol, Tigard).
- Design and manage solutions that meet business needs through a combination of cloud-based, purchased, and custom in-house developed applications.
- Process and organizational maturity

IT Operational Overview

Technical Services Delivery

Service Desk

ITIL Call Center
Tier 1 Triage
Ticket Tracking and Escalation
Knowledgebase
Mobile Device Management

Asset Management

Hardware/Software Inventory
Warranty Management
Lifecycle Management
Issue monitoring and reporting

Desktop Support

Patching
Tier 2 Troubleshooting
End-User support

Application Services

Application Development

Application Development and Maintenance
COTS/SaaS Evaluation and Implementation
COTS Updates
Integration
Web Design

Data Management

Database Administration
Data Analysis
Data Management

Banking Operations

Transaction Processing
Job Scheduling

Information Security

Agency-wide Information Security Program
Information Security Risk Management

Application Security

Information Security Policy

Network & Systems Security
Third-party Due Diligence

Security Awareness

Incident Response

Threat and Vulnerability Management

Continuous Monitoring
Identity and Access Management
Data Security

Infrastructure Services

Systems

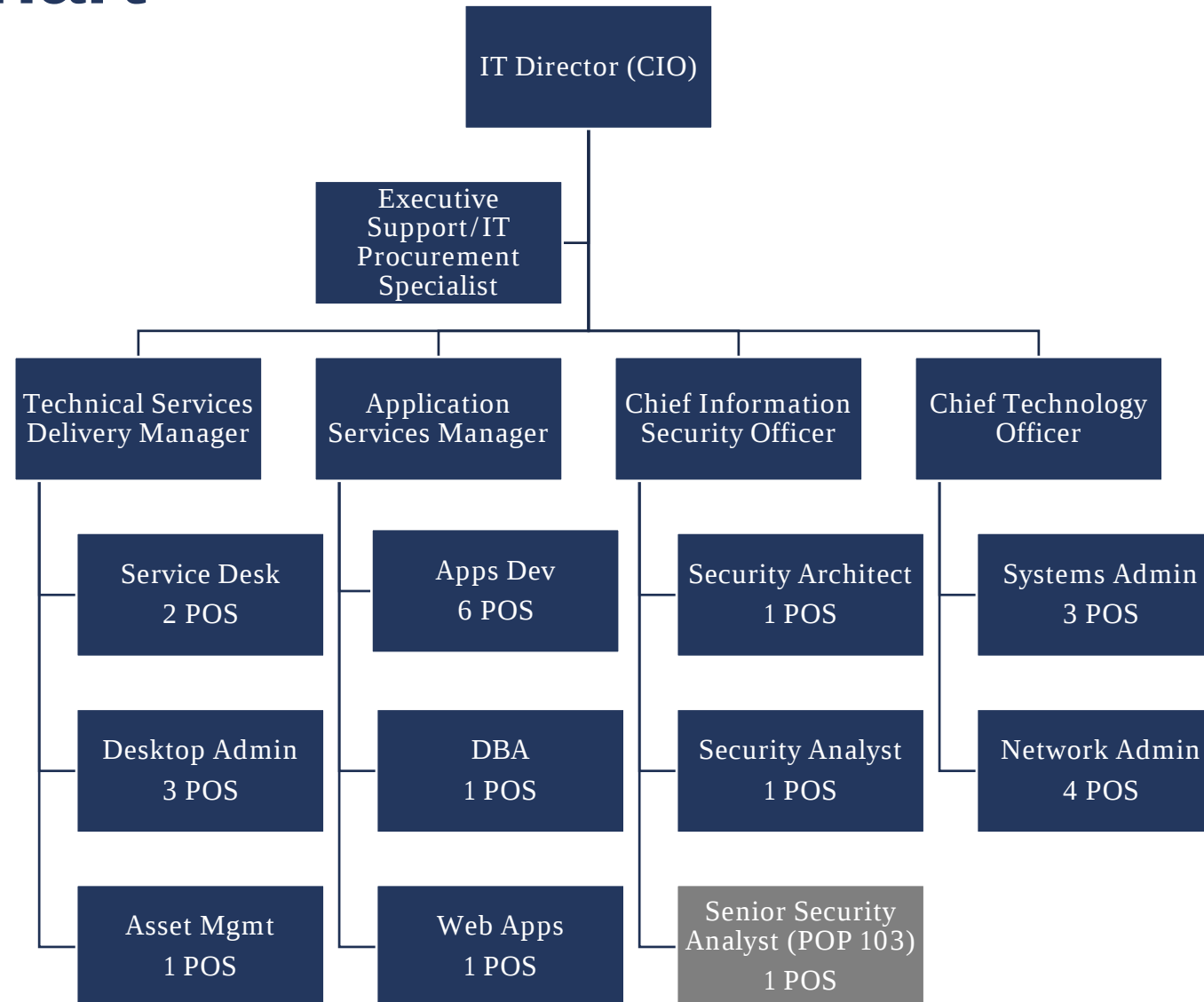
Server and Desktop Infrastructure
Office and Collaboration Tools
Patching and Compliance
Remote Access
Secure Data Transmission

Network

Network Infrastructure
Network Management and Monitoring
Virtual Infrastructure
Backup and Recovery
Physical Infrastructure



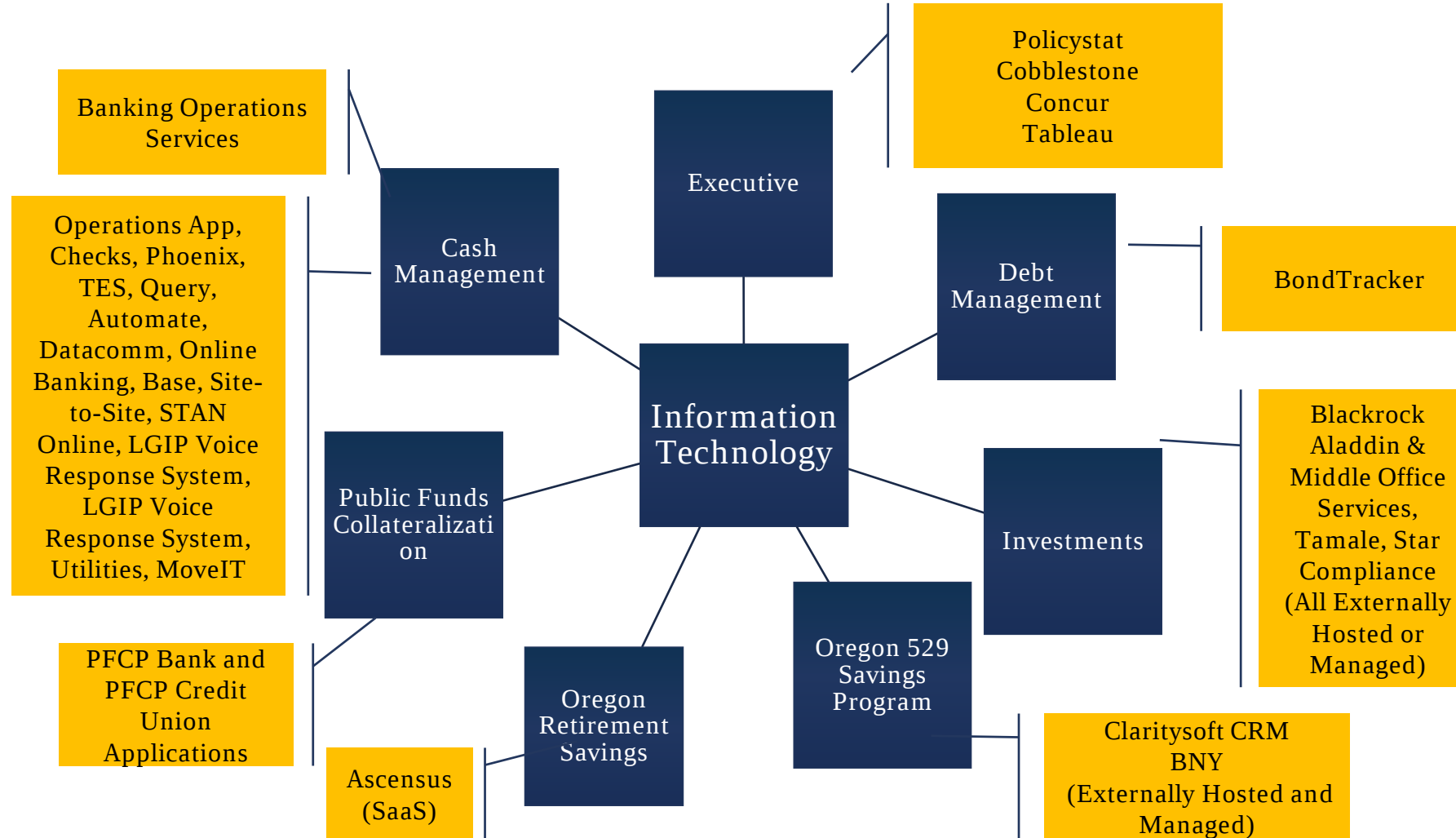
IT Org Chart



2017-19 LAB
\$12.7 million
29 Positions
27.42 FTE

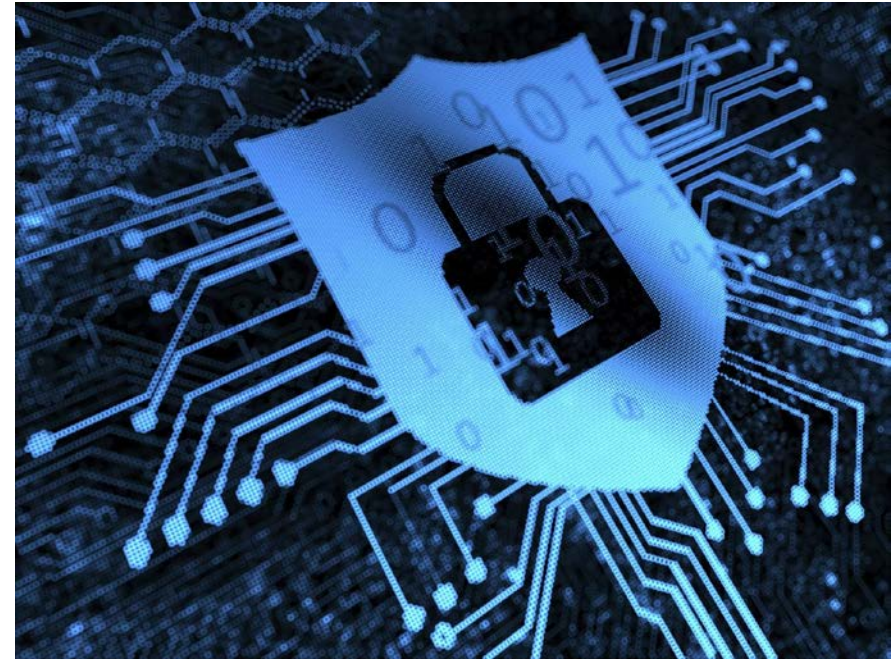
2019-21 GRB
\$12.8 million
30 Positions
29.42 FTE

IT Systems Supported



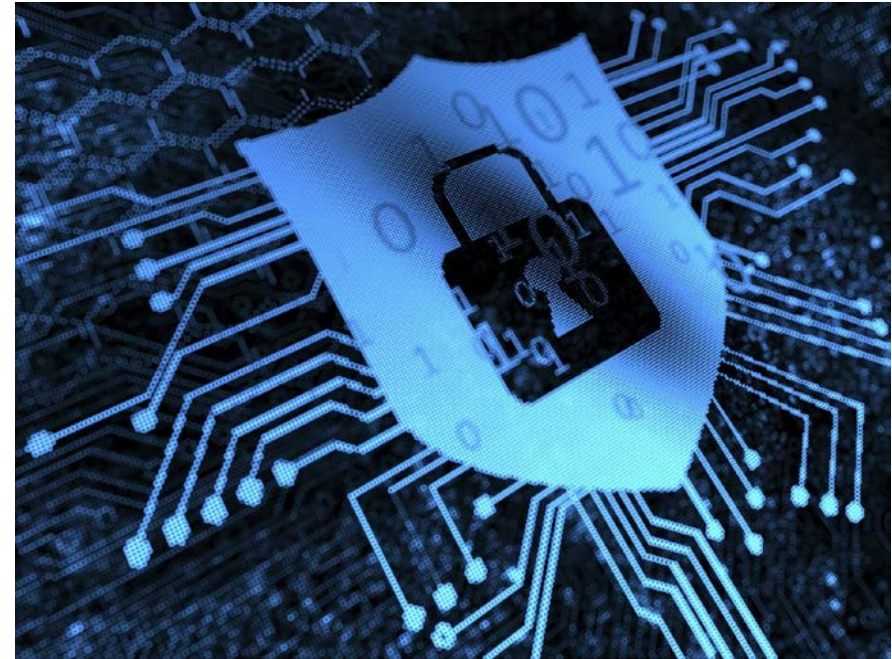
IT Major Milestones in 2018

- ITIL fundamentals – move from “Help Desk” to “Service Desk”
- Organizational restructuring to embed security functions across the IT Operation
- Implementation of robust Mobile Device Management tool
- Faster, better encryption for telework devices
- Voice over IP (VoiP)
- IT General Controls – Change Management Audit by Deloitte. (May 2018)



IT Strategic Initiatives 2018-2019

- Implementation of Information Technology Service Management (ITSM)
- Office 365
- Systems Modernization:
 - Cash Management Improvement and Renewal Program (CMIRP): Electronic Funds Transfer Business Systems Renewal (EFT BSR)
- Maturing the Asset Management Program
- Evolution of IT Project Steering Group
- Project Portfolio Development
- IT General Controls – Network, Operations, and Data Center Security Audit by Deloitte. (March 2019)



Chief Information Security Officer (CISO): Alain Bouit

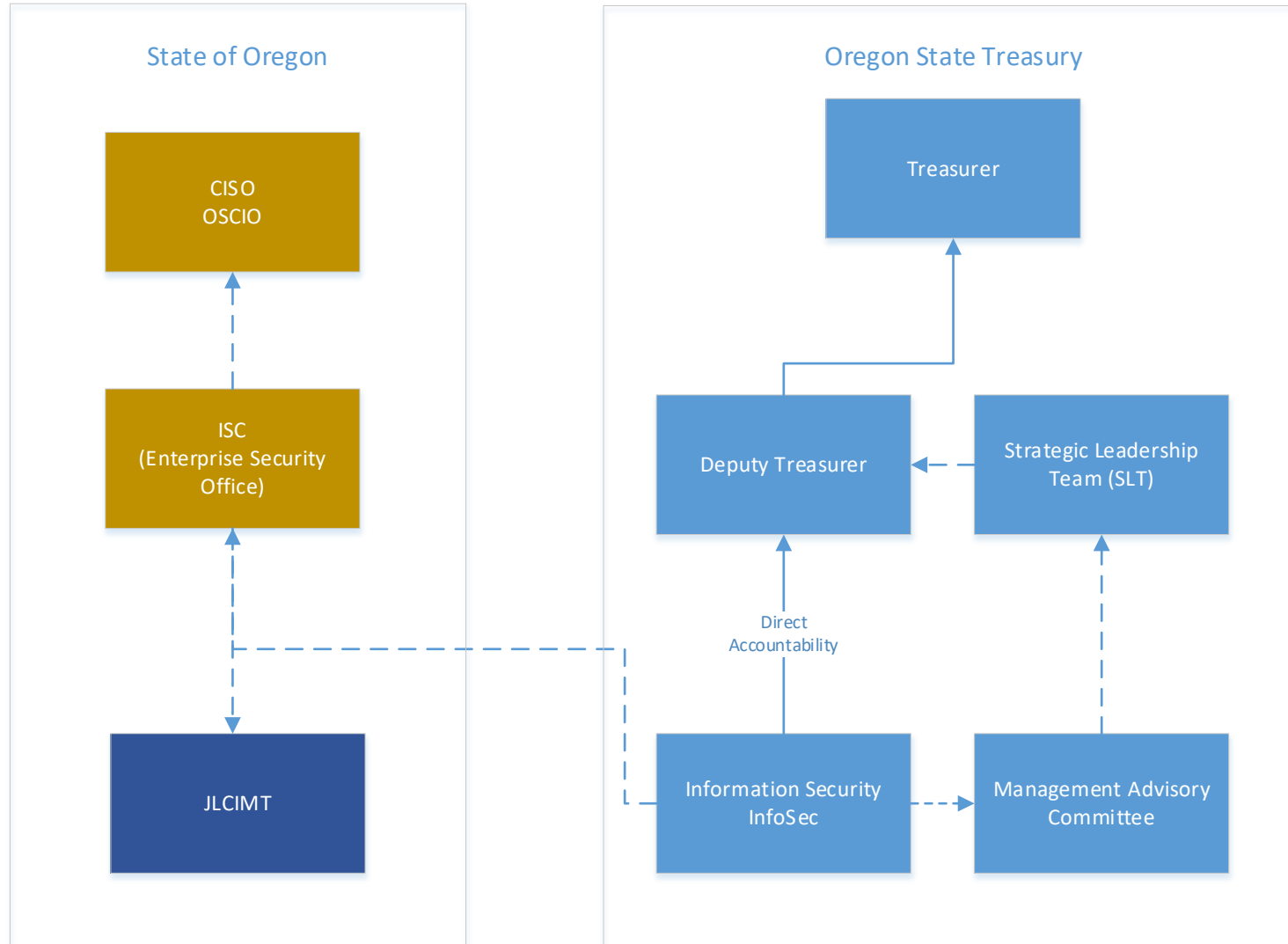
- MBA (October 2018)
- CISSP (2006)/CISM (2015)
- 12 Years of InfoSec experience
- ISO at Adventist Health Systems (2005-2014)
- Systems Admin at HealthNet (2000-2005)
- Co-Founded ProjectNet (1997-2000)
- Internationally Licensed Nurse

Information Security Program

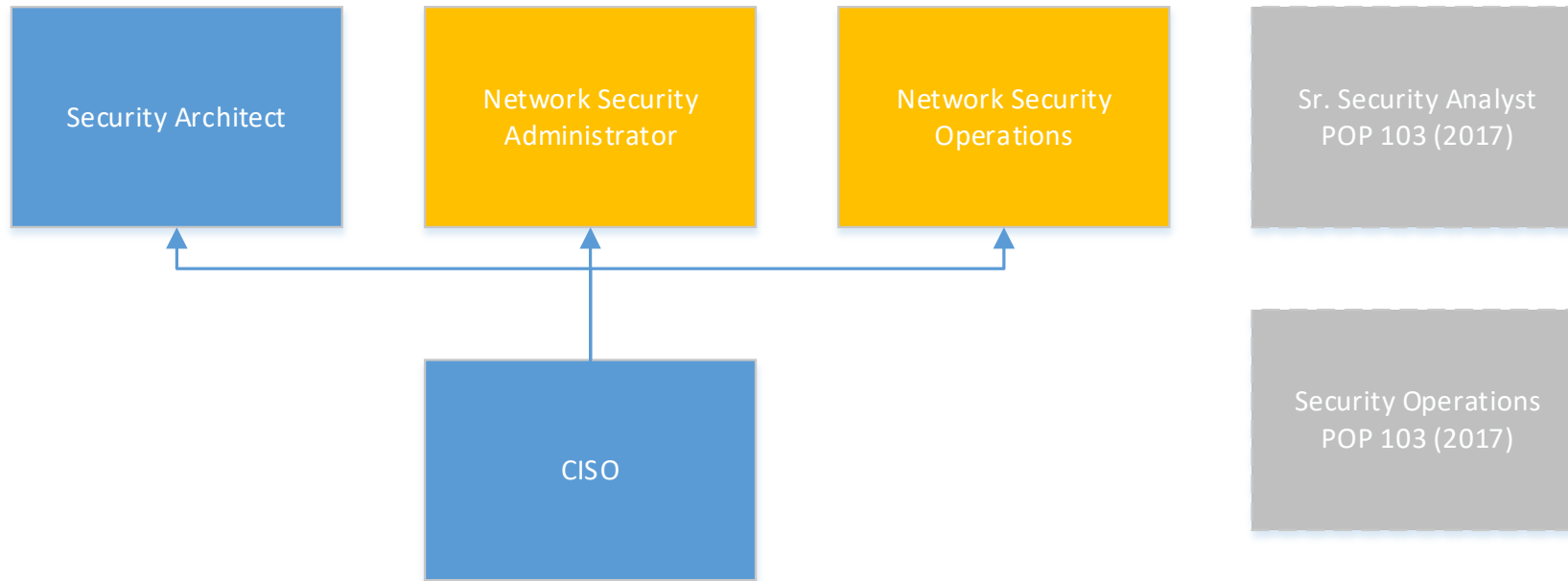
Frameworks

- ISO 27001:2013
- NIST (National Institute of Standards and Technology)
- Cybersecurity Framework v1
- CIS (Center for Internet Security) Critical Security Controls v7
- Oregon Statewide Information Security Standards (2017)
- Oregon Statewide Information Security Plan (2018)

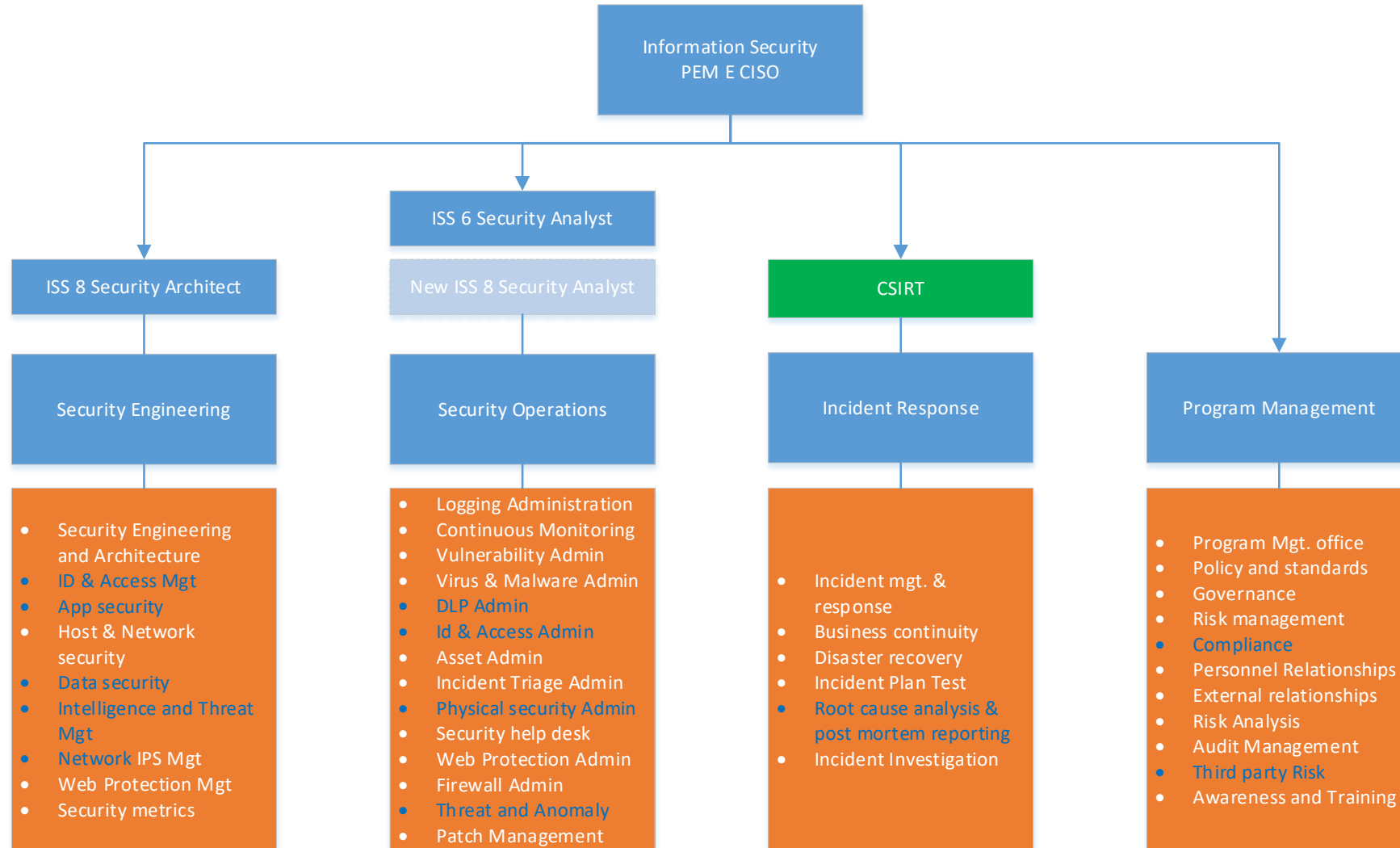
Security Governance



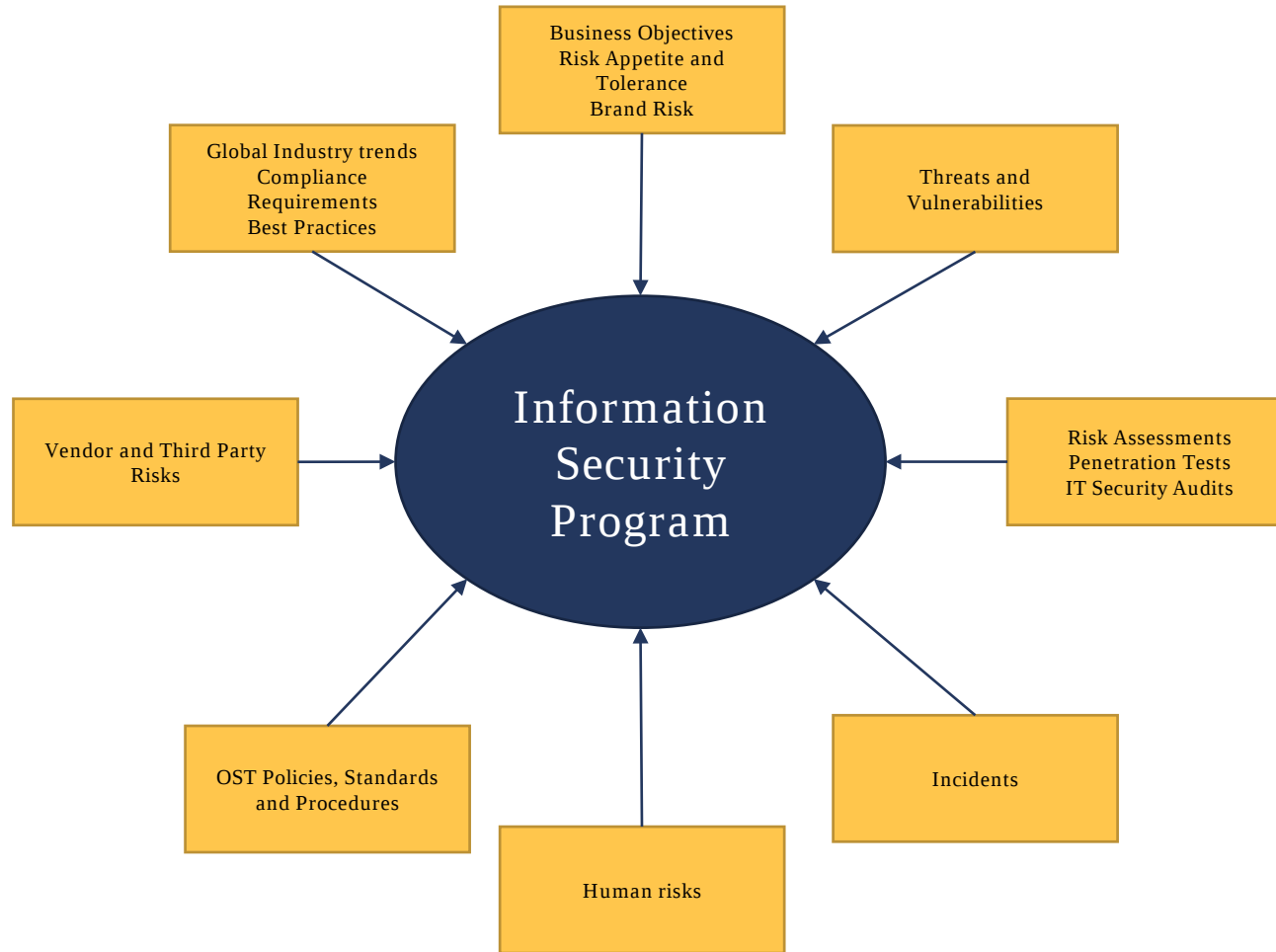
InfoSec Organization



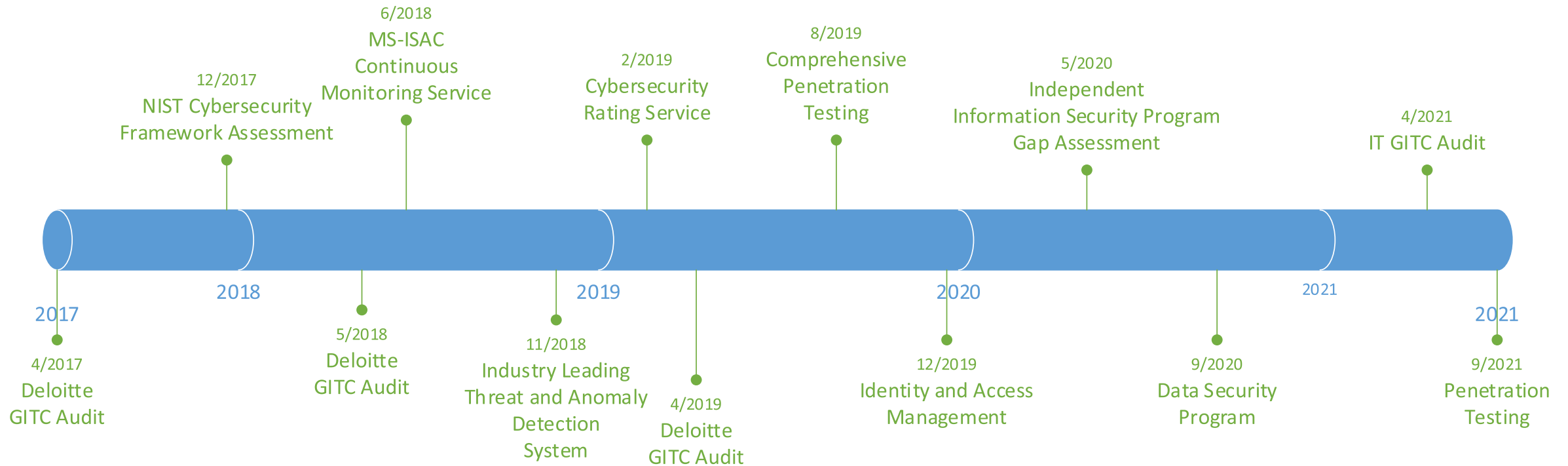
Major Security Functions



InfoSec Key Drivers

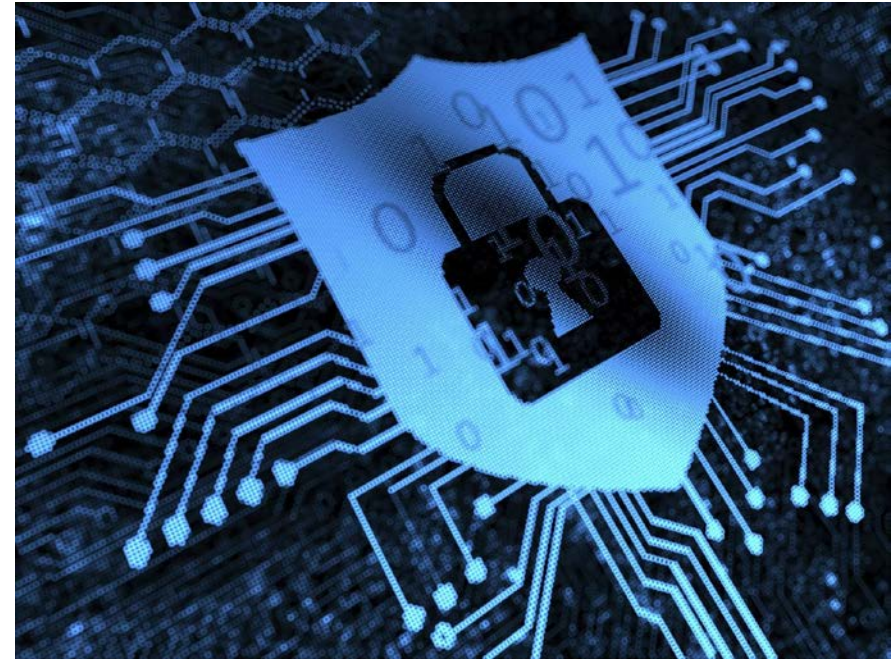


InfoSec Roadmap



Recent/Ongoing Security Assessments

- Functional Incident Response Test and Review by SecureWorks. (October 2017)
- IT General Controls – Change Management Audit by Deloitte. (May 2018)
- Comprehensive penetration test – (2019)
- Security Program Gap Assessment – (2020)
- IT General Controls – (2020)
- Network Penetration Testing – (2021)



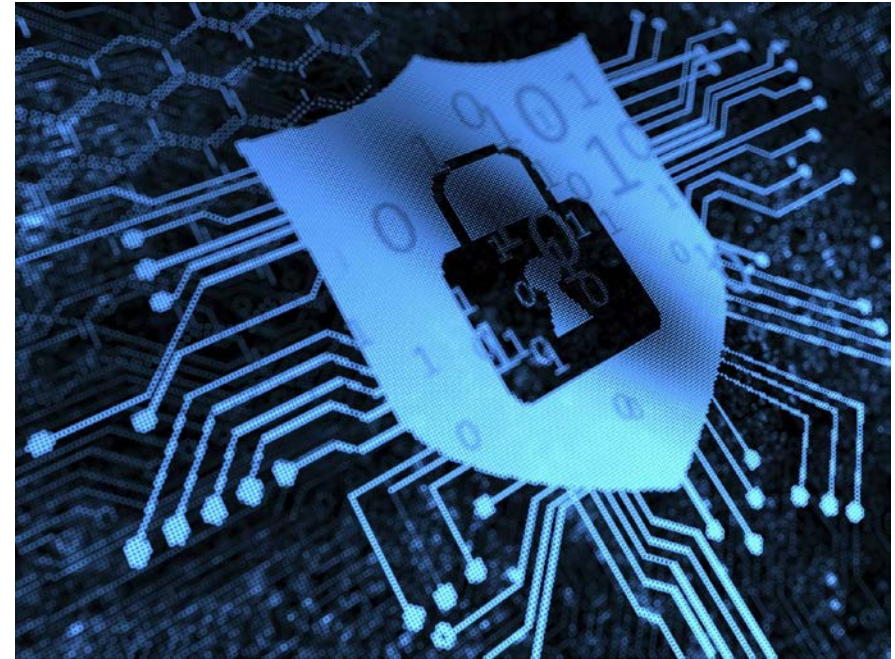
Security Collaboration

- Enterprise Security Office (ESO)
- Enterprise Security Strategy 5-year
- ESO Incident response
- Independent agency security
- Info-Tech Consultation
- Financial Services – Information Sharing and Analysis Center (FS-ISAC)
- Gartner Consultation



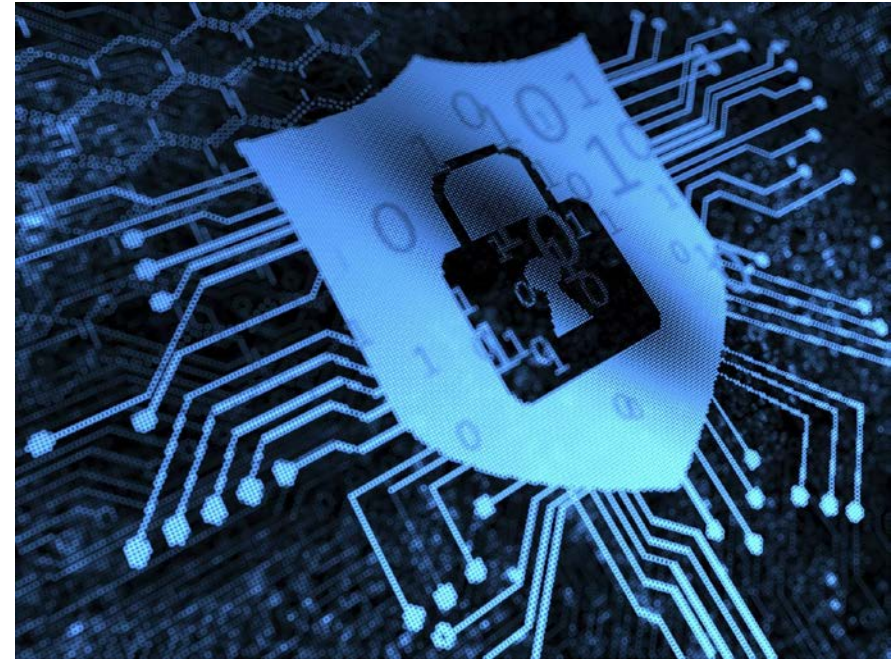
Information Security Investments

- Threat and anomaly detection
- Continuous monitoring
- Information security research and advisory services (Info-Tech/Gartner)
- IAM service provider (Current RFP)
- Cybersecurity rating service
- Risk register



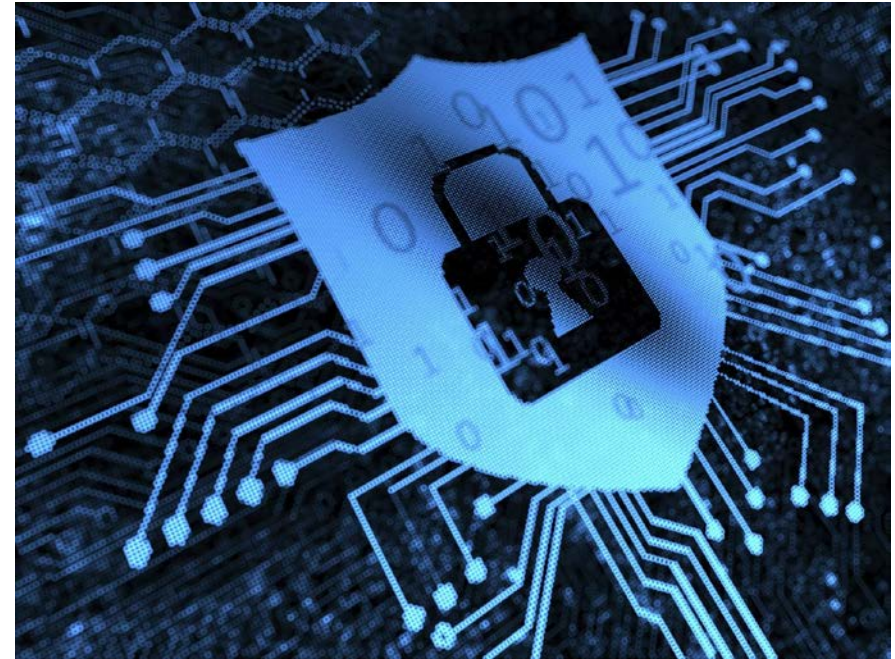
Recent Key Improvements

- Next Generation firewall technology (2017-2018)
- Security Hygiene (2018)
- Third-party security risk management (April 2018)
- Continuous Security Monitoring Service Migration (June 2018)
- Security awareness (September 2018)
- Implementation of Security Threat and Anomaly Detection Capabilities (November 2018)



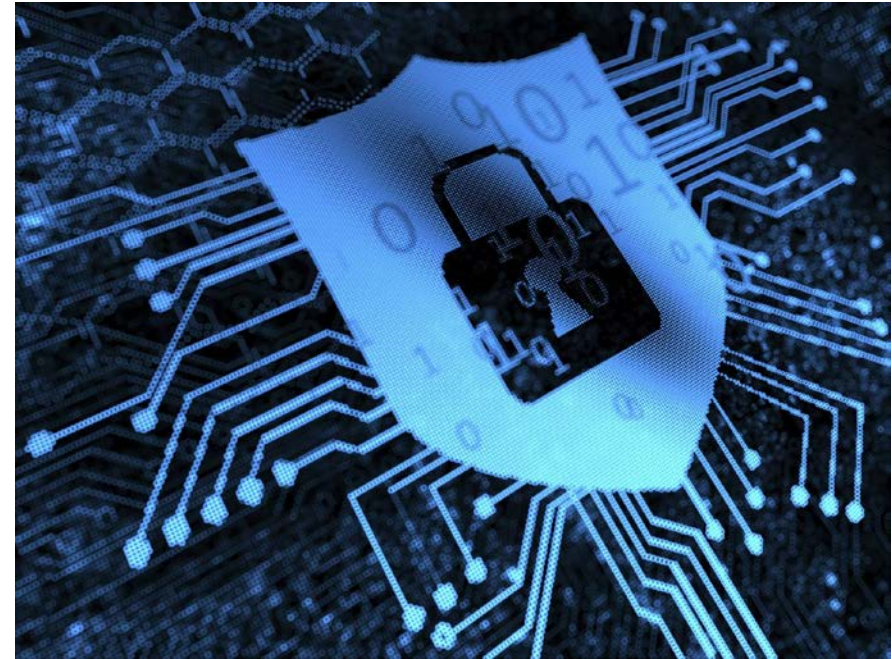
Staff Training

- Security boot camp
- Microsoft Conference
- Security Conferences
 - Annual FS-ISAC Security Conferences
 - Annual RSA Conference
 - Gartner Information Security Summit
- Banking Security Conference
 - US Bank
- SANS Security Training



InfoSec Policies

- ADM 904: Information Classification & Management
- IT 901: Information Security Policy
- IT 902: Acceptable Use Policy
- IT 903: Laptop and Mobile Device Security
- IT 401: Workstation Protection Standard
- IT 402: Vulnerability Management
- IT 403: Malware Protection & Management
- IT 405: Incident Response Policy
- IT 406: Privileged Account Management
- IT 407: Cloud Computing Policy
- IT 408: Third Party Access
- IT 409: Log Management
- IT 410: Account and Access Management
- IT 411: Disposal of Information
- IT 412: Removable Media

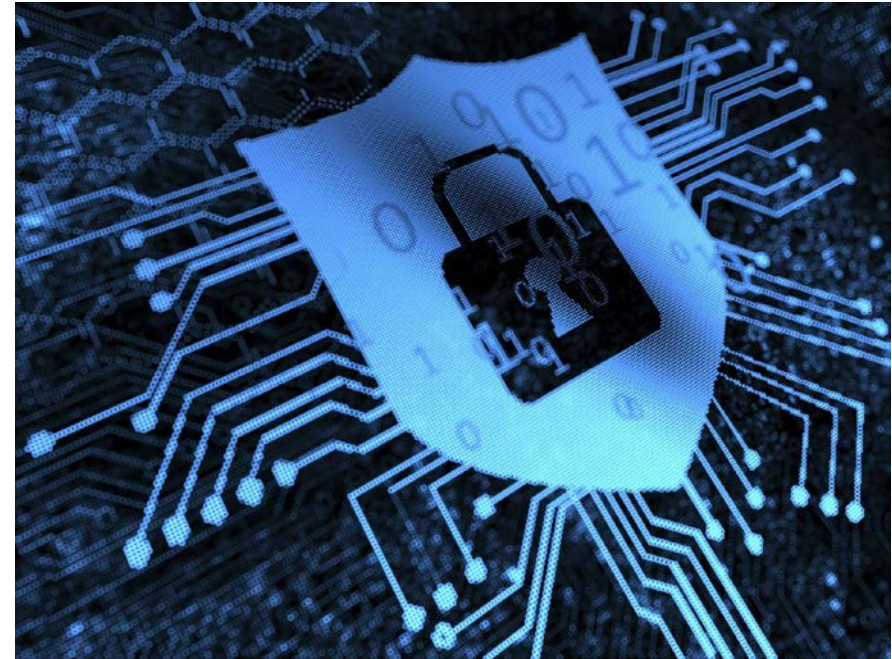


Looking Ahead

#	Project Status	Project Name	Priority	Anticipated FTE Hrs	Start Date	Target Date				2019				2020				2021		
							Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
-		Security Projects		8077																
	●	Identity and Access Management	Very High	880	04/02/18	12/27/19														
	●	Security Maintenance and Operation	High	5040	04/02/18	06/30/21														
	●	Office 365 Project	High	240	10/01/18	06/28/19														
	●	Comprehensive Penetration Testing	Medium	168	10/07/19	03/27/20														
	●	EFT BSR Project	Medium	240	01/07/19	09/25/20														
	●	Data Security Program	Low	880	08/28/19	09/30/20														
	●	Independent Security Gap Assessment	Low	288	04/06/20	06/26/20														
	●	Enhance Malware Detection	Low	168	10/07/19	02/04/19														
		Unforeseen Projects	Medium	168	?	?														
		Total FTE Requirements		4.95																

2019 – 21 InfoSec Strategy

- Mature Information Security Governance processes
- Risk management – Conduct risk assessments, penetration tests and vendor due diligence
- Improve cyber security hygiene – security operations, incident response, vulnerabilities, patches, secure configuration, threat detection and monitoring
- Establish and implement an identity and access management program including privileged access and user access review
- Boost OST perimeter security with advanced persistent threat (APT) detection and protection capabilities
- Establish and implement a data security program including data loss prevention and data encryption
- Enhance security awareness training





OREGON STATE TREASURY

Tobias Read
Oregon State Treasurer

350 Winter St NE, Suite 100
Salem, OR 97301-3896

oregon.gov/treasury