

# FFIEC Changes: How Will They Affect Me?

*October 27, 2021*

---

Viviana Campanaro, CISSP  
Sr. Security & Compliance Solutions Specialist



# FFIEC

Federal Financial Institutions Examination Council

June 30, 2021

New booklet in the FFIEC Information  
Technology Examination Handbook  
series:

**“Architecture, Infrastructure, and  
Operations”**

August 11, 2021

Guidance on effective **authentication**  
and **access risk management** for  
digital banking services and information  
systems.



**New “Architecture, Infrastructure, and Operations” booklet:**

Expanded guidance to help assess the risk profile and adequacy of information technology architecture, infrastructure, and operations.



**New “Architecture, Infrastructure, and Operations” booklet:**

Replaces the “Operations” booklet issued in July 2004.

Provides examiners with expectations regarding architecture and infrastructure planning, governance, risk management and operations of regulated entities.



## **New Authentication guidance:**

Provides examples of effective principles and practices for customers, employees, and third parties accessing digital banking services and information systems.

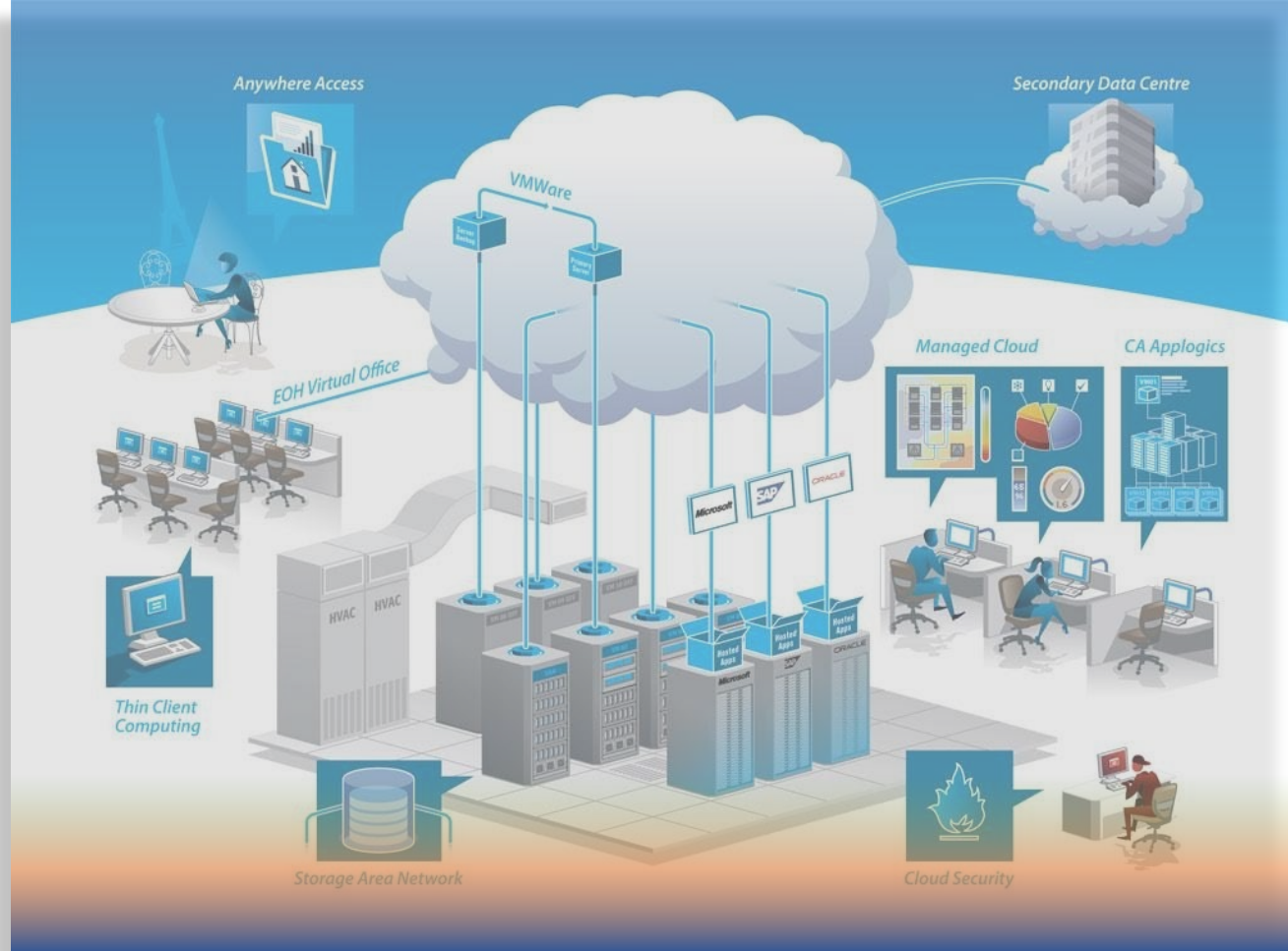
# Business Objectives

First things first:

What's your  
current state?

- 
- ✓ Improve Liquidity
  - ✓ Reduce Costs
  - ✓ Increase Market Share
  - ✓ Innovate and Sustain
  - ✓ Improve Speed to Market
  - ✓ Drive Profitability

Products/Services  
vs.  
IT system  
capabilities, security  
and resilience





Next:

Map your Network

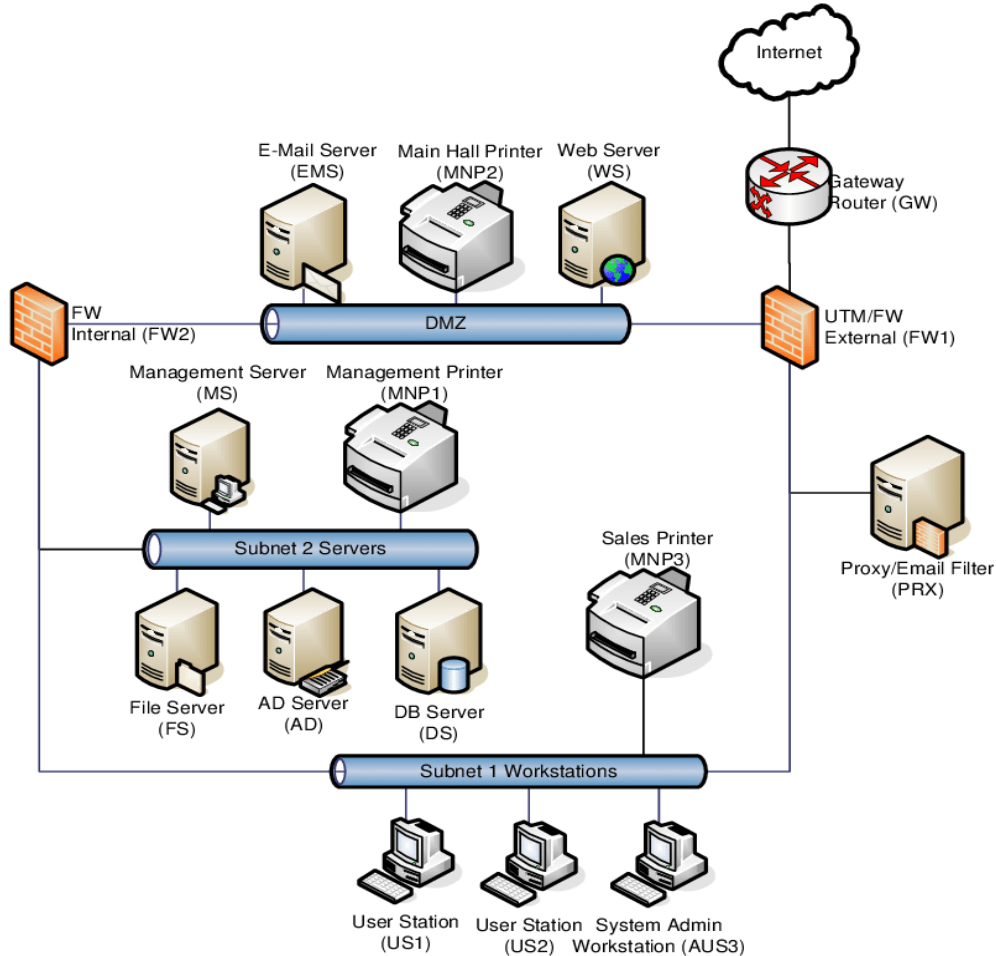
Hardware

Software

Connectivity

ALM

(Audit, Logging, Monitoring)







# FFIEC Examination Handbook

<https://ithandbook.ffiec.gov/>

## FFIEC IT BOOKLETS

Access all the resources associated with the individual handbooks



### AUDIT

Guidance to examiners and financial institutions on the characteristics of an effective technology (IT) audit function



### BUSINESS CONTINUITY MANAGEMENT



### DEVELOPMENT AND ACQUISITION

Guidance to examiners to determine whether an institution identifies and controls information risks



## ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS

Guidance to examiners on enterprise-wide, process-oriented approaches that relate to the design of technology within the overall business structure, implementation of IT infrastructure components, and delivery of services and value for customers.



### E-BANKING

Guidance to examiners on identifying and controlling the risks associated with electronic banking activities



### ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS

Guidance to examiners on enterprise-wide, process-oriented approaches that relate to the design of technology within the overall business structure, implementation of IT infrastructure components, and delivery of services and value for customers.



Guidance to examiners to evaluate risk management processes to establish, manage, and monitor third-party service provider relationships



Guidance to examiners to evaluate systems and related banking activities



### IT SYSTEMS

Guidance to examiners on identifying and controlling risks associated with retail payment systems

## FFIEC IT BOOKLETS

Access all the resources associated with the individual handbooks



### AUDIT

Guidance to examiners and financial institutions on the characteristics of an effective technology (IT) audit function



### BUSINESS CONTINUITY MANAGEMENT



### DEVELOPMENT AND ACQUISITION

Guidance to examiners to determine whether an



## MANAGEMENT

Guidance to examiners outlining the principles of overall governance and IT governance and provides examination procedures to evaluate IT governance and processes for ITRM



### E-BANKING

Guidance to examiners on identifying and controlling the risks associated with e activities



### ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS

Guidance to examiners on enterprise-wide, process-oriented approaches that relate to the design of technology within the overall business structure, implementation of IT infrastructure components, and delivery of services and value for customers.



### OUTSOURCING TECHNOLOGY SERVICES

Guidance and examination procedures for examiners evaluate risk management processes to establish, manage, and monitor third-party service provider relationships



### RETAIL PAYMENT SYSTEMS

Guidance to examiners on identifying and controlling risks associated with retail payment systems and related banking activities



# FFIEC Examination Handbook

<https://ithandbook.ffiec.gov/>

## FFIEC IT BOOKLETS

Access all the resources associated with the individual handbooks



### AUDIT

Guidance to examiners and financial institutions on the characteristics of an effective information technology (IT) audit function



### BUSINESS CONTINUITY MANAGEMENT

Guidance to examiners on the principles of BCM



### DEVELOPMENT AND ACQUISITION

Guidance to examiners to determine whether an institution effectively identifies and controls

risks



### E-BANKING

Guidance to examiners on identifying and controlling the risks associated with electronic banking activities



### ARCHITECTURE, INFRASTRUCTURE AND OPERATIONS

Guidance to examiners on enterprise-wide, process-oriented approaches that relate to the design of technology within the overall business structure, implementation of IT infrastructure components, and delivery of services and value for customers.



## INFORMATION SECURITY

Guidance to examiners on factors to assess information security risks and procedures to evaluate the adequacy of the information security program



Guidance and examination procedures for examiners to evaluate risk management processes to establish, manage, and monitor third-party service provider relationships

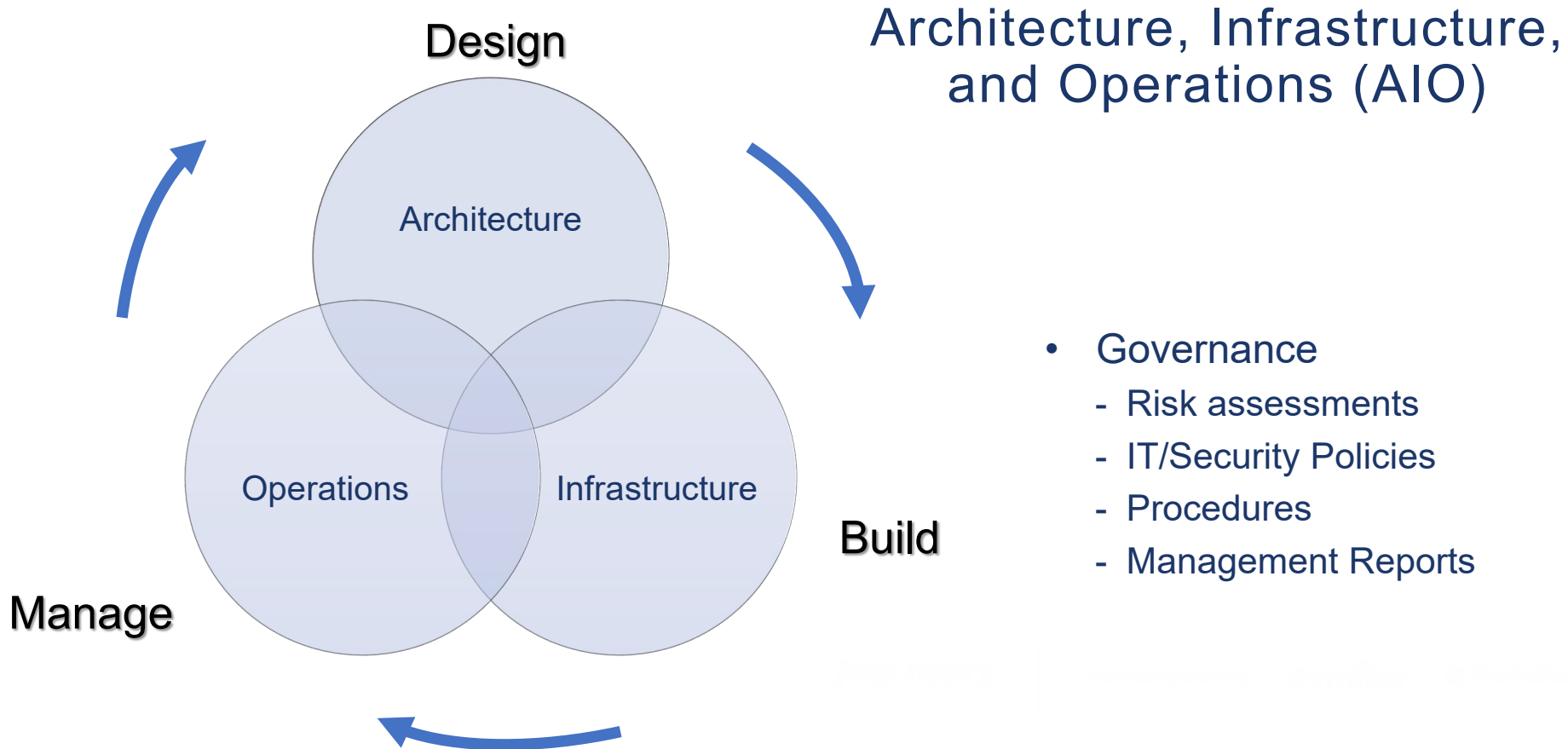


controlling risks associated with retail payment systems and related banking activities



# FFIEC Examination Handbook

<https://ithandbook.ffiec.gov/>





# Architecture, Infrastructure, and Operations (AIO)

## Asset Management

- Roles & Responsibilities
- Security
- Resiliency
- Shadow IT
  - Unauthorized software
  - Unsupported technology



# Architecture, Infrastructure, and Operations (AIO)

## 3<sup>rd</sup> Party Management

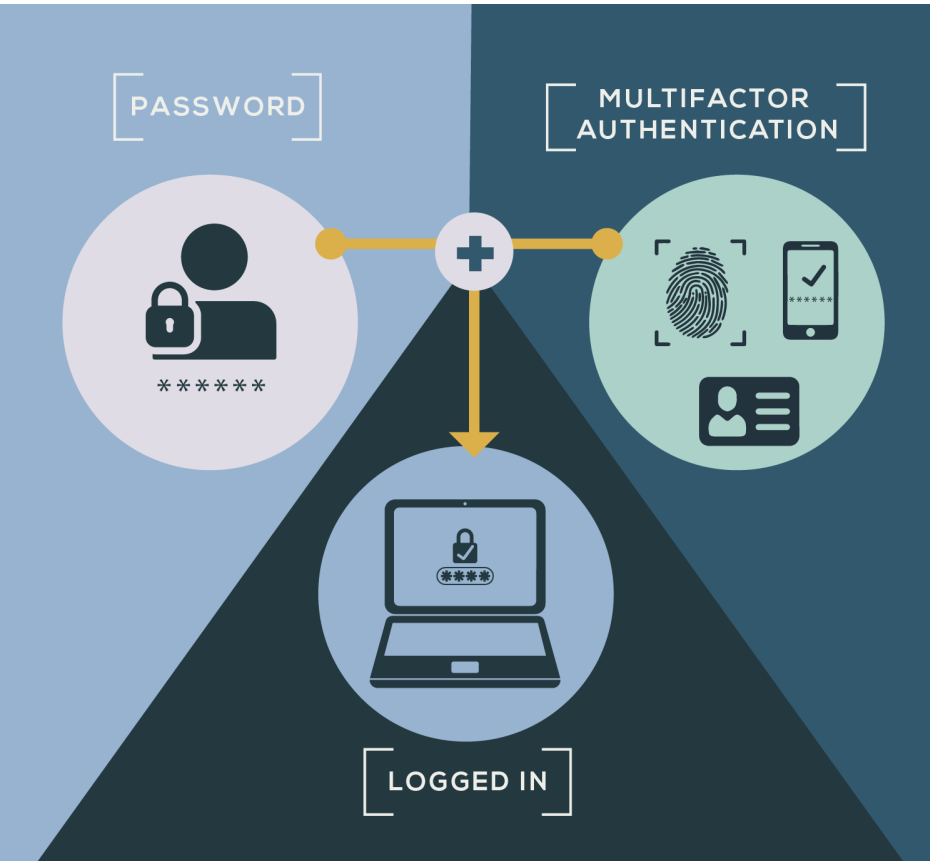
- Roles & Responsibilities
  - Vendor selection/onboarding
  - Vendor relationships
  - 3<sup>rd</sup> Party risk assessments
  - 3<sup>rd</sup> Party budget/spend



# Authentication Guidance

---

- Risk Assessment to determine:
  - Users (employees, vendors, customers)
  - Banking products/services
  - Authentication practices
  - Control effectiveness



# Authentication Guidance

---

- Risk Assessment
- Layered Security
- Multi-Factor Authentication (MFA)
- Monitoring, Logging and Reporting
- Email and Internet systems
- MFA for:
- Outlook Web Access (OWA)
- VPN
- Admin/Privileged users







# Authentication Guidance

---

- Risk Assessment
  - Prior to implementing new services
  - Integrated, enterprise-wide
  - Maintain current access and authentication risks & controls
- Inventory of
  - Information Systems
  - Digital Banking services
  - High-risk transactions
  - High-risk users





# Authentication Guidance

---

- Layered security
  - Preventive
  - Detective
  - Corrective
  - Compensating controls
  - Protect from unauthorized access
- Examples
  - User time-outs
  - System hardening
  - Network segmentation
  - Monitoring processes
  - Transaction amount limits





# Authentication Guidance

---

- Multi-Factor Authentication
  - Part of layered security
  - High-risk transactions / users
  - Something you know
  - Something you have
  - Something you are
- Examples
  - OTP devices (tokens)
  - Keys
  - Passphrases
  - Biometrics





# Authentication Guidance

---

- Monitoring, Logging and Reporting
  - Visibility into unauthorized access
  - Timely response and investigation
  - Promote accountability
- Examples
  - Transaction/audit logs
  - Fraud monitoring
  - Anomaly detection monitoring
  - Fraud response policies





# Authentication Guidance

---

- Email and Internet systems
  - Common attack surface
  - Misconfigured systems
  - Unpatched vulnerabilities
  - Social engineering
  - Phishing
- Examples
  - Browser pop-up blocking
  - URL re-directs
  - MFA for email
  - Awareness education



# Establish and maintain...

- People in the right roles (ISO, Risk Officer, IT Officer)
- Transparency and commitment
- Proper documentation and technology
- Risk appetite/tolerance statement

...to achieve key outcomes



**Regulatory  
Compliance**



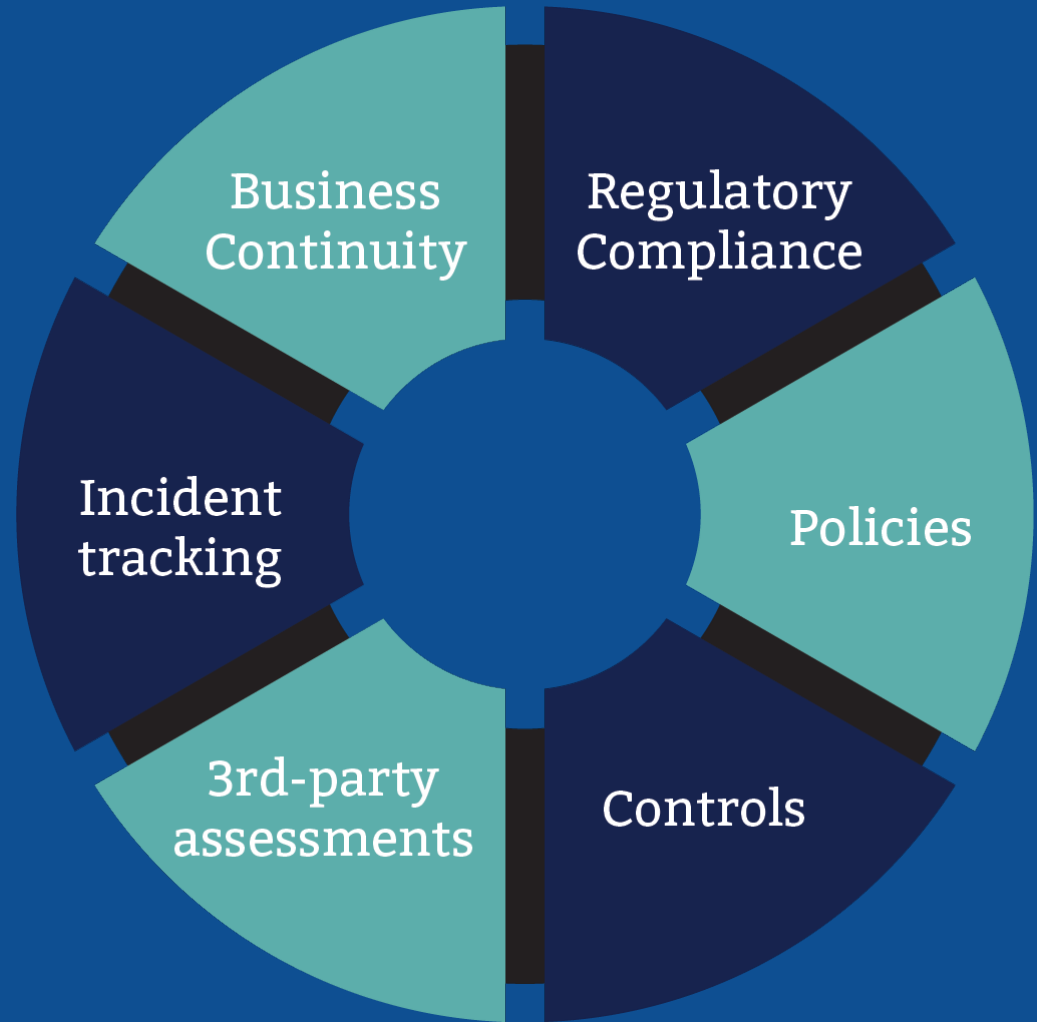
**Authoritative  
Asset Inventory**



**Common Language of  
Risks and Controls**



# Connect across the organization





# Gladiator™ Services



## Total Protect Managed Security Services

- UTM Management & Monitoring
- SIEM Monitoring, Alerting & Reporting
- Incident Alert, Early Breach Detection
- Advanced Malware Protection
- Enterprise Vulnerability Scanning
- OS and Application Patching
- Endpoint Security Management
- Data Backup & Recovery



## Governance, Risk & Compliance Services

- Virtual Information Security Officer
- Information Security Risk Assessment
- Written Information Security Program
- Security Awareness Training
- Business Continuity Management
- Mock Disaster Drills
- Vendor Management
- GRC



## Centurion® - Disaster Recovery Services

- Enterprise Level Backup
- On premise Recovery
- Virtual Server Recovery
- In-house Core Hosted High Availability
- Tape Recovery
- Testing Facilities



## Hosted Network Solutions

- IaaS in JHA's private cloud
- VMWare Virtual Servers
- VMWare Virtual desktop
- Hosted JHA and third-party apps
- Hardware and Microsoft licensing
- Hardware and software maintenance
- SD-WAN services





# About Gladiator

---

## Operations

- Certified System, Network & Security Professionals
  - Network Routing, Virtualization, Windows, Security
  - Cisco, VMWare, Microsoft, Firewalls
- 24/7 Network Monitoring & Management
- 24/7 Security Operations Center
- Governance Risk & Compliance Center
- Remote End-User Help Desk
- Located in the USA





# CYBERSECURITY FORUM



SAFER. SMARTER. TOGETHER.

## When

Thursday, November 18, 2021 | 10 A.M. – 4 P.M. CT

## Where

Hyatt Regency | Louisville, KY

## Cost

FREE (\$1,495 Value)

THE RANSOMWARE ROLLER COASTER:  
ARE YOU READY TO RIDE?

New this year: Hear about Jack Henry's modern  
approach to cyber defense.

Register Now: <https://discover.jackhenry.com/jack-henry-cybersecurity-forum>

# Thank You!

Viviana Campanaro, CISSP  
[vcampanaro@jackhenry.com](mailto:vcampanaro@jackhenry.com)