

Risk, Security and GRC: How to Avoid Audit Findings

Viviana Campanaro – CISSP

Senior Security & Compliance Solutions Specialist

December 2, 2021



Shoes here...

...and here...

...and here...!

An Audit Tale

Risk, Security & GRC



An Audit Tale

- FDIC / NCUA examination findings

Access Controls – Administrative Accounts
Finding:

“Weak password criteria and management of default administrator accounts.”

If you Fail to prepare, prepare to fail.



An Audit Tale

- FDIC / NCUA examination findings

Information Security Program

Finding:

“Information Security Policy does not fully document activities or include processes which are repeatable and measurable.”

If you Fail to prepare, prepare to fail.



An Audit Tale

- FDIC / NCUA examination findings

Governance

Finding:

“No comprehensive metrics to evaluate the effectiveness of the Information Security Program and provide early indication of a breakdown in the control environment.”

If you Fail to prepare, prepare to fail.



An Audit Tale

- FDIC / NCUA examination findings

Risk Assessment

Finding:

“Insufficient detailed information to help prioritize actions and make business decisions.”

If you Fail to prepare, prepare to fail.



An Audit Tale

- FDIC / NCUA examination findings

Vendor Due Diligence

Finding:

“Policies and procedures do not properly document the review and verification of third-party SOC reports.”

If you Fail to prepare, prepare to fail.

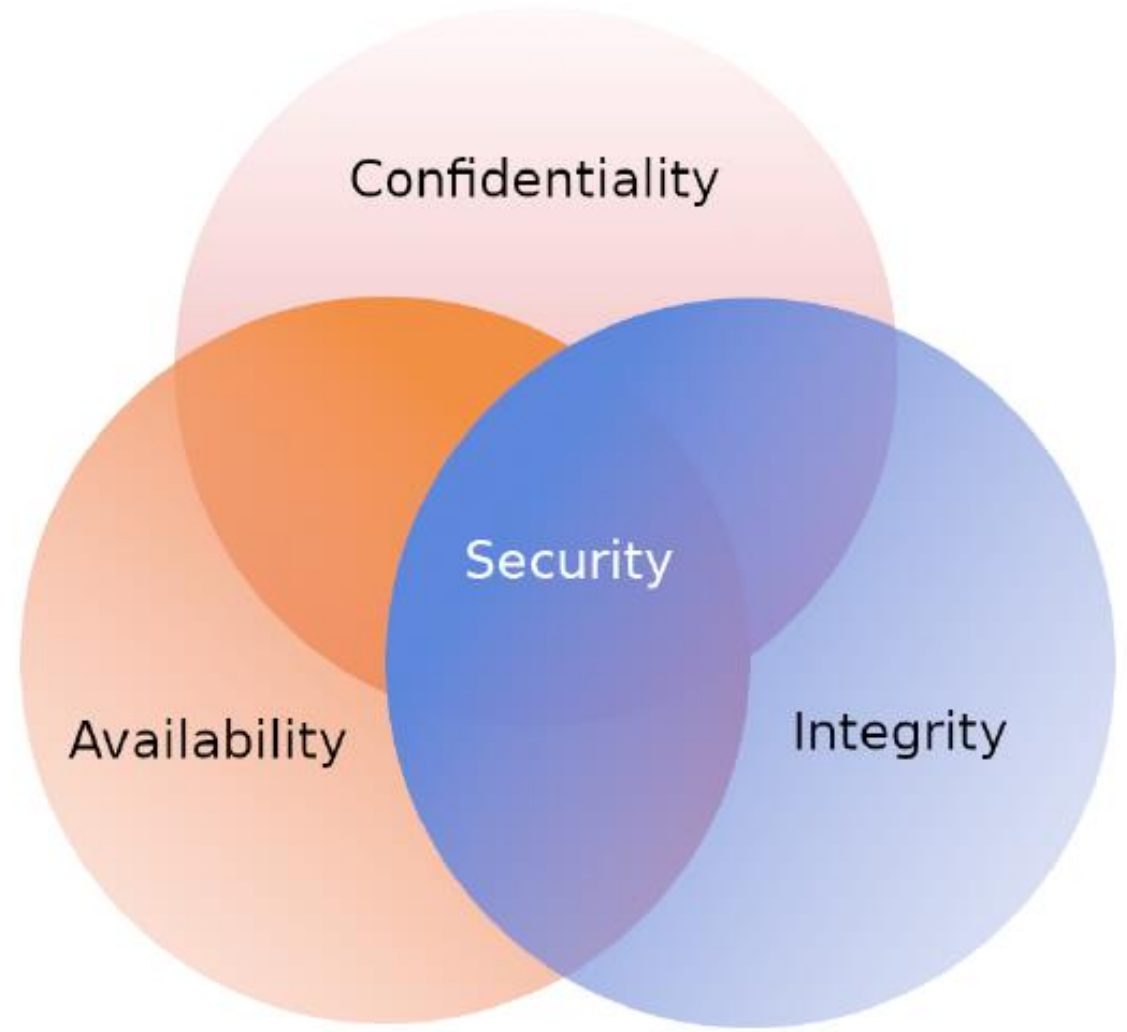


A Strong Foundation

Risk, Security & GRC

Information Security Program

- It's about Protection of critical information assets



Establish and maintain...

- People in the right roles (ISO, Risk Officer, IT Officer)
- Transparency and commitment
- Proper documentation
- Appropriate technology

...to achieve key outcomes



**Authoritative Asset
Inventory**



**Common Language of
Risks and Controls**



**Regulatory
Compliance**

Authoritative Asset Inventory

- Set asset types/categories
- Assign business owners
- Determine inherent risk
- Determine required controls
- Monitor and report



Common Language of Risks and Controls

- Risk categories and rating scales
- Business owners
- Control categories
- Measure and report



Governance, Risk, and Compliance (GRC)

- Strategy of alignment and visibility
- Common language of risks and controls
- Technology-enabled



Governance

- ✓ Set strategy and objectives
- ✓ Determine risk appetite
- ✓ Monitor/measure performance



Risk

- ✓ Risk appetite
- ✓ Mitigate, accept, avoid, or transfer



Compliance

- ✓ Relevant laws, regulations, and corporate policies
- ✓ Validate that risk mitigation practices are effective

FFIEC Examination Handbook

★FFIEC
IT EXAMINATION
HANDBOOKS

IT BOOKLETSIT WORKPROGRAMSGLOSSARYFFIEC HOME


Q?


FFIEC IT BOOKLETS

Access all the resources associated with the individual handbooks

AUDIT

Guidance to examiners and financial institutions on the challenges of examining technology





BUSINESS CONTINUITY
MANAGEMENT

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





DEVELOPMENT AND ACQUISITION

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





E-BANKING

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.





ARC AND OPERATIONS

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






INFORMATION SECURITY


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






SERVICES

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



SYSTEMS

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



FFIEC Examination Handbook

FFIEC IT BOOKLETS

Access all the resources associated with the individual handbooks



AUDIT

Guidance to examiners and financial institutions

on the characteristics of an eff
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 iden
controlling the risks associated
activities



ARCHITECTURE, INFRA STRUCTURE 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.



SERVICES

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



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



FFIEC Examination Handbook

| FFIEC IT EXAMINATION HANDBOOK | | IT BOOKLETS | IT WORKPROGRAMS | GLOSSARY | FFIEC HOME | Q ? |
|--|--|-------------|-----------------|----------|------------|-----|
| Table of Contents | | | | | | |
| Information Security | | | | | | |
| Introduction | | | | | | |
| I Governance of the Information Security Program | | | | | | |
| I.A Security Culture | | | | | | |
| I.B Responsibility and Accountability | | | | | | |
| I.C Resources | | | | | | |
| II Information Security Program Management | | | | | | |
| II.A Risk Identification | | | | | | |
| II.A.1 Threats | | | | | | |
| II.A.2 Vulnerabilities | | | | | | |
| II.A.3 Supervision of Cybersecurity Risk and Resources | | | | | | |
| II.A.3(a) Supervision of Cybersecurity Risk | | | | | | |
| II.A.3(b) Resources for Cybersecurity Preparedness | | | | | | |
| II.B Risk Measurement | | | | | | |
| II.C Risk Mitigation | | | | | | |

Ensuring Audit Success

Reports and Documentation



- Provide visibility
- Enforce accountability
- Show the work
- Evidence for audit

An Audit Tale

- Management Response

Access Controls – Administrative Accounts

Corrective Action:

“Enhanced password criteria and management of default administrator accounts. Implemented monthly review of administrator access to critical systems.”



An Audit Tale

- Management Response

Information Security Program

Corrective Action:

“Updated Information Security Policy to document activities and include processes which are repeatable and measurable.”



An Audit Tale

- Management Response

Governance

Corrective Action:

“Established comprehensive metrics to evaluate the effectiveness of the Information Security Program and provide early indication of a breakdown in the control environment.”



An Audit Tale

- Management Response

Risk Assessment

Corrective Action:

“Detailed remediation information will include mitigation response, assigned individuals and target completion dates to help prioritize actions and enable management to make informed business decisions.”



An Audit Tale

- Management Response

Vendor Due Diligence

Corrective Action:

“Policies and procedures will be enhanced to properly document and assign the review and verification of third-party SOC reports to the right individuals.”



Have a Plan

Measure
Success





Gladiator® Governance Risk and Compliance Services

- GRC SaaS Platform
- Virtual Information Security Officer
- InfoSec Asset Based Risk Assessment
- Written Information Security Policy
- Business Continuity Management
- Vendor Management
- Security Education Services

Unleashing the Power of GRC (blog)

<https://discover.jackhenry.com/fintalk/unleashing-the-power-of-grc>

Security Risk Assessments – A Balance of Risk and Controls (article)

<https://discover.jackhenry.com/fintalk/security-risk-assessments-a-balance-of-risk-and-controls>



Next in our Webinar Series

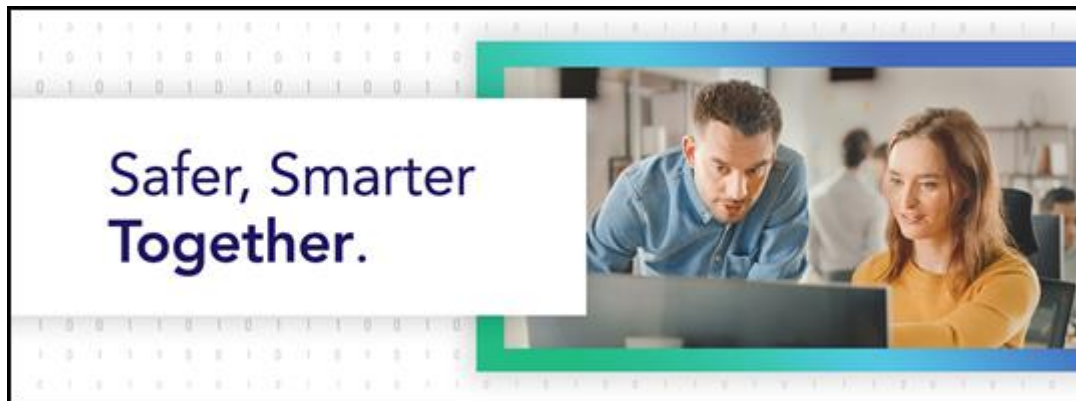
Cyber Threats and Trends for 2022

Wednesday, January 26, 2022

2:00 p.m. CT

Register Now:

<https://discover.jackhenry.com/cyber-security/new-webinars>



jack henry
& ASSOCIATES INC.

jack henry Banking

Symitar

ProfitStars

THANK YOU!