Agenda

Introduction to FIS


Cybersecurity Compliance & Cyber Resilience

Cyber Resilience Frameworks Overview

Questions & Answers
ABOUT FIS

FIS™ is a global leader in financial services technology, with a focus on retail and institutional banking, payments, asset and wealth management, risk and compliance, consulting, and outsourcing solutions. Through the depth and breadth of our solutions portfolio, global capabilities and domain expertise, FIS serves more than 20,000 clients in over 130 countries. Headquartered in Jacksonville, Fla., FIS employs more than 55,000 people worldwide and holds leadership positions in payment processing, financial software and banking solutions. Providing software, services and outsourcing of the technology that empowers the financial world, FIS is a Fortune 500 company and is a member of Standard & Poor’s 500® Index. For more information about FIS, visit www.fisglobal.com.
FIS – Unmatched Expert Advisor

FIS’ Expert Team
- Experts who are former bank examiners, attorneys, compliance officers, risk managers, law enforcement, bank executives
- Experts with 15+ years subject matter expertise in all areas of risk management ranging from BSA/AML, fraud management, DFAST, CCAR, model validation, consumer compliance, fair lending, information security, PCI, privacy, cybersecurity, mortgage lending/servicing, UDAAP, vendor risk management, safety and soundness, and more

Diverse Clients
- Range from community banks to FIs over $250B
- Specializing in clients over $50B
- Clients also include:
  - FDIC
  - CFPB
  - FRB
  - NCUA
  - State regulators
- Training partner to banking regulators. (e.g. trainer to CFPB examiners and consumer response staff)

Industry-Leading Risk Management Best Practices
- Several hundred complex consulting engagements
- Dozens of high-profile, concurrent engagements
- Frequently hired by banking regulators or recommended to banks on enforcement actions
- Unique deep expertise in BSA/AML, model validation, CCAR, DFAST, consumer compliance, fair lending, UDAAP, mortgage lending/servicing, cybersecurity, vendor risk management and more
FIS – Unparalleled Thought Leadership

Providing Actionable Regulatory Intelligence

- Through the Center, FIS interfaces with key policymakers and regulators to provide its clients with early insight on regulatory changes and emerging issues
- We offer bi-weekly Regulatory Intelligence Briefings (RIBs) only to FIS clients

FIS’ Risk, Information Security and Compliance (RISC) Summit

FIS’ annual thought leadership event with distinguished speakers, regulators and industry experts

Industry-Leading Risk Management Best Practices

Unique deep expertise in BSA/AML, model validation, CCAR, DFAST, consumer compliance, fair lending, UDAAP, mortgage lending/servicing, cybersecurity, vendor risk management and more
FIS – Comprehensive, Highly-Effective Solutions

**EXPERT CONSULTING**
- Co-sourcing / Outsourcing
  - Enterprise Risk Assessment
  - DFAST Stress Testing Review
  - Compliance Monitoring and Testing
  - BSA/AML CTR / SAR Analysis
  - BSA/AML Staff Augmentation
  - BSA/AML Audit
  - Fraud Analysis
  - Model Validation
  - Mortgage Quality Control
  - Mortgage Servicing Testing
  - Compliance Training
  - Information Security
  - Cybersecurity Assessment Review

**TECHNOLOGY SOLUTIONS**
- Essential Tools
  - Early Risk Manager
  - Prime Compliance Suite
  - WatchListIQ
  - Memento Fraud Detection
  - CyberForce Anomalous Activity Detection
  - BISG Fair Lending Analyzer
  - TRID Compliance Analyzer
  - Mortgage Servicing Analyzer
  - Compliance Risk Indicator
  - CallReporter
  - BankTrends
  - Regulatory University

**MANAGED SERVICES**
- Mission-critical Managed Services
  - Compliance Management System (CMS) Optimizer
  - Regulatory Advisory Service
  - CISO Service
  - Cybersecurity Assessment Management
  - Internal Defense (IT Asset Monitoring)
  - Perimeter Defense (Vulnerability Scanning)
  - Vendor Risk Management
Expert Consulting Example: Enterprise Risk Assessment using FIS Early Risk Manager
Technology Solution Example: CyberForce

CyberForce detects anomalous activity as required per FFIEC Cybersecurity Assessment

- Privileged user credential hijacking monitoring
- Powerful data analytics engine
- Alerts, Dashboard, Forensics, Case Management
Managed Services Example: Vendor Risk Management, Perimeter Defense and Internal Defense

**Vendor Risk Manager**

- Centralizing the due diligence of third party risk via FIS’ people, process and platform end-to-end
  - Configurable, quantitative Risk Scoring
  - Configurable Inherent Risk Scoring (Completion, Monitoring, Support)
  - >300 Global Watch List Checks
  - Ongoing Financial Health Monitoring (Public and Private Sectors)
  - Regulatory (OCC) and Industry (PCI/CFPB) Compliance Monitoring
  - Vendor Control Assessment and Audit Review Completion/Support
  - Real time access to FIS Professional Risk Support Services

**Perimeter Defense**

- Identifying and prioritizing vulnerabilities that are exposed to the public internet daily
  - Daily External Vulnerability Identification
  - Configurable Vulnerability Risk Scoring and Prioritization
  - Custom Risk Remediation Timelines
  - Vulnerability Management and workflow
  - Custom Scan, Vulnerability and End User Reports
  - Real time access to FIS Professional Security Support Services

**Internal Defense**

- Discovering and monitoring IT assets, internal vulnerabilities, and end point controls
  - Weekly Internet Device Vulnerability Identification
  - Ongoing Device End Point Control Compliance Monitoring
  - Custom Vulnerability Risk Scoring and Prioritization
  - Custom Risk Remediation Timelines
  - Vulnerability Management and workflow
  - Custom Scan, Vulnerability and End User Reports
  - Real time access to FIS Professional Security Support Services
Regulatory Climate: EU Cybersecurity Directive and FSOC 2016
YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your MoneyPak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address fine@fbi.gov.

green dot MoneyPak

Where I can buy MoneyPak?

RITE AID

CVS

7-11
Ultra Malware – Malware that acts like another type of malware like Ransomware but is in fact a remote access Trojan designed to monitor systems for transactional activities.
Bangladesh, Vietnam, & Ecuador

What do these countries have in common?

Banks were hacked through the SWIFT International Remittance network.

$951 M Scheduled
$81 M Routed
$0 Recovered

$1.2 M Scheduled
$0 Routed

$12 M Scheduled
$12 M Routed
$0 Recovered
Released July 6, 2016 – Becomes EU Law 2018

As law, it creates minimum standards and obligations for member states and their organizations to insure protections against cybersecurity risk, which include confidentiality, integrity, and availability. As well as a mandate to assess penalties for violating these standards.

Key Provisions include: Obligations over cooperation, information exchange, incident response, notifications, and the definition of a “disruptive effect”.

- Number of Users
- Dependency on other businesses and critical infrastructure
- Degree and duration of harm on the economy, society, and public safety
- Market share of business
- Geographic spread of incidents
- Alternative means of service possible

Standardization of Risk Assessment methods and a single point of contact for incident response.

Definition of “Essential Services” and “Digital Service Providers”.
Definition of “Essential Services” – The EU Directive

**Internet Exchange Point (IXP)** – An IXP exists to interconnect networks that are technically and organizationally separate. These are typically Internet Service Providers or Content Delivery Providers like Amazon or Akamai who use IXPs to accelerate content delivery and improve Internet data speeds.

**Domain Name Service (DNS) Service providers** – A type of Internet hosting provider that translates network addresses to word friendly Internet names such as [www.yourbank.com](http://www.yourbank.com).

**Top Level Domain Name Registries** – Organizations that control the registration of Internet domain names such as “.com” or “.org”.

**“Digital Service Providers”**

**Online marketplace** – A service that allows consumers and/or traders to conclude online sales or service contracts with traders either on the online marketplace’s website or on a trader’s website that uses computing services provided by the online marketplace. Other activities include processing transactions, aggregating data or profiling of users, along with application stores.

**Online search engine** – A service that allows users to perform searches with key words and returns links in which information requested can be found.

**Cloud computing services** – A service that enables access to a scalable and elastic pool of shareable computing resources.
FSOC Annual Report 2016

Created by the Dodd-Frank Act, its mission is to:

• To identify risks to the financial stability of the United States that could arise from the material financial distress or failure, or ongoing activities, of large, interconnected bank holding companies or nonbank financial companies, or that could arise outside the financial services marketplace.

• To promote market discipline, by eliminating expectations on the part of shareholders, creditors, and counterparties of such companies that the U.S. government will shield them from losses in the event of failure.

• To respond to emerging threats to the stability of the U.S. financial system

• The Annual Report was released on June 21, 2016

• It is considered to be the most powerful finance council in the US government.
Key Points To Consider:

• FSOC considers cyber threats to be the number 1 risk to the US financial services sector. They state:

  “Cyber threats and vulnerabilities continue to be a pressing concern for companies and governments in the United States and around the world. Significant investment in cybersecurity by the financial services sector over the past several years has been critical to reducing cybersecurity vulnerabilities within companies and across the sector as a whole, and such investments should continue. **Government agencies and the private sector should continue to work to improve and enhance information sharing, baseline protections such as security controls and network monitoring, and response and recovery planning.**”

• They also consider malware attacks as unique threats that must be detected and responded. They state:

  “Destructive malware attacks represent a **unique threat** in that they are both infrequent and yet potentially catastrophic. Financial institutions, working with government agencies, should understand this risk and take steps to improve cybersecurity, engage in information sharing efforts, and prepare to respond to, and recover from, a major incident. These preparations should include consideration of the technical impacts, appropriate response mechanisms, business implications, and possible effect on the financial system.”
Observations

• Up until the EU Directive and the FSOC Annual Report, Cybersecurity was considered an additive threat actor that can be addressed with existing IT controls issued by Regulatory agencies.

• FSOC’s handling of Cybersecurity has significant innuendo for financial institutions over $50 billion dollars who just finished their liquidity and capital stress testing exercises. It implies that the US will have similar legal obligations and more importantly will emphasis testing for Cybersecurity protections just like liquidity and capital testing.

• Organizations must also have the capability to detect and respond to the unique threat of malware.

• Organizations in the US, whether regulated or not will have to face inevitably the consequences of Cybersecurity Compliance regime.
Cybersecurity Compliance & Cyber Resilience
FFIEC Business Continuity Planning Handbook

Table of Contents

- Introduction 1
- Board and Senior Management Responsibilities 2
- Business Continuity Planning Process 3
- Business Impact Analysis 5
- Risk Assessment 8
- Risk Management 9
- Business Continuity Plan Development 9
  - Assumptions 11
- Internal and External Components 11
- Mitigation Strategies 12
- Risk Monitoring and Testing 12
  - Principles of the Business Continuity Testing Program 13
  - Roles and Responsibilities 14
  - Testing Policy 15
- Execution, Evaluation, Independent Assessment, and Reporting of Test Results 20
- Updating Business Continuity Plan and Test Program 22
- Other Policies, Standards and Processes 22
  - Security Standards 23
  - Project Management 23
  - Change Control Policies 24
  - Data Synchronization Procedures 24
  - Crisis Management 24
  - Incident Response 25
  - Remote Access 25
  - Employee Training 26
  - Notification Standards 26
  - Insurance 26

FEBRUARY 2015
If you don’t know where to start the cyber resilience journey, this is the definitive and “how to” guide.

First Published in March 2003. Substantially unchanged up to February 2015

Major catalyst for the update involved a recognition of Cyber Resilience as a key requirement of a BCP Program.

Documents and work programs are freely downloadable from the FFIEC Website.

Provides examination guidance for institutions preparing for a BCP review. Hint: Audit insider’s guide on what is expected.

We’ll take a peek at the changes and where updates may need to happen as a result of these changes.
## FFIEC Business Continuity Planning Handbook

### Cyber Resilience

Cyber Resilience adds new threats to be evaluated in the BCP Plan.

### Standard vs. New Risks

<table>
<thead>
<tr>
<th>Standard</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud, Theft, or Blackmail</td>
<td>Malware</td>
</tr>
<tr>
<td>Terrorism</td>
<td>Simultaneous Attacks on Financial Institutions and TSPs</td>
</tr>
<tr>
<td>Severe Weather</td>
<td>Insider Threats</td>
</tr>
<tr>
<td>Comm. Failure</td>
<td>Strategic Considerations</td>
</tr>
<tr>
<td>Electronic Payment System Providers</td>
<td></td>
</tr>
<tr>
<td>Sabotage</td>
<td></td>
</tr>
<tr>
<td>Fire</td>
<td></td>
</tr>
<tr>
<td>Air Contaminants</td>
<td></td>
</tr>
<tr>
<td>Customers</td>
<td></td>
</tr>
<tr>
<td>Affiliates, Vendors, and Service Providers</td>
<td></td>
</tr>
<tr>
<td>Vandalism &amp; Looting</td>
<td></td>
</tr>
<tr>
<td>Flood</td>
<td></td>
</tr>
<tr>
<td>Hazardous Spill</td>
<td></td>
</tr>
<tr>
<td>Employees</td>
<td></td>
</tr>
<tr>
<td>Power Failure</td>
<td></td>
</tr>
<tr>
<td>Data or Systems Destruction and Corruption</td>
<td></td>
</tr>
<tr>
<td>Communication Infrastructure Disruption</td>
<td></td>
</tr>
<tr>
<td>Equipment &amp; Software Failure</td>
<td></td>
</tr>
<tr>
<td>Transportation System Disruption</td>
<td></td>
</tr>
<tr>
<td>Water System Disruptions</td>
<td></td>
</tr>
</tbody>
</table>

### Updated February 2015

Appendix J: Strengthening the Resilience of Outsourced Technology Service Providers
Each of the new threat type should undergo a BIA, RTO analysis, and Plan Update for each aspect of a business process and/or unit.

Scenarios must be conducted to take into account DDoS attacks and Malware both with and without a TSP.

Incident response must not simply take into account managing the crisis, but planning for resiliency from attack (Cyber DRaaS).
Common Pitfalls To Watch Out For

Do you have a discussion with the CEO on the BCP Program based on the information collected from business leaders?

When was the last update of the plan?

Are your Recovery Time Objectives realistic for the company’s current capabilities?

Can you recall the last time you performed an integrated test?

What is the Crisis Management Team and do they know what to do exactly?

How closely do you monitor critical TSPs for recovery capabilities?

Do you include “Essential Services” and “Digital Service Providers”?

What are the detective controls in place to be alerted to an emerging resiliency threat?

Can you withstand and recover from a cyber attack?
Cyber Resilience Frameworks Overview
Advanced Cyber-Resilience

3 Major Bodies of Work Exist In the Discipline of Advanced Cyber-Resilience

1. Cyber Resiliency Engineering Framework Published September 2011 by the MITRE Corporation

2. Cyber DRaaS by Risk Masters Inc. Published 2014

3. The FFEIC Cybersecurity Assessment Tool Published June 2015

We’ll Take A Quick Tour of Advanced Cyber-Resilience To Get A Glimpse of Future State Requirements
Cyber Resilience Engineering Framework

Cyber resiliency goals are:

• Anticipate: maintain a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks,

• Withstand: continue essential mission/business functions despite successful execution of an attack by an adversary,

• Recover: restore mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary, and

• Evolve: to change missions/business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted adversary attacks.
Conceptual Foundation

Figure 4. Cyber Resiliency Goals and Objectives
### How To Achieve

**Table 3. Mapping Cyber Resiliency Practices to Objectives**

<table>
<thead>
<tr>
<th>Practice</th>
<th>Understand</th>
<th>Prepare</th>
<th>Prevent</th>
<th>Constrain</th>
<th>Continue</th>
<th>Reconstitute</th>
<th>Transform</th>
<th>Re-Architect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Response</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytic Monitoring</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coordinated Defense</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Deception</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diversity</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic Positioning</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Dynamic Representation</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Non-Persistence</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Privilege Restriction</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Realignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redundancy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Segmentation</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Substantiated Integrity</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Unpredictability</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
# Threat Modeling

Table 6. Adversary Characteristics at Cyber Prep Levels 3 Through 5

<table>
<thead>
<tr>
<th>Threat Level</th>
<th>Capability</th>
<th>Intent</th>
<th>Targeting</th>
</tr>
</thead>
<tbody>
<tr>
<td>5: Advanced</td>
<td>The adversary is very sophisticated and well resourced and can generate its own opportunities to support multiple successful, continuous, and coordinated attacks.</td>
<td>The adversary seeks with great determination to undermine or impede severely, or destroy, a mission, program, or enterprise, by exploiting a presence in the organization’s systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede their ability to complete their goal.</td>
<td>The adversary targets a specific organization, enterprise, program, or mission, focusing on specific high value or mission-critical information, resources, supply flows, or functions and specific employees supporting those functions, as well as on supporting infrastructure providers and suppliers and on partnering organizations.</td>
</tr>
<tr>
<td>4: Significant</td>
<td>The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.</td>
<td>The adversary seeks with determination to undermine or impede critical aspects of a mission, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization’s systems or infrastructure. The adversary is very concerned about minimizing detection of their attacks or disclosure of tradecraft, particularly while preparing for future attacks.</td>
<td>The adversary targets a specific organization, enterprise, program, or mission, focusing on specific high value or mission-critical information, resources, supply flows, or functions and specific employees supporting those functions.</td>
</tr>
<tr>
<td>3: Moderate</td>
<td>The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.</td>
<td>The adversary persistently seeks to obtain or modify specific, critical information and/or to usurp or disrupt the organization’s cyber resources by establishing a foothold in the organization’s systems or infrastructure, but is concerned about minimizing detection of their attacks or disclosure of tradecraft, particularly when carrying out attacks (e.g., exfiltration) over long time periods. The adversary is willing to knowingly impede aspects of the organization’s mission to achieve these ends.</td>
<td>The adversary targets specific high value organizations, programs, or information.</td>
</tr>
</tbody>
</table>
Cyber DRaaS Goals:

- Practical “Let’s Do This Today Approach”
- Leverages Cloud base backup services with Next Generation Firewall technology and end to end encryption.
- Flexible Approach – Applies to an existing Fortress/Moat or as a Zero-Trust Network.
- Fast Deployment and Implementation
Cyber DRaaS™ Cloud Architecture

Cyber DRaaS integrates the Next Generation Firewall with subscription services and administrative tools to protect trusted backups from cyber attack.

- Connectivity to the Production Network
- Next Generation Firewall (NGF)
- Network Management and Monitoring
- Malware Sandbox
- Private Cloud-based Backup and Recovery

Cyber DRaaS™—Critical Technology Components

- **Cloud Backup and Recovery**
  - Manage data backup and restore processes for trusted images
  - Routine integrity checking of trusted image backups
  - Optimal performance with data compression and duplication

- **Next Generation Firewall**
  - Network policy enforcement at application/user level, not port
  - Content scanning for known and unknown malware signatures
  - Predictable high-performance single-pass software engine

- **Network Management**
  - Policy-driven security management across deployed firewalls
  - Visibility into network traffic, deployed applications and policies
  - Graphical tools enabling immediate investigation of malware

- **Malware Sandbox**
  - Malicious content/malware redirected to virtualized sandbox
  - Monitoring of known signatures and malicious network behaviors
  - New malware discoveries generate new database signatures
Cyber DRaaS – Fortress/Moat
Cyber DRaaS – Zero Trust
FFEIC CAT’s Goals

• Let’s make sure we are all doing it right.

• Let’s find out who does it better than Baseline (Minimum)

• What Attributes Define Better Than Baseline.

• Consist of 500 Questions To Determine “Maturity”

• May be predictive of cyber resilience compliance requirements in light of the EU Directive and FSOC.
FFIEC Cybersecurity Assessment Tool (CAT)
FFEIC CAT Synthesizes MITRE’s Cyber Resilience Engineering Framework within the “Evolving” and higher Maturity Levels.

If you expect to be beyond Baseline Maturity, much of the pioneering work of Cyber DraaS is a stated requirement.

Concepts of Dynamic, Self-Healing, System Design are also addressed.

While responding to incidents is an option, the prevailing direction on cyber resilience is to withstand and recover as the desirable end state.
Conclusions

EU Cybersecurity Directive and the FSOC Annual Review presents a bellwether for cyber resilience requirements from a compliance perspective.

Whether organizations are regulated or not, a legal obligation will be created to insure that organizations maintain minimum cyber resilience capabilities or face potential criminal and punitive damages.

To achieve these minimum capabilities, organization must show sophistication in understanding cyber resilience requirements under well known frameworks.

Early warning of impending risks to organizational resiliency is an absolute requirement to respond to and mitigate the impact of cyber attack.

Organizations should seek to review with Subject Matter Experts and Systems Engineering the capabilities to understand and correlate anomalous behavior as a precursor to a cyber attack, which impacts availability.
Andy Kim

626.660.4702
andrew.kim@fisglobal.com