FDIC Advisory Committee on Community Banking

June 1, 2023

Supervision and Policy Updates

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

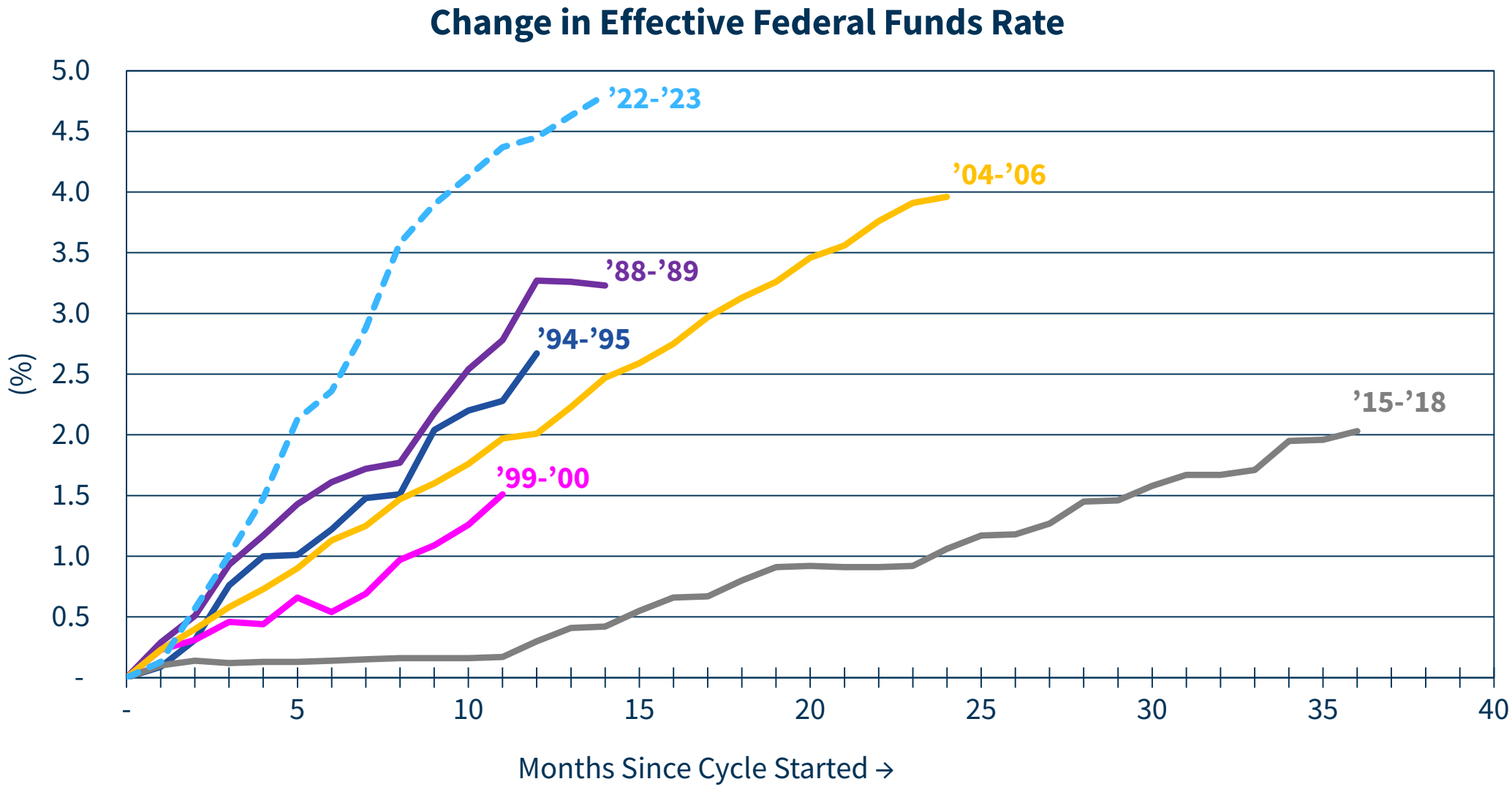
FDIC Advisory Committee on Community Banking

June 1, 2023

Asset Liability Management

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Asset Liability Management During a Challenging Interest Rate Environment

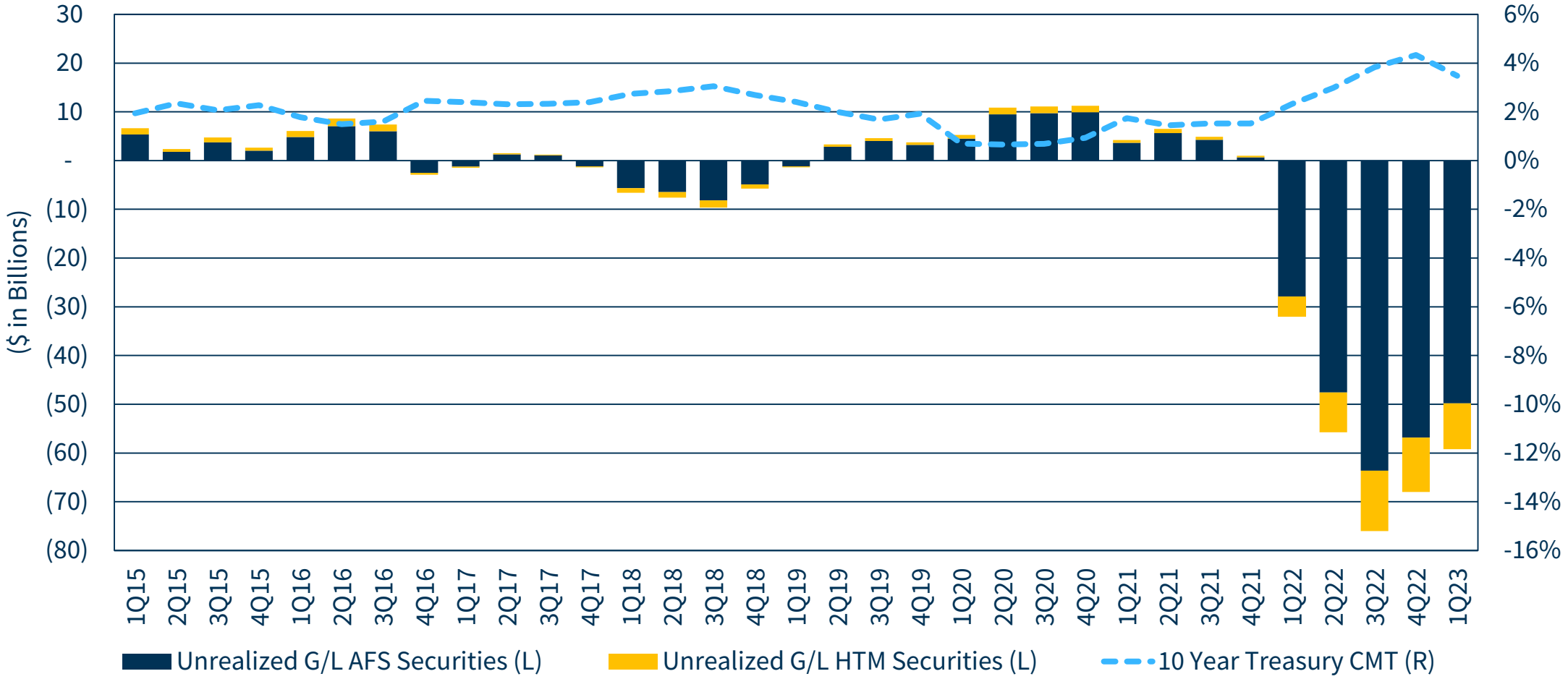


Source: Board of Governors of the Federal Reserve System (H.15 Selected Interest Rates, downloaded using the Federal Reserve Bank of Saint Louis's FRED Tools).
Change is calculated as the monthly average level.

FDIC

Asset Liability Management During a Challenging Interest Rate Environment

Higher Rates Caused Long-Term Bond Values to Decline, Potentially Impacting Capital and Liquidity



Source: Call Report data for community banks as defined in the FDIC's 2020 Community Banking Study and https://fred.stlouisfed.org/series/DGS10#0

FDIC

Interagency Policy Statement on Funding and Liquidity Risk Management (2010)

- Effective corporate governance by Board and management
- A diverse mix of existing and potential future funding sources
- Appropriate strategies, policies, procedures, and limits
- Adequate levels of highly liquid marketable securities
- Comprehensive liquidity risk measurement and monitoring systems
- Comprehensive contingency funding plans (CFP)
- Active management of intraday collateral
- Internal controls and internal audit processes

FDIC

Bank Term Funding Program (BTFP) Facility

New temporary Federal Reserve borrowing facility

Advances can be requested until at least March 11, 2024

Institutions eligible for primary credit under the Discount Window are eligible to borrow under BTFP

Institutions are encouraged to obtain and confirm access to the Discount Window and the BTFP

Eligible collateral: collateral that was owned as of March 12, 2023 and is eligible for purchase by the Federal Reserve in open market conditions (12 CFR 201.108(b))

Testing the Discount Window, BTFP, and other back-up funding is prudent and supports operational readiness under the institution's contingency funding plan

Collateral value based on securities' par value

FDIC

FDIC Advisory Committee on Community Banking

June 1, 2023

Asset Liability Management

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

FDIC Advisory Committee on Community Banking

June 1, 2023

Cybersecurity

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Ransomware Horizontal Review

Background

- Searched FDIC and other agency databases for ransomware attacks over a two-year period (June 2019-May 2021)
- Searched for only attacks at FDIC-supervised institutions

  Identified 36 ransomware attacks of interest
- The FDIC reviewed forensic reports from, and conducted interviews with, attacked financial institutions

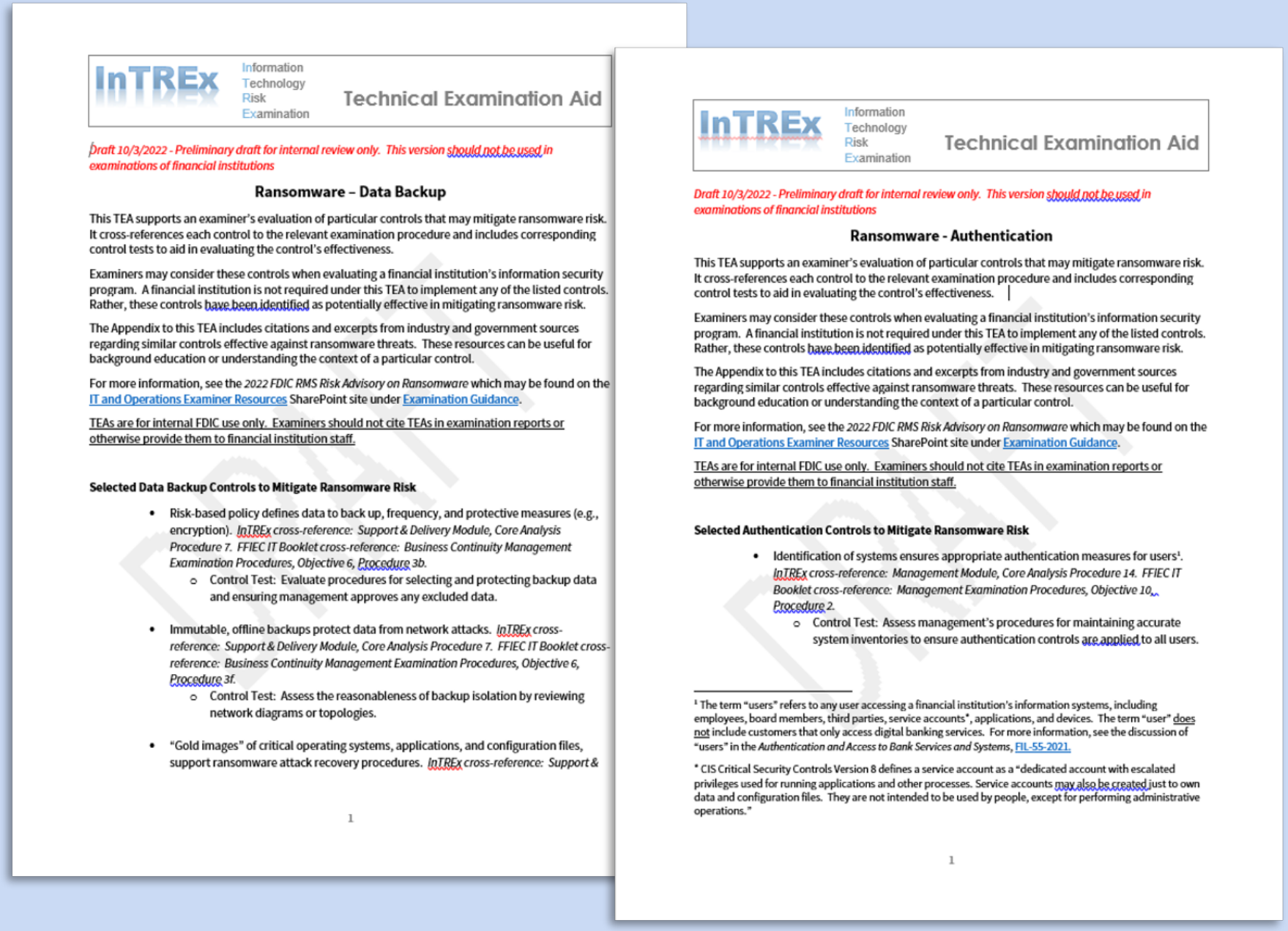
FDIC

What controls make a difference in defense?

Internet (HTTP) Address Filtering	Logging	Operating System Hardening
Multifactor Authentication	Preventing Unauthorized Executables and Macros (including PowerShell)	Least Privilege Implementation
Backup Isolation and Viability	Network Segmentation	Intrusion Detection System / Intrusion Prevention System Implementation

FDIC

Resulting Supervisory Adjustments



InTREx Information Technology Risk Examination — Technical Examination Aid

Draft 10/3/2022 - Preliminary draft for internal review only. This version should not be used in examinations of financial institutions

Ransomware – Data Backup

This TEA supports an examiner's evaluation of particular controls that may mitigate ransomware risk. It cross-references each control to the relevant examination procedure and includes corresponding control tests to aid in evaluating the control's effectiveness.

Examiners may consider these controls when evaluating a financial institution's information security program. A financial institution is not required under this TEA to implement any of the listed controls. Rather, these controls have been identified as potentially effective in mitigating ransomware risk.

The Appendix to this TEA includes citations and excerpts from industry and government sources regarding similar controls effective against ransomware threats. These resources can be useful for background education or understanding the context of a particular control.

For more information, see the *2022 FDIC RMS Risk Advisory on Ransomware* which may be found on the IT and Operations Examiner Resources SharePoint site under Examination Guidance.

TEAs are for internal FDIC use only. Examiners should not cite TEAs in examination reports or otherwise provide them to financial institution staff.

Selected Data Backup Controls to Mitigate Ransomware Risk

- Risk-based policy defines data to back up, frequency, and protective measures (e.g., encryption). *InTREx cross-reference: Support & Delivery Module, Core Analysis Procedure 7. FFIEC IT Booklet cross-reference: Business Continuity Management Examination Procedures, Objective 6, Procedure 3b.*
  - Control Test: Evaluate procedures for selecting and protecting backup data and ensuring management approves any excluded data.
- Immutable, offline backups protect data from network attacks. *InTREx cross-reference: Support & Delivery Module, Core Analysis Procedure 7. FFIEC IT Booklet cross-reference: Business Continuity Management Examination Procedures, Objective 6, Procedure 3f.*
  - Control Test: Assess the reasonableness of backup isolation by reviewing network diagrams or topologies.
- "Gold images" of critical operating systems, applications, and configuration files, support ransomware attack recovery procedures. *InTREx cross-reference: Support &*

1

InTREx Information Technology Risk Examination — Technical Examination Aid

Draft 10/3/2022 - Preliminary draft for internal review only. This version should not be used in examinations of financial institutions

Ransomware - Authentication

This TEA supports an examiner's evaluation of particular controls that may mitigate ransomware risk. It cross-references each control to the relevant examination procedure and includes corresponding control tests to aid in evaluating the control's effectiveness.

Examiners may consider these controls when evaluating a financial institution's information security program. A financial institution is not required under this TEA to implement any of the listed controls. Rather, these controls have been identified as potentially effective in mitigating ransomware risk.

The Appendix to this TEA includes citations and excerpts from industry and government sources regarding similar controls effective against ransomware threats. These resources can be useful for background education or understanding the context of a particular control.

For more information, see the *2022 FDIC RMS Risk Advisory on Ransomware* which may be found on the IT and Operations Examiner Resources SharePoint site under Examination Guidance.

TEAs are for internal FDIC use only. Examiners should not cite TEAs in examination reports or otherwise provide them to financial institution staff.

Selected Authentication Controls to Mitigate Ransomware Risk

- Identification of systems ensures appropriate authentication measures for users[1]. *InTREx cross-reference: Management Module, Core Analysis Procedure 14. FFIEC IT Booklet cross-reference: Management Examination Procedures, Objective 10, Procedure 2.*
  - Control Test: Assess management's procedures for maintaining accurate system inventories to ensure authentication controls are applied to all users.

[1] The term "users" refers to any user accessing a financial institution's information systems, including employees, board members, third parties, service accounts*, applications, and devices. The term "user" does not include customers that only access digital banking services. For more information, see the discussion of "users" in the *Authentication and Access to Bank Services and Systems*, FIL-55-2021.

* CIS Critical Security Controls Version 8 defines a service account as a "dedicated account with escalated privileges used for running applications and other processes. Service accounts may also be created just to own data and configuration files. They are not intended to be used by people, except for performing administrative operations."

1

FDIC

Updated FFIEC Cybersecurity Resource Guide for Financial Institutions

- The Federal Financial Institutions Examination Council (FFIEC) issued a Cybersecurity Resource Guide for Financial Institutions in 2018.
- The Guide provides resources to assist financial institutions in meeting their security control objectives and in preparing to respond to cyber incidents.
- The Guide includes resources to help:
  - Assess cybersecurity readiness
  - Perform exercises to test cybersecurity readiness
  - Monitor threats and vulnerabilities
  - Report incidents

FDIC

Updated FFIEC Cybersecurity Resource Guide for Financial Institutions

- On October 3, 2022, the FFIEC published an update to the Cybersecurity Resource Guide that includes ransomware-specific resources:
  - **Cybersecurity and Infrastructure Security Agency (CISA) Cyber Security Evaluation Tool: Ransomware Readiness Assessment**
    https://www.cisa.gov/downloading-and-installing-cset
  - **CISA Ransomware Guide**
    https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf
  - **CISA Stop Ransomware Resource Site**
    https://www.cisa.gov/stopransomware
  - **Conference of State Bank Supervisors Ransomware Self-Assessment Tool**
    https://www.csbs.org/ransomware-self-assessment-tool

FDIC

CISA Cyber Hygiene Scanning

- One listed resource worth highlighting is the cyber hygiene vulnerability scanning service available from the Cybersecurity and Infrastructure Security Agency (CISA) and listed under “CISA Cyber Resource Hub” in the updated Guide.

- Vulnerability scanning evaluates an entity’s external network presence by scanning public network interfaces for vulnerabilities.

- The CISA service is free and provides weekly vulnerability reports and ad-hoc alerts.

- Requests should be sent to vulnerability@cisa.dhs.gov, with the subject line “Requesting Cyber Hygiene Services.”

FDIC

Updated FFIEC Cybersecurity Resource Guide for Financial Institutions

- On October 27, 2022, the FDIC shared the FFIEC Resource Guide with financial institutions through Financial Institution Letter 50-2022.

- Additional information is available at:

  - **FFIEC Cybersecurity Awareness webpage**: https://www.ffiec.gov/cybersecurity.htm

  - **FDIC Cybersecurity Resources webpage**: https://www.fdic.gov/regulations/resources/cybersecurity/index.html

FDIC

FDIC Advisory Committee on Community Banking

June 1, 2023

Cybersecurity

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

FDIC Advisory Committee on Community Banking

June 1, 2023

Supervisory Guidance on Charging Overdraft Fees for Authorize Positive, Settle Negative Transactions

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Authorize Positive/Settle Negative

FIL-19-2023: Supervised institutions must be aware of the consumer compliance risks associated with charging an overdraft fee on a transaction that was authorized against a positive balance but settled against a negative balance, a practice commonly referred to as “Authorize Positive, Settle Negative” (APSN).

- APSN Background
- Potential Risks
- Risk Mitigation Practices
- Resources

FDIC

APSN Background

Overdraft fees may be charged against consumer accounts when the account balance was sufficient at the time the transaction was initiated, but due to transaction clearing & settlement processes, was later posted to the customer's account when their balance was negative.

These situations may occur when using an "available balance" or "ledger balance" in assessing overdraft fees. Risk exists in both the available & ledger balance scenarios but may be more pronounced in the available balance scenario.

The FDIC has determined that the practice of assessing fees on transactions that authorized positive and settle negative **are unfair**.

FDIC

Potential Risks

Federal Trade Commission Act

- Violations of Section 5 prohibiting unfair or deceptive acts or practices (UDAP).
- An unfair act or practice is one that causes or is likely to cause substantial injury; cannot be reasonably avoided, and is not outweighed by countervailing benefits to consumer. Public policy may also be considered.

Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010

- Violations of Section 1036(a)(1)(B) prohibiting unfair, deceptive or abusive acts or practices in connection with a consumer financial product/service.

Basis of Unfairness

- Unanticipated & unavoidable overdraft fees may cause substantial injury to consumers.
- The injury is not reasonably avoidable because the consumer does not have the ability to control payment systems & overdraft processing systems.
- The methods of charging overdraft fees are not outweighed by countervailing benefits to consumers or competition.

FDIC

Risk Mitigation Practices

Review Policies/Procedures

- Review overdraft fee practices pertaining to APSN transactions to ensure customers are not charged overdraft fees they cannot anticipate or avoid.

Review Disclosures/Account Agreements

- Review disclosures/account agreements ensuring that practices for charging any fees on deposit accounts are clearly, accurately & consistently communicated.
- **However, disclosures alone generally do not fully address the risks in this area.**

Third-Party Arrangements

- Review third-party arrangements & ensure that third-party systems are compliant with all applicable laws/regulations. This review should cover third-party system settings for charging overdraft fees, methods for identifying & tracking transactions authorized on a positive balance but settled on a negative balance, & maintaining data on such transactions.

FDIC

Resources

FDIC FIL-44-2008	"Guidance for Managing Third-Party Risk"
FDIC FIL-81-2010	"Overdraft Payment Supervisory Guidance"
CFPB Circular 2022-06	"Unanticipated Overdraft Fee Assessment Practices"
OCC Bulletin 2023-12	"Overdraft Protection Programs: Risk Management Practices"
FDIC FIL-19-2023	"Supervisory Guidance on Charging Overdraft Fees for Authorize Positive, Settle Negative Transactions"

FDIC

FDIC Advisory Committee on Community Banking

June 1, 2023

Supervisory Guidance on Charging Overdraft Fees for Authorize Positive, Settle Negative Transactions

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION