Replaces October 2018 Resource Guide

Cybersecurity Resource Guide for Financial Institutions

September 2022

(Revised November 2022)

Legend	Assessment	Exercise	Information Sharing	Ransomware	Response/Reporting

3501 Fairfax Drive • E-2035-C • Arlington, VA 22226-3550 • (703) 516-5588 • www.ffiec.gov

Overview

The Federal Financial Institutions Examination Council (FFIEC), on behalf of its members, is issuing an update to the October 2018 Cybersecurity Resource Guide for Financial Institutions. The programs and tools in the guide are designed for, or otherwise available to, financial institutions. The purpose of this guide is to help financial institutions meet their security control objectives and prepare to respond to cyber incidents.

In recent years, ransomware incidents have become increasingly prevalent. These incidents continue to evolve in severity and complexity impacting the financial sector and other critical infrastructure organizations. To address this evolving threat, the resource guide now includes ransomware-specific resources to address this ongoing threat.

Legend	Assessment A	Exercise E	Information Sharing I	Ransomware	Response/Reporting R

Federal Financial Institutions Examination Council

3501 Fairfax Drive • E-2035-C • Arlington, VA 22226-3550 • (703) 516-5588 • www.ffiec.gov

Cybersecurity Resource Guide for Financial Institutions

This guide outlines resources to assist financial institutions in strengthening their resilience to cyber threats. Use of these resources is voluntary. FFIEC members do not endorse the listed organizations or tools identified.

Resources	Type	Cost
Assessments		
Center for Internet Security (CIS) https://www.cisecurity.org/	A	Free Paid
Cybersecurity and Infrastructure Security Agency (CISA) Cyber Resilience Review (CRR) https://www.cisa.gov/uscert/resources/assessments	A	Free
CISA Cyber Resource Hub https://www.cisa.gov/cyber-resource-hub	A	Free
Cyber Risk Institute's (CRI) Profile https://cyberriskinstitute.org/the-profile/	A	Free Paid
Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) https://www.ffiec.gov/cyberassessmenttool.htm	A	Free
Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Toolkit www.cisa.gov/ict-supply-chain-toolkit	A	Free
National Credit Union Administration (NCUA) Automated Cybersecurity Evaluation Toolbox (ACET) https://www.ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources/acet-and-other-assessment-tools	A	Free
National Institute of Standards and Technology (NIST) Cybersecurity Framework https://www.nist.gov/cyberframework	A	Free
Exercises		
CISA Tabletop Exercise Package https://www.cisa.gov/publication/cisa-tabletop-exercise-package	E	Free
Federal Insurance Deposit Corporation (FDIC) Cyber Challenge: A Community Bank Cyber Exercise https://www.fdic.gov/regulations/resources/director/technical/cyber/cyber.html	E	Free
Financial Sector Cyber Exercise Template https://www.fbiic.gov/public/2017/Financial_Sector_Cyber_Exercise_Template.pdf	E	Free

Legend	Assessment A	Exercise E	Information Sharing I	Ransomware	Response/Reporting R

Financial Services - Information Sharing and Analysis Center (FS-ISAC) Exercises https://www.fsisac.com/resilience/exercises *Note: In November 2022, the icon for FS-ISAC Exercises was changed from free to paid.*	E	Paid
Information Sharing		
CISA Services and Tools Repository https://www.cisa.gov/publication/cisa-services-catalog	I	Free
Financial Services Information Sharing and Analysis Center (FS-ISAC) https://www.fsisac.com	I	Free Paid
fTLD Registry Services (fTLD) https://www.ftld.com/	I	Free Paid
Global Resilience Federation Business Resilience Council (BRC) https://grf.org/brc	I	Free Paid
Homeland Security Information Network (HSIN) https://www.dhs.gov/homeland-security-information-network-hsin	I	Free
InfraGard https://www.infragard.org	I	Free
National Credit Union Information Sharing and Analysis Organization https://www.nacuso.org/wp-content/uploads/2016/12/National-Credit-Union-ISAO_Execuive-Level-Briefing.pdf	I	Free Paid
U.S. Computer Emergency Readiness Team https://www.cisa.gov/uscert/	I	Free
U.S. Secret Service https://www.secretservice.gov/investigation/cyber	I	Free
Response/Reporting		
CISA Report Incidents, Phishing, Malware, or Vulnerabilities https://us-cert.cisa.gov/report	R	Free
Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) https://www.ic3.gov	R	Free
Reporting to Primary Regulator https://www.govinfo.gov/content/pkg/FR-2005-03-29/pdf/05-5980.pdf https://www.govinfo.gov/content/pkg/FR-2021-11-23/pdf/2021-25510.pdf	R	Free
Sheltered Harbor https://shelteredharbor.org/about	R	Paid
Ransomware		
CISA Cyber Security Evaluation Tool (CSET): Ransomware Readiness Assessment (RRA) https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr		Free
CISA Ransomware Guide https://www.cisa.gov/publication/ransomware-guide		Free
CISA Stop Ransomware Resource Site https://www.cisa.gov/stopransomware		Free
Conference of State Bank Supervisors (CSBS) Ransomware Self-Assessment Tool https://www.csbs.org/ransomware-self-assessment-tool		Free

Legend	Assessment	Exercise	Information Sharing	Ransomware	Response/Reporting
	A	E	I		R

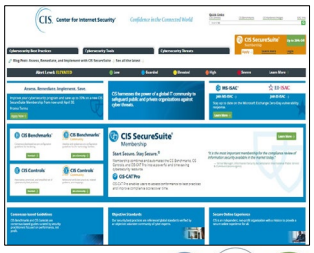
Assessments

Center for Internet Security, Inc. (CIS®)

CIS is a nonprofit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.

- CIS Benchmarks™: 100+ configuration guidelines for various technology platforms to safeguard systems against today's evolving cyber threats.
- CIS Configuration Assessment Tool Lite (CIS-CAT): A free detailed assessment of systems (Windows, Google Chrome, Ubuntu, Mac OS) in conformance with CIS Benchmarks.

https://www.cisecurity.org



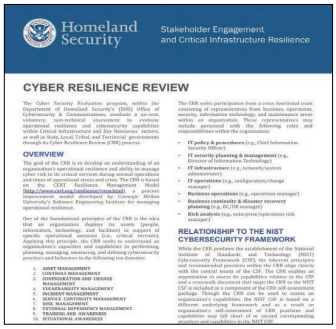
A Free Paid

CISA Cyber Resilience Review (CRR)

The CRR is a free, voluntary, and nontechnical tool for assessing an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by the U.S. Department of Homeland Security (DHS) cybersecurity professionals. The CRR assesses enterprise programs and practices across 10 domains including risk management, incident management, and service continuity.

The assessment measures existing organizational resilience and provides a gap analysis for improvement based on recognized best practices. For more information, email cyberadvisor@cisa.dhs.gov

https://www.cisa.gov/uscert/resources/assessments



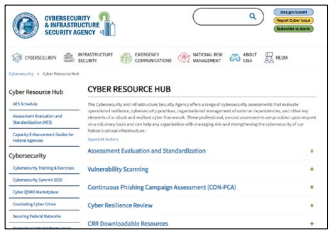
A Free

CISA Cyber Resource Hub

CISA supports U.S. government and industry critical infrastructure by providing proactive testing and assessment services. CISA Resource Hub services are available at no cost to financial institutions. For more information, email vulnerability@cisa.dhs.gov. Services include:

- Cyber hygiene vulnerability scanning: To secure internet accessible systems by continuously scanning for known vulnerabilities and configuration errors.
- Phishing Campaign Assessment: Measures your team's propensity to click on email phishing lures.
- Risk and Vulnerability Assessment: Allows organizations to select the network security area to have assessed by CISA.
- Evaluates systems, networks, and security services to determine if they are designed, built, and operated in reliably and resiliently.

https://www.cisa.gov/cyber-resource-hub



A Free

Cyber Risk Institute's (CRI) Profile

The Cyber Risk Institute (CRI) is a not-for-profit coalition of financial institutions and trade associations. CRI's mission is simple: Sharpen cybersecurity to protect the global economy. CRI does this by creating (and updating) a common framework for cybersecurity and resilience assessment. The Profile tool consists of a list of assessment questions based on the intersection of global regulations and cyber standards, such as International Organization for Standardization (ISO) and NIST.

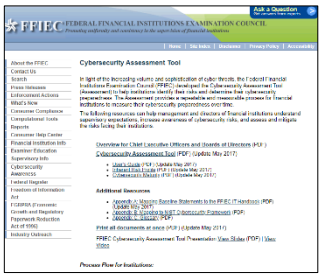
https://cyberriskinstitute.org/the-profile/

A Paid

FFIEC Cybersecurity Assessment Tool (CAT)

In light of the increasing volume and sophistication of cyber threats, the FFIEC developed the CAT to help institutions identify their risks and determine their cybersecurity preparedness. The CAT provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness.

https://www.ffiec.gov/cyberassessmenttool.htm



A Free

Information and Communications Technology (ICT) Supply Chain Risk (SCRM) Management Toolkit

This toolkit—which includes strategic messaging, social media, videos, and resources—emphasizes the role that everyone has in securing information and communications technology (ICT) supply chains. All the products detailed below incorporate industry standards to make them highly effective tools to help increase supply chain resilience.

- **Strategic messaging to enhance supply chain security**: Internal and public communications to inform personnel, vendors, suppliers, partners, and others about their role in supply chain risk management.
- **Social media tools to spread awareness**: Tools that can be leveraged on your organization's social channels to drive awareness and action on the importance of supply chain security.
- **Resources to strengthen supply chain resilience**: CISA's ICT SCRM Task Force developed voluntary products - Industry best practices and standards such as those from NIST and the Open Trusted Technology Provider Standard (O-TTPS) to make these products the best possible tools.

www.cisa.gov/ict-supply-chain-toolkit

A Free

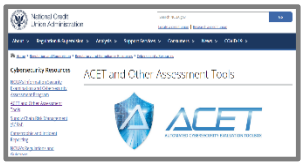
Legend	Assessment A	Exercise E	Information Sharing I	Ransomware	Response/Reporting R

National Credit Union Administration (NCUA) Automated Cybersecurity Evaluation Toolbox (ACET)

The NCUA's ACET application provides credit unions the capability to conduct a maturity assessment aligned with FFIEC CAT. The ACET self-assessment is completely voluntary and does not introduce any new requirements or expectations on credit unions. The tool allows credit unions to identify and determine their levels of cybersecurity preparedness. Using the ACET to conduct assessments on a regular basis may help institutions to:

- Identify areas of risk proactively before there is a problem
- Determine the depth and breadth of cyber risk that the institution is exposed to
- Discover the institution's preparedness to deal with cyber threats
- Make decisions about security processes and programs based on the true nature of existing risk
- Use a measurable and repeatable process to assess risk preparedness over time
- Understand, address, and mitigate cybersecurity risks

https://www.ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources/acet-and-other-assessment-tools



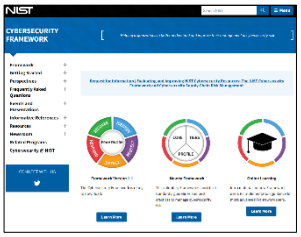
A Free

NIST Cybersecurity Framework

A product of the Cybersecurity Enhancement Act of 2014, the framework was developed to improve cybersecurity risk management in critical infrastructure and provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today.

The framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles.

https://www.nist.gov/cyberframework



A Free

Ransomware Risk Management: A Cybersecurity Framework Profile

The NIST Ransomware Profile identifies the Cybersecurity Framework Version 1.1 security objectives that support identifying, protecting against, detecting, responding to, and recovering from ransomware events. The profile can be a guide to managing the risk of ransomware events. That includes helping to gauge an organization's level of readiness to counter ransomware threats and to deal with the potential

consequences of events. The Ransomware Profile is intended for any organization with cyber resources that could be subject to ransomware attacks, regardless of sector or size.

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf

Exercises

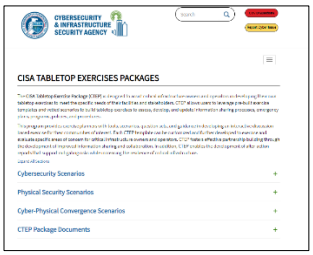
E

CISA Tabletop Exercise Package (CTEP)

The CTEP assists critical infrastructure owners and operators in developing their own tabletop exercises to meet the specific needs of their facilities and stakeholders. The CTEP allows users to leverage pre-built exercise templates and vetted scenarios to build tabletop exercises to assess, develop, and update information sharing processes, emergency plans, programs, policies, and procedures. The packages are organized under the following areas:

- Cybersecurity Scenarios
- Physical Security Scenarios
- Cyber-Physical Convergence Scenarios
- CTEP Package Documents

https://www.cisa.gov/publication/cisa-tabletop-exercise-package

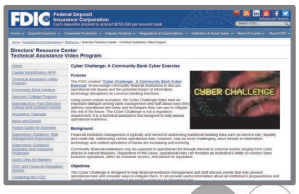


E Free

Federal Deposit Insurance Corporation (FDIC) Cyber Challenge: A Community Bank Cyber Exercise

The FDIC Cyber Challenge is designed to help financial institution management and staff discuss events that may present operational risks and consider ways to mitigate them. The Cyber Challenge consists of nine short video vignettes and related challenge questions. Each video vignette depicts a unique scenario.

https://www.fdic.gov/regulations/resources/director/technical/cyber/cyber.html



E Free

Financial Sector Cyber Exercise Template

The Financial Sector Cyber Exercise Template is designed for smaller financial sector institutions to test their preparedness. The template helps institutions run their own internal cyber exercises and facilitates discussion on how best to engage with the national architecture for coordinating responses to significant cybersecurity incidents among government and industry. Institutions can modify the template to suit their specific needs.

https://www.fbiic.gov/public/2017/Financial_Sector_Cyber_Exercise_Template.pdf

E Free

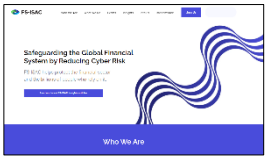
Financial Services - Information Sharing and Analysis Center (FS-ISAC) Exercises	
Cyber Attack Against Payment Systems (CAPS): The CAPS exercise is a two-day tabletop exercise specifically designed for an incident response team to practice overcoming a robust, simulated attack on payment systems and processes. The exercise is a paid service and open to FS-ISAC members. **Cyber-Range Exercises:** A one-day, hands-on-keyboard exercise in which participants observe and respond to different attacks such as ransomware or business email compromise. Teams share and review results, identify methods for improving defenses, then rerun the simulated attack to see if the suggested mitigation techniques improve results. The exercise is a paid service and open to FS-ISAC members. https://www.fsisac.com/resilience/exercises *Note: In November 2022, the information and the accompanying icon for CAPS was changed from free to paid.*	FS-ISAC E Paid

Information Sharing

I

CISA Services and Tools Repository	

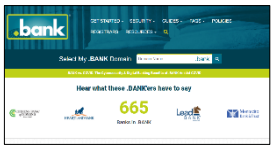
The CISA Services Catalog is an all-in-one resource that provides users with access to information on services across all of CISA's mission areas and that are available to
 	
• Federal, state, local, tribal and territorial government
• Non-government and nonprofit organizations
  ○ Academia
  ○ Private Industry
• General public stakeholders
 	
CISA compiled a list of free cybersecurity tools and services to help organizations advance their security capabilities. The repository includes CISA's cybersecurity services, widely used open-source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community.
 	
https://www.cisa.gov/free-cybersecurity-services-and-tools
	
	I Free

Financial Services Information Sharing and Analysis Center (FS-ISAC)	
The FS-ISAC is a global cyber intelligence-sharing community focused on financial services. Serving financial institutions and, in turn, their customers, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network to anticipate, mitigate, and respond to cyber threats. https://www.fsisac.com/	 I Free Paid

fTLD Registry Services (fTLD)

fTLD (TLD for 'top-level domain') Registry Services is a coalition of banks, insurance companies and financial services trade associations from around the world. fTLD's mission is to operate a trusted, verified, more secure and easily identifiable online location for these financial companies and their customers. fTLD was granted the right to operate .BANK on September 25, 2014, and .INSURANCE on February 19, 2015, and launched the TLDs in 2015 and 2016 respectively. All applicants to use these extensions undergo a thorough verification process before being awarded a domain and must comply with strict registry policies ensuring ongoing compliance with the fTLD security requirements.

https://www.ftld.com/about/



I Paid

Global Resilience Federation Business Resilience Council (BRC)

The BRC is a member-driven, analyst-supported, multi-sector community created to foster sharing and cooperation regarding significant incidents, threats, and vulnerabilities that impact business operations of critical infrastructure and supporting sectors. The BRC provides members with business continuity and resilience information and offers an operational resilience framework to assist in developing and refining an industry-driven framework of rules supported by architecture and controls.

https://grf.org/brc

I Free Paid

Homeland Security Information Network (HSIN)

HSIN is DHS' official system for trusted sharing of Sensitive-But Unclassified information between federal, state, local, territorial, tribal, international, and private sector partners. Mission operators use HSIN to access Homeland Security data, send requests securely between agencies, manage operations, coordinate planned event safety and security, respond to incidents, and share the information they need to fulfill their missions and help keep their communities safe.

For more information about HSIN, please contact HSIN@hq.dhs.gov.

https://www.dhs.gov/homeland-security-information-network-hsin

I Free

InfraGard

InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector community. InfraGard promotes public-private collaboration and timely exchanges of information. In addition, InfraGard promotes learning opportunities relevant to the protection of critical infrastructure. For more information, email infragardteam@fbi.gov.

https://www.infragard.org

I Free

National Credit Union Information Sharing and Analysis Organization (NCU-ISAO)

Presidential Executive Order 13691 directed DHS to encourage the development of ISAOs to address information sharing beyond the traditional infrastructure sectors. NCU-ISAO's mission is to enable and sustain credit union critical infrastructure cyber resilience and preserve the public trust by advancing trusted security coordination and collaboration to identify, protect, detect, respond, and recover from threats and vulnerabilities. The NCU-ISAO comprises an experienced group of industry leaders in cybersecurity, information sharing, and member associations. NCU-ISAO is not affiliated with the National Credit Union Administration.

https://www.nacuso.org/wp-content/uploads/2016/12/National-Credit-Union-ISAO_Execuive-Level-Briefing.pdf

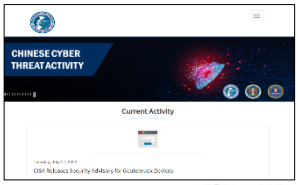
I Free Paid

* Not a federal agency

U.S. Computer Emergency Readiness Team (US-CERT)

The U.S. Computer Emergency Readiness Team is a branch of the Office of Cybersecurity and Communications' National Cybersecurity and Communications Integration Center within DHS's CISA and was established to protect the nation's internet infrastructure.

https://www.cisa.gov/uscert/



I Free

U.S. Secret Service

Financial and Cyber Crime Investigations: The Secret Service established the Financial and Cyber Crime Investigations Division with a mission to protect the financial infrastructure of the United States by investigating complex, often cyber-enabled financial crimes.

Cyber Fraud Task Forces (CFTFs): The CFTFs are the focal point of the Secret Services' cyber investigative efforts, are a partnership between the Secret Service, other law enforcement agencies, prosecutors, private industry, and academia. CFTFs are strategically located throughout the United States to combat cybercrime through prevention, detection, mitigation, and investigation.

https://www.secretservice.gov/investigation/cyber

I Free

Legend	Assessment A	Exercise E	Information Sharing I	Ransomware	Response/Reporting R

Response/Reporting

CISA Report Incidents, Phishing, Malware, or Vulnerabilities

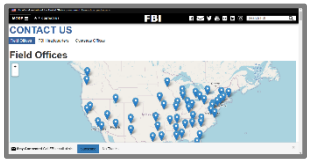
CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities.

https://us-cert.cisa.gov/report

FBI Internet Crime Complaint Center (IC3)

The Internet Crime Complaint Center provides the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.

Field Offices/Regions: https://www.fbi.gov/contact-us/field-offices



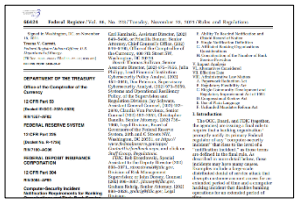
R Free

Reporting to Primary Regulator

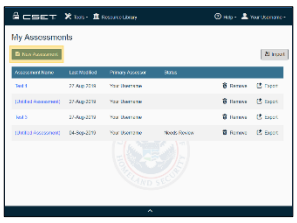
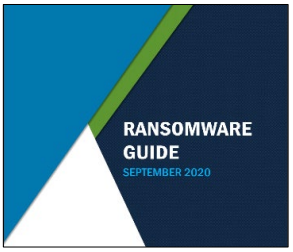
If a cyber-incident results in unauthorized access to or use of sensitive customer information, the institution should notify its primary federal regulator, and state regulator(s) if it is state chartered, as soon as possible.

Institutions supervised by the Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and the Federal Reserve Bank (the agencies) are required to notify their primary federal regulator of "notification incidents." The agencies issued a final rule requiring banking organizations to notify their primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident" as soon as possible and no later than 36 hours after the banking organization determines a notification incident has occurred. Additionally, it requires a bank service provider to notify affected banking organization customers as soon as possible when it determines it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, "covered services" provided to such banking organization customers for four or more hours. Covered banking organizations under the final rule include all depository institutions, holding companies, and certain other financial entities supervised by one or more of the agencies.

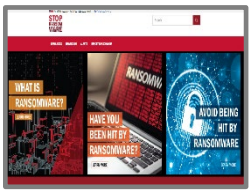
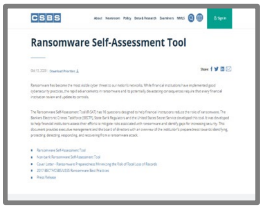
When institutions are victims of other cyber-incidents, they are encouraged to inform their primary regulator(s). Regulators also encourage incident reporting to law enforcement.



R Free

Computer-Security Incident Notification Final Rule: https://www.govinfo.gov/content/pkg/FR-2021-11-23/pdf/2021-25510.pdf	
Sheltered Harbor	
Sheltered Harbor is a not-for-profit subsidiary of the FS-ISAC, that was created to protect customers, financial institutions, and public confidence in the financial system if a catastrophic event like a cyber-attack causes critical systems, including backups to fail. The Sheltered Harbor standard combines secure data vaulting of critical customer account information with a comprehensive resiliency plan to provide customers timely access to their account information and underlying funds during a prolonged systems outage or destructive cyberattack. https://shelteredharbor.org/	 R Paid
Ransomware	
CISA Cyber Security Evaluation Tool (CSET): Ransomware Readiness Assessment (RRA)	
CSET is a desktop software tool that guides network defenders through a step-by-step process to evaluate their cybersecurity practices on their networks. CSET enables users to perform a comprehensive evaluation of their cybersecurity posture using many recognized government and industry standards and recommendations. The RRA is a self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident. CISA tailored the RRA to varying levels of ransomware threat readiness to make it useful to all organizations regardless of their current cybersecurity maturity. https://us-cert.cisa.gov/ics/Downloading-and-Installing-CSET https://github.com/cisagov/cset/	 Free
CISA Ransomware Guide	
The CISA Ransomware Guide is a customer centered, one-stop resource with best practices and ways to prevent, protect, and respond to a ransomware attack. The guide can be used to inform and enhance network defense and reduce exposure to a ransomware attack. The CISA Ransomware Guide includes two resources: • Part 1: Ransomware Prevention Best Practices • Part 2: Ransomware Response Checklist https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf	 Free

Legend	Assessment A	Exercise E	Information Sharing I	Ransomware	Response/Reporting R

CISA Stop Ransomware Resource Site	
The CISA Stop Ransomware website is a collection of guidance and resources designed to help individuals and organizations prevent attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. For more information on the CISA Stop Ransomware Resource Site, contact central@cisa.gov. https://www.cisa.gov/stopransomware	 Free
Conference of State Bank Supervisors (CSBS) & U.S. Secret Service Ransomware Self-Assessment Tool (R-SAT)	
The R-SAT is a question-based tool designed to help financial institutions assess their efforts to mitigate risks associated with ransomware and identify gaps for increasing security. The tool provides executive management and the board of directors with an overview of the institution's preparedness to identify, protect, detect, respond, and recover from a ransomware attack. For more information on R-SAT information visit: https://www.csbs.org/sites/default/files/2020-10/R-SAT_0.pdf	 Free

Legend	Assessment A	Exercise E	Information Sharing I	Ransomware	Response/Reporting R

Appendix A

Ransomware References

- **Conference of State Bank Supervisors (CSBS)**
  - Best Practices for Banks: Reducing the Risk of Ransomware, 2020
- **Cybersecurity & Infrastructure Security Agency (CISA)**
  - Alert (AA21-008A): Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure, 2022
  - Alert (AA21-008A): Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments, 2021
  - Alert (AA21-131A): DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks, 2021
  - Alert (AA21-291A) : BlackMatter Ransomware, 2021
  - Alert (AA21-265A): Conti Ransomware, 2021
  - Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations, 2021
  - Alert (AA20-049A): Ransomware Impacting Pipeline Operations, 2020
  - Security Tips (ST19-001): Protecting Against Ransomware, 2021
  - Security Tip (ST04-014): Avoiding Social Engineering and Phishing Attacks, 2020
  - Security Tip (ST04-006): Understanding Patches and Software Updates, 2019
- **Department of Treasury**
  - Office of Foreign Assets Control Advisory: Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, 2020
  - FinCEN Advisory (FIN-2020-A006): Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, 2020
- **Federal Bureau of Investigation (FBI)**
  - Flash CU-000167-MW: BlackCat/ALPHV Ransomware Indicators of Compromise, 2022
  - Flash CU-000162-MW: Indicators of Compromise Associated with LockBit 2.0 Ransomware, 2022
  - Ransomware Prevention and Response for CISOs: How to Protect Your Networks from Ransomware
  - Flash CU-000161-MW: Indicators of Compromise Associated with Diavol Ransomware, 2021
- **Financial Services Information Sharing and Analysis Center (FS-ISAC)**
  - The Rise and Rise of Ransomware, 2020
- **National Institute of Standards and Technology (NIST)**
  - Special Publication 1800-11, Data Integrity Recovering from Ransomware and Other Destructive Events, dated September 2020
- **Office of the Comptroller of the Currency (OCC)**
  - OCC Bulletin 2020-94: Operational Risk: Sound Practices to Strengthen Operational Resilience, dated 30 October 2020
  - OCC Bulletin 2020-5: Cybersecurity: Joint Statement on Heightened Cybersecurity Risk, dated 16 January 2020