Strengthening Sensitive Data Sharing Practices Between Supervised Institutions and Financial Regulators – Risk-Based Practices Framework

July 2026

I. Introduction

Financial regulators have long requested sensitive strategic, operational and cybersecurity-related information from supervised institutions to fulfill their supervisory responsibilities and statutory obligations. Historically, financial regulators conducted on-site manual inspections of supervised institutions' books and records. Today, this process is increasingly digital, presenting growing risks to the security of both the supervised institutions and the financial regulators that collect and hold data from multiple firms. While the ability to inspect the books and records of financial institutions is foundational to effective oversight, sharing sensitive information through direct file transfers, such as via regulator-managed portals or encrypted email, presents significant risks and should be reconsidered. It is critical to ensure that the supervisory process itself does not introduce unnecessary risks to supervised institutions or regulatory agencies themselves.

In response to these risks, the Federal Reserve, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation issued an interagency statement outlining a new coordinated approach for handling sensitive financial institution data during supervisory examinations.[1] That statement recognizes the sensitivity of certain categories of data and notes the agencies will consider a range of options to minimize collecting and storing this information. Under this new approach, supervised institutions are responsible for identifying for regulators any requested data or documents the institution considers highly sensitive.

The following document provides a set of risk-based practices to assist supervised institutions in identifying sensitive data that should be subject to alternate sharing methods to ensure that information is adequately protected in a threat environment where this information and the regulators that collect it are a target. Those alternate review methods include supervised institutions providing firm-controlled access to sensitive data either electronically via firm-hosted applications, by screen-sharing or physically via on-site review.

A. Background

Supervised institutions go to great lengths to protect the end-to-end security of their sensitive data, carefully controlling who can access it, how it is transmitted and stored, when and how it is disposed of and when it cannot be shared in the first place. Institutions prioritize data minimization strategies in accordance with regulatory requirements and to limit their overall attack surface, as the existence of multiple copies of sensitive information increases the risk of exposure and misuse. Accordingly, when asked to share sensitive information externally, regardless of recipient, institutions consider how to minimize the information shared and what additional protective measures are needed. These measures are critical to maintaining institutions' long-term data security.

Supervised institutions and their regulators face a shared and growing threat from increasingly sophisticated cyber adversaries, including nation-state actors and organized criminal groups. Given the interconnected nature of the financial system, securing sensitive information held by supervised institutions and regulators alike is a mutual priority. Effective protection requires ongoing collaboration, shared responsibility and coordinated efforts to strengthen collective resilience against cyber threats.

When sensitive information is sent directly to regulators or indirectly via their agents or contractors, supervised institutions inevitably lose some degree of control over its security, management and retention. Even with robust transfer protocols in place, once sensitive data leaves an institution's environment, visibility into its handling and protection becomes limited. This limited visibility begins with the security of the transfer method itself, but extends to how the sensitive data is accessed, managed, copied, redistributed, safeguarded and ultimately disposed of on an external system.

[1] FED. RESERVE BD., FED. DEP. INS. CORP., OFF. COMPTROLLER OF THE CURRENCY, *Statement regarding Coordinated Federal Banking Agency Approach for the Handling of Highly Sensitive Information During Examinations* (Jul. 2026), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20260716a1.pdf.

After cybersecurity incidents discovered at the Office of the Comptroller of the Currency in February 2025 and the Department of the Treasury in December 2024, the U.S. prudential banking regulators worked with industry to update, standardize and strengthen pragmatic sharing practices for sensitive supervisory data. Among other things, these updated practices:

- Reduce the attack surface of supervisory data by limiting information requested and provided to information that is both material to supervisory obligations concerning safety and soundness, investor protection, market integrity and/or risk management while balancing the data security concerns of the supervised institutions;
- Encourage consistency among secure data transfer methods and protections in line with risk-based best practices;
- Increase reliance on information sharing via firm-controlled access, electronically or physically via on-site review;
- Apply additional content and access control measures for particularly sensitive types of information; and
- Establish clear alignment between institutions and regulators on the protection, storage, sharing and disposal of directly transferred data.

These improved data sharing practices will collectively reduce the cybersecurity risks associated with the collection, retention and transmission of sensitive supervisory information, benefiting customers, investors, financial regulators and supervised institutions alike.

B. Purpose of This Document

The risk-based practices identified in this document reflect extensive feedback from financial institutions and other stakeholders collected through a survey and a series of industry discussions. They are designed to provide supervised institutions and their financial regulators with clear, consistent baseline expectations for securely sharing and managing sensitive data across a wide range of data categories.

These practices are intended to apply broadly to requests for information, including inquiries, examinations, ongoing monitoring submissions, routine meetings, ad hoc data requests and related correspondence. The intended audience includes U.S. federal financial regulators, state banking agencies and other industry-specific regulatory bodies such as insurance regulators, as well as the agents and contractors that regulators hire to collect information on their behalf and the institutions these regulators supervise.

These practices are intended to facilitate constructive collaboration as the threat landscape continues to evolve, ensuring that data security remains a shared priority and a routine topic of discussion.

II. Methods for Sharing and Protecting Sensitive Information

Financial institutions regularly share a variety of sensitive information with their regulators to support the supervisory process. Broadly, this information falls into four institution-identified categories: Strategy, Planning & Financial Data (e.g., strategic initiatives and transaction details), Security, Resilience & Third-Party Risk Management Data (e.g., cybersecurity controls and assessments and architecture and network diagrams), Internal Business Data (e.g., governance and employee information) and Legal, Regulatory & Compliance Data (e.g., privileged investigations and audit filings). Given the sensitivity and diversity of this information, regulators and institutions should use appropriate methods for sharing it and consistently apply protective measures tailored to each specific data type.

Institutions identified three primary methods for sharing sensitive data with regulators, as well as measures that can be deployed to further protect or control access to particularly sensitive types of information. These measures are previewed below before discussion of specific risk-based best practices.

A. Methods for Sharing Sensitive Data

Institutions emphasized that the method through which they deliver sensitive information to regulators has the greatest impact on their ability to control and ensure the continued security of this information. Sensitive data is currently shared through one of three methods:

- *Direct Transfer*. Institutions frequently upload documents directly into regulator-managed portals, such as the Federal Reserve's OASiS, transmit data to regulators by email, or, less frequently, provide hard copies. Direct transfer methods should utilize cybersecurity best practices, including appropriate encryption, authentication, access management and password protection. Moreover, regulator systems holding supervised institutions' data should be subject to robust cybersecurity and resiliency standards that match the sensitivity of the information entrusted to them, and regulators should use the utmost care in selecting agents and contractors that will be handling any sensitive financial institution information. However, even with these practices, direct transfers inherently involve risks associated with the creation of additional copies of sensitive data, loss of institutional control over that data and limited visibility into data access, redistribution and retention.

- *Firm-Controlled Access.* Institutions sometimes share sensitive information with regulators in multiple ways that avoid creating and sending additional copies that the institution no longer possesses. Regulators can be provided with persistent or temporary electronic access to sensitive information through firm-hosted applications that record views and restrict access, copying and downloading. Alternatively, institutions may conduct screen-sharing sessions that allow regulators to view data without file transfer capabilities. Institutions also arrange physical, on-site data review using firm-controlled devices. These options are highly desirable because they limit the number of copies of the data and reduce the corresponding attack surface. Importantly, these options ensure institutions' compliance with their own existing data security protocols.

- *Oral Discussion.* Institutions occasionally convey certain sensitive information exclusively through oral briefings, without providing written responses, documentation or visuals. Oral discussions often provide helpful context that can address the regulator's underlying request and reduce the need for direct data sharing. However, meeting notes and subsequent correspondence to oral discussion require the same considerations for both direct transfer and firm-controlled access methods.

Alternatively, for especially sensitive information, institutions and regulators may agree that alternative, less sensitive information satisfies the regulators' request.

B. Methods for Limiting Content or Controlling Access to Shared Sensitive Data

When institutions share certain sensitive data with regulators either directly or through firm-controlled access pursuant to the regulator's request, there often remain significant concerns about the recipient audience, the format of the data, and incidental or especially sensitive information contained within files that should not be exposed.

To effectively and sufficiently mitigate these risks, supervised institutions and financial regulators should proactively consider deploying one or more of the following protective measures:

- *Access Restrictions.* Narrow regulator audience by tracking and controlling access to certain examiners with a demonstrable need to know. Access to firm-hosted environments should track and restrict user access, copying, downloading, printing and sharing.

- *Summaries and Aggregation.* Create summaries or aggregated data instead of transmitting detailed records, individually identifiable information or entire privileged documents. Although it can take additional resources to prepare data in these formats, doing so can be extremely helpful to reduce unnecessary exposure to large sets of data or otherwise especially sensitive content.

- *Samples and Excerpts.* Provide samples or excerpts instead of comprehensive data sets or documents to reduce unnecessary exposure. As with summaries and aggregated data, samples and excerpts are especially preferable where entire data sets are not necessary to address a regulator's request or are unlikely to ever be analyzed in full by the regulator. Additionally, incomplete data sets can pose inherently less risk of misuse, if ever exposed.

- *Redactions.* Redact sensitive details such as personally identifiable information (PII), employee compensation and performance data, board member evaluations, internal IP addresses and any material protected by the attorney-client privilege or the attorney work product doctrine.

- *Restricted File Formats.* Share information in the form of screenshots or other restricted formats rather than editable native files, such as Word or Excel. A screenshot is inherently more difficult to extract data from and misuse, while still providing regulators with access to a primary data source.

- *Secure Storage, Retention and Disposal.* Prior to sharing information via direct transfer, align in writing on where the data will be stored, who will have access to it, what protections will ensure it remains secure and what process to follow if further sharing or changes to the storage arrangement are needed. Align on the duration of retention, which may, if an exact retention period is not yet known, include periodic points in time to revisit retention needs and designating parties responsible for appropriate disposition at those times. Agree on a method of data disposal, such as returning the data to the institution or securely destroying it. And memorialize agreements regarding secure storage, retention and disposal in writing.

These measures can be used in combination with other methods, e.g., providing on-site, view-only access to a complete data set while directly sharing only a sample or aggregated data, to best mitigate risk while meeting supervisory aims.

III. Risk-Based Sharing Best Practices Across Sensitive Data Categories

The practices outlined below establish clear, consistent, risk-based standards to guide supervised institutions when designating for financial regulators what supervisory data contains sensitive information warranting heightened protection. They are intended to ensure that supervisory data sharing is secure, effective and aligned with contemporary cybersecurity requirements appropriate for the threat environment.

Institutions identified four major categories of sensitive data frequently requested by financial regulators:

- Strategy, Planning & Financial Data
- Security, Resilience & Third-Party Risk Management Data
- Internal Business Data
- Legal, Regulatory & Compliance Data

Within each major category, institutions also identified especially sensitive data types that require additional methods of protection.

In accordance with the risk-based practices herein, financial regulators should enable and encourage supervised institutions to provide firm-controlled access to sensitive data across all four categories electronically via firm-hosted applications, by screen-sharing or physically via on-site review, while allowing institutions flexibility to implement additional protections for especially sensitive data on a case-by-case basis.

If a financial regulator receives sensitive data from a supervised institution directly (e.g., via a regulator-hosted portal or an encrypted email), the financial regulator should be prepared to align with the supervised institution regarding how that data will be protected and ultimately disposed of, and who will access it, such as the methods described in Section II.

A. Strategy, Planning & Financial Data

Financial regulators may request that supervised institutions share the following types of sensitive strategy, planning, and financial data: (i) strategic objectives and implementation plans, (ii) succession-related information, (iii) capital plans, (iv) material non-public information, (v) M&A and transaction information, (vi) financial statements, (vii) investment strategies and (viii) revenue analyses.

Institutions have been asked to share this information through direct transfer, uploading materials using either regulator-managed portals or encrypted or password-protected emails. However, some institutions place these materials in a firm-controlled electronic environment or offer on-site review only, and, for especially sensitive data types, some institutions offer oral briefings only or decline to provide certain files altogether.

Financial regulators should enable and encourage supervised institutions to provide firm-controlled access to most of these materials either electronically via firm-hosted applications or screen-sharing or physically via on-site review.

Pre-deal M&A information is exceptionally sensitive and should be shared through oral discussion only or with additional protective measures, such as narrowing regulator audiences and providing information in summary form until plans become public. Succession-related information is among the most sensitive data that a supervised institution holds. The cost to a firm from leaked succession-related information outweighs any examiner's need-to-know for purposes of assessing an institution's safety and soundness.

B. Security, Resilience & Third-Party Risk Management Data

Financial regulators often request that supervised institutions share the following types of sensitive security, resilience and third-party risk management data: (i) technical information such as network diagrams and configuration settings for both the financial institution and its vendors, (ii) specific security controls, (iii) security testing methodologies, (iv) resilience and backup capabilities, (v) vulnerability lists and acknowledgments, (vi) incident-management information and disruptive-event records, (vii) results of security assessments such as penetration tests and red-team outputs and (viii) third-party engagement reports.

Information in this category is particularly sensitive because disclosure to a malicious third party could pose a material risk to firm operations. Institutions have been asked to share this information through direct transfer, uploading materials using either regulator-managed portals or encrypted or password-protected emails. However, some institutions place these materials in a firm-controlled electronic environment, offer on-site review only or choose not to share this information.

Once identified by supervised institutions, financial regulators should enable and encourage firm-controlled access to most of these materials either electronically via firm-hosted applications or screensharing or physically via on-site review and, wherever possible, enable and encourage supervised institutions to share security and resilience information through oral briefings only.

Raw technical artifacts such as configuration files are exceptionally sensitive data types that should be further protected by narrowing regulator audiences, providing summaries of materials, and redacting unnecessary sensitive information. Terms with technology vendors are also exceptionally sensitive because they could cause substantial competitive harm if revealed to another firm, and they should thus be handled with similar additional protections. Lastly, supervised institutions' most sensitive cybersecurity and technology data, including penetration test or red-team outputs, detailed network diagrams, IP addresses, control discussions and locations of data centers, should not be shared externally.

C. Internal Business Data

Financial regulators often request that supervised institutions share the following types of sensitive internal business data: (i) Board of Directors and senior governance body meeting materials, (ii) board assessment or evaluation materials, (iii) designs for emerging products, services and innovations, (iv) intellectual property, (v) detailed business reviews, (vi) trading data and information about client accounts, (vii) fraud monitoring-related materials, (viii) customer, investor and employee PII and other sensitive information, (ix) employee compensation and performance data and (x) AI-related information including governance materials, models, data sources and validation records.

Institutions have similarly been asked to share this information through direct transfer, uploading materials using either regulator-managed portals or encrypted or password-protected emails. However, some institutions place these materials in a firm-controlled electronic environment, offer on-site review only or decline to provide certain files altogether. Many institutions also report using redaction before transmission where PII, individual employee data or internal deliberation is involved.

Once identified by supervised institutions, financial regulators should enable and encourage firm-controlled access to most of these materials either electronically via firm-hosted applications or screensharing or physically via on-site review.

Customer and employee PII, individual employee compensation and performance information and records of internal board and executive deliberations are exceptionally sensitive data types that should be shared with additional protective measures, including narrowing regulator audiences and redacting, aggregating or excerpting PII and individually identifiable employee data.

D. Legal, Regulatory & Compliance Data

Financial regulators often request supervised institutions share the following types of sensitive legal, regulatory, and compliance data: (i) internal audit methodologies and results, (ii) AML/BSA suspicious activity report filings and related modeling and tuning, (iii) non-privileged sensitive investigation materials and (iv) materials subject to the attorney-client privilege or the attorney work product doctrine.

Institutions have been asked to share this information through direct transfer, uploading materials using either regulator-managed portals or encrypted or password-protected emails. However, they sometimes restrict or refuse to transmit unredacted privileged documents or offer on-site review only.

Once identified by supervised institutions, financial regulators should enable and encourage firm-controlled access to most of these materials, either electronically via firm-hosted applications or screen-sharing, or physically via on-site review.

Given the extremely sensitive nature of legal data, regulators should also enable and encourage institutions to withhold any access to materials that are attorney-client privileged, subject to the attorney work product doctrine or otherwise contain legal advice because regulators' examination authority does not override attorney-client

privilege.[2] When sharing is unavoidable, supervised institutions should be able to deploy additional protections to restrict regulator audiences, provide summaries of materials and redact unnecessary privileged information.

IV. Conclusion

Financial regulators and supervised institutions will continue to face persistent threats from well-resourced and sophisticated cyber adversaries, including nation-state actors and affiliated criminal organizations. In this evolving threat landscape, supervised institutions and their financial regulators have a responsibility to ensure that sensitive data is shared only under conditions that reflect modern best practices for cybersecurity and incident response.

By reducing unnecessary data exposure and preserving firm-level discretion over the most sensitive materials, regulators can work in partnership with the industry to strengthen the resilience of the supervisory process itself. Implementing meaningful reforms will help reduce the risk to sensitive information and ensure that it is appropriately safeguarded, ultimately supporting stronger cybersecurity across the financial system.

[2] *See, e.g.,* Memorandum from Cleary Gottlieb Steen & Hamilton LLP, Covington & Burling LLP, Davis Polk & Wardwell LLP, Debevoise & Plimpton LLP, Simpson Thacher & Bartlett LLP, Sullivan & Cromwell LLP and Wilmer Cutler Pickering Hale and Dorr LLP, "Banking Regulators' Examination Authority Does Not Override Attorney-Client Privilege." (May 16, 2018).

Appendix A: Risk-Based Sharing Best Practices Across Sensitive Data Categories

Data Category	Sensitive Data Types *Especially sensitive data types appear in bold.*	Risk-Based Sharing Best Practice	Additional Risk-Based Access Restrictions for Especially Sensitive Data Types
Strategy, Planning & Financial Data	• **Succession-related information** • Capital plans • Material non-public information • **M&A and transaction information** • Financial statements • Investment strategies • Revenue analyses	• Provide firm-controlled access, either electronically via firm-hosted applications or screen-sharing, or physically via on-site review	• **Share through oral discussion only** • **Narrow regulator audiences** • **Provide information in summary form until plans become public** • **Do not provide succession-related information**
Security, Resilience & Third-Party Risk Management Data	• **Technical information such as network diagrams and configuration settings for both the financial institution and its vendors** • Specific security controls • Security-testing methodologies • Resilience and backup capabilities • Vulnerability lists and acknowledgments • Incident-management information and disruptive-event records • **Results of security assessments such as penetration tests and red-team outputs** • **Third-party engagement reports**	• Provide firm-controlled access, either electronically via firm-hosted applications or screen-sharing, or physically via on-site review • Share security and resilience information through oral briefings only	• Narrow regulator audiences • Provide summaries of materials • Redact unnecessary sensitive information • Do not provide the most sensitive cybersecurity and technology data, including penetration test or red-team outputs, detailed network diagrams, IP addresses, control discussions and locations of data centers, when it would pose significant operational risks if exploited

Data Category	Sensitive Data Types *Especially sensitive data types appear in bold.*	Risk-Based Sharing Best Practice	Additional Risk-Based Access Restrictions for Especially Sensitive Data Types
Internal Business Data	• **Board of Directors and senior governance body meeting materials** • Board assessment or evaluation materials • Designs for emerging products, services and innovations • Detailed business reviews • Trading data and client account information • Fraud monitoring-related materials • **Customer and employee PII and other sensitive information** • **Employee compensation and performance data** • AI-related information including governance materials, models, data sources and validation records	• Provide firm-controlled access, either electronically via firm-hosted applications or screen-sharing, or physically via on-site review	• Narrow regulator audiences • Redact, aggregate or excerpt PII and individually identifiable employee data
Legal, Regulatory & Compliance Data	• Internal audit methodologies and results • AML/BSA suspicious activity report filings and related modeling and tuning • Non-privileged sensitive investigation materials • **Materials subject to the attorney-client privilege or the attorney work product doctrine**	• Provide firm-controlled access, either electronically via firm-hosted applications or screen-sharing, or physically via on-site review	• Narrow regulator audiences • Provide summaries of materials • Redact unnecessary privileged information • Do not provide data subject to attorney-client privilege, protected by the attorney work product doctrine or containing legal advice