MAYER | BROWN

AVOID AN 'OCTOBER SURPRISE': DOJ'S DATA SECURITY RECORDKEEPING AND AUDITING RULES GO LIVE

Adam Hickey (Mayer Brown) & Wilder Angarita (Pondurance)

October 30, 2025

PARTNER

CYBERSECURITY & DATA PRIVACY, NATIONAL SECURITY, GLOBAL INVESTIGATIONS & ENFORCEMENT

ADAM HICKEY

AHICKEY@MAYERBROWN.COM

SR. CYBERSECURITY CONSULTANT AND VCISO – C-CISO, CISSP, CISM, CISA, CASP

WILDER ANGARITA

WILDER.ANDRADE-ANGARITA@PONDURANCE.COM

AGENDA

1. Data Security Program & Compliance Requirements
2. Scoping the Audit
3. Testing the Data Compliance Program
4. Testing the Security Requirements
5. Deliverables, Findings, And Remediation Framework
6. Q&A

01

DATA SECURITY PROGRAM & COMPLIANCE REQUIREMENTS

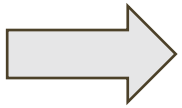
DATA SECURITY PROGRAM TIMELINE

‡Starting April 8, 2025, entities and individuals are required to comply with the DSP's prohibitions and restrictions, and with all other provisions of the DSP with the exception of the affirmative obligations of subpart J (related to due diligence and audit requirements for restricted transactions), § 202.1103 (related to reporting requirements for certain restricted transactions), and § 202.1104 (related to reports on rejected prohibited transactions). Starting October 6, 2025, entities and individuals must comply with subpart J and §§ 202.1103 and 202.1104.

KEY QUESTIONS UNDER DOJ'S DATA SECURITY PROGRAM

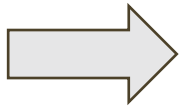
Are you a U.S. Person and do you collect covered data?

- "Bulk" sensitive personal data (U.S. persons)
  - Covered personal identifiers
  - Human 'omic data
  - Biometric identifiers
  - Precise geolocation info
  - Personal health or financial data
- Government-related data (no bulk threshold):
  - Precise locations within the GRLD list
  - "Marketed as" gov't employee SPD



Do any covered persons have "access" to that data as a result of a covered transaction?

- Who has access to the data we collect and store?
  - Employees? (employment agreement)
  - Vendors? (vendor agreement)
  - Investors? (investment agreement)
  - Commercial partners or licensees? (data brokerage agreement)
- Are any of those persons "covered persons"?
  - Look at residence, jurisdiction, ownership and ties to other covered persons (like employment).



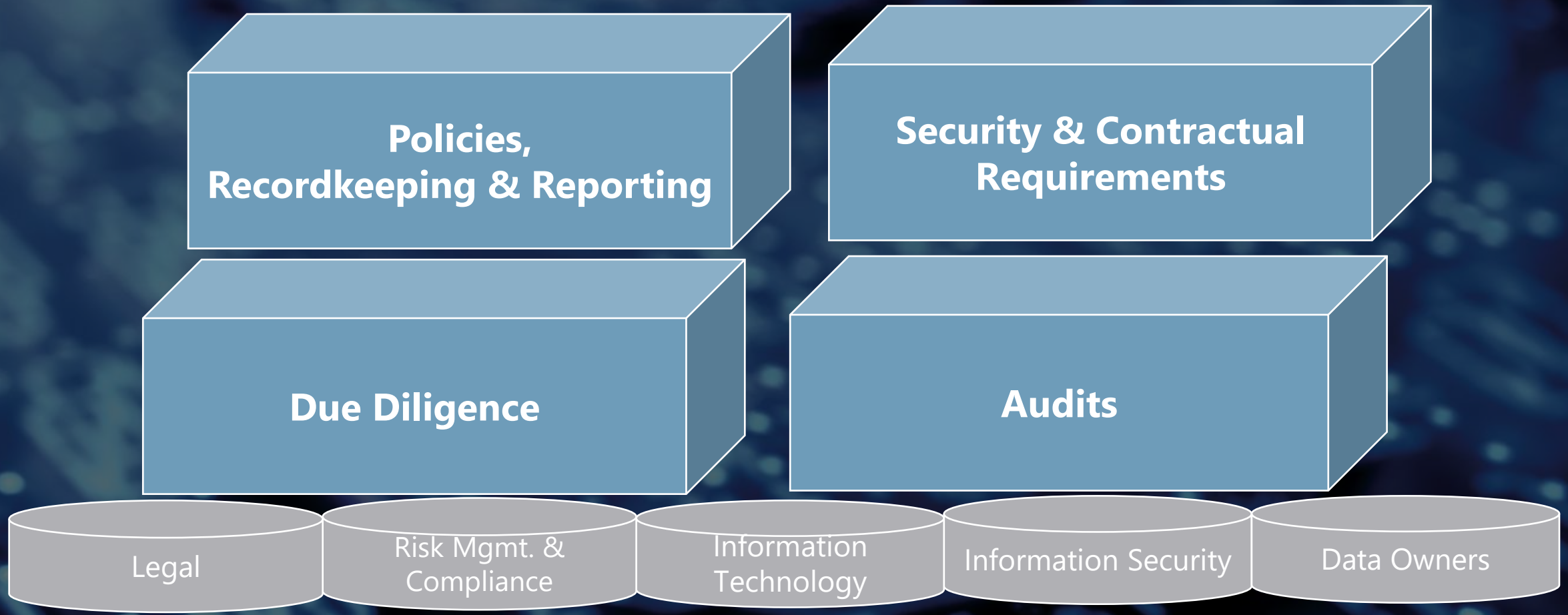
Does an exemption apply?

- Financial services.
- Corporate group transactions.
- Telecommunications services.
- Drug, biological product, and medical device authorizations.
- CFIUS mitigation agreements.
- Transactions authorized by federal law or international agreements.
- Personal communications.
- Information or informational materials.

RESTRICTED TRANSACTIONS

202.401 Authorization to conduct restricted transactions. (a) *Restricted transactions.* Except as otherwise authorized pursuant to subparts E or H of this part or any other provision of this part, no U.S. person, on or after the effective date, may knowingly engage in a covered data transaction involving a vendor agreement, employment agreement, or investment agreement with a country of concern or covered person unless the U.S. person complies with the security requirements (as defined by § 202.408) required by this subpart D and all other applicable requirements under this part.

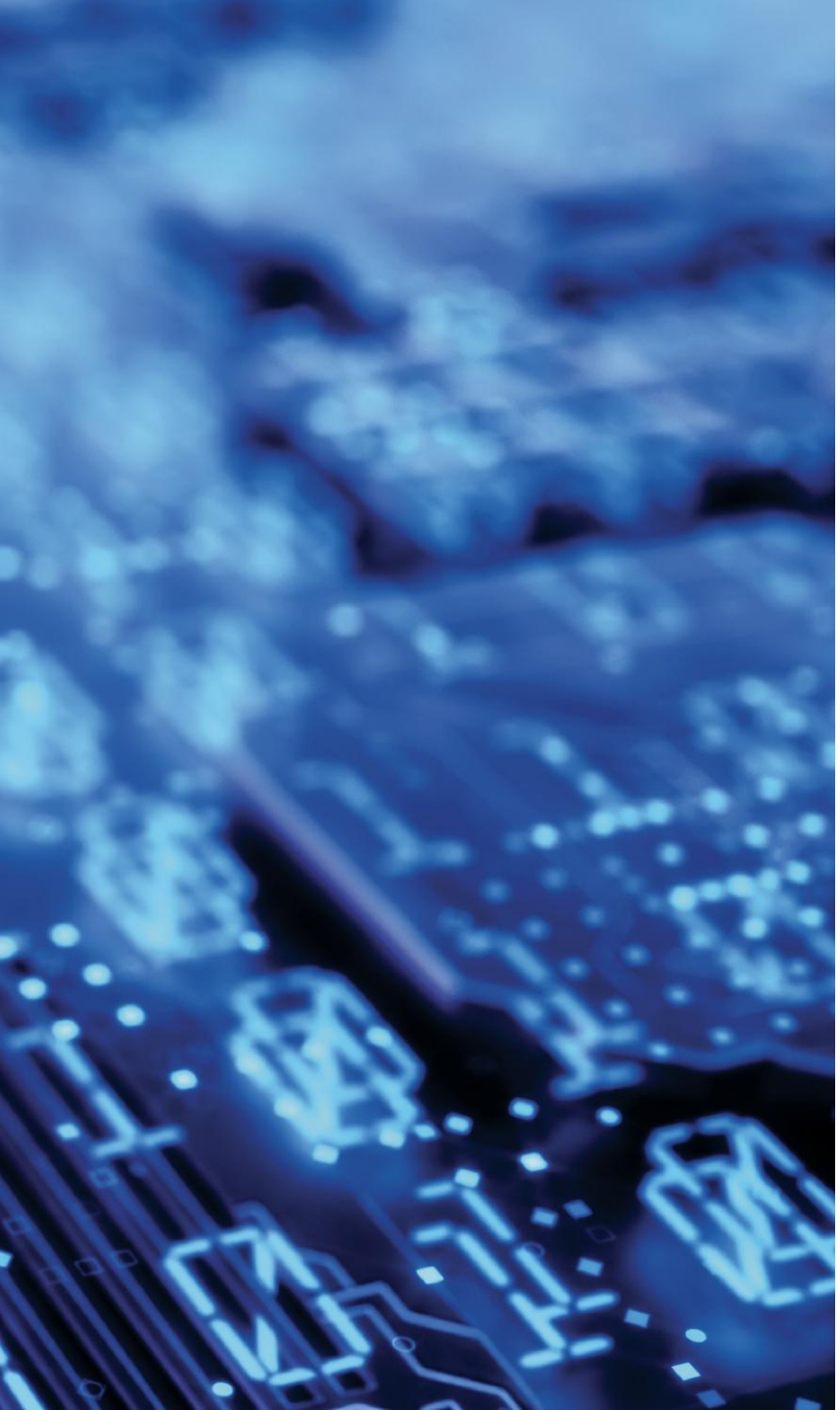
COMPLIANCE PROGRAM FOR RESTRICTED TRANSACTIONS: BUILDING BLOCKS



SECURITY REQUIREMENTS OVERVIEW

- For a *covered data transaction* involving a *vendor agreement*, *employment agreement*, or *investment agreement* with a *country of concern* or *covered person*, a *U.S. person* must comply with the following security requirements:
  - **Organizational-level requirements** such as asset management, designating an individual accountable for cybersecurity, maintaining policies for new hardware/software deployments, and patching vulnerabilities quickly (within 45 calendar days);
  - **System-level requirements** such as implementing multifactor authentication on all covered systems, collecting logs, and limiting system access to only individuals who need it to perform their jobs; and
  - **Data-level requirements** such as implementing a data retention and deletion policy, applying encryption during transit and storage, and using privacy enhancing technologies.
- **Keep in Mind:** The security requirements are based on already-existing standards and frameworks such as the NIST Cybersecurity Framework, NIST Privacy Framework, and CISA Cybersecurity Performance Goals.
- **Related Requirements:**
  - A written **policy** that describes the implementation of the security requirements and that is certified annually by an officer, executive, or other employee responsible for compliance (§ 202.1001(b)(4)).
  - A data **risk assessment** that explains how the requirements prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable, taking into consideration the likelihood of disclosure and harm based on the nature of the transaction and the data at issue. Includes mitigation. (Required for each [class of] restricted transaction[s].]
  - An independent examination of the U.S. person's compliance with the security requirements as part of the required annual **audit** (§ 202.1002(e)(4)).

While the requirements on covered systems and on an organization's governance of those systems apply more broadly than to the data at issue and the restricted transaction itself, CISA assesses that implementation of these requirements is necessary to validate that the organization has the technical capability and sufficient governance structure to appropriately select, successfully implement, and continue to apply the covered data-level security requirements in a way that addresses the risks identified by DOJ for the restricted transactions.
– CISA



WHAT CHANGED OCTOBER 6?

- **Recordkeeping** requirements (effective April 8, 2025) --- even more important. (§ 202.1101)
  - Requires "a full and accurate record of each transaction" "subject to" Part 202.
  - Covered transactions only? (I.e., Access to covered data by covered persons?)
  - Or do you have to prove a negative?
- **Annual reports** by covered-person-owned (25%) U.S. persons engaged in restricted **cloud-computing services** (after this date) (§ 202.1103).
- **Reports on rejected data brokerage transactions** (after this date) (§ 202.1104).
- **Due diligence** program implemented for restricted transactions. (§ 202.1001)
- **Data Compliance Program** (§§ 202.1001, 202.1101) must be in place.
  - Must be memorialized in a "written policy" that is certified annually by an officer, executive, or other employee responsible for compliance.
  - Must address certain topics, such as due diligence on the nature of covered data is the subject of restricted transactions, the identity of the transaction parties, and the end-use of the data.
  - Must include a written **Security Requirements Policy**, separately certified annually by a responsible employee.
- **Audit period began**. (§ 202.1002)
  - Applies to any U.S. person engaging in restricted transactions "on or after October 6, 2025."
  - "Must be performed once for each calendar year" in which you engage in any restricted transactions.
  - "Must cover the preceding 12 months."

RECORDKEEPING AND REPORTING

- **General Recordkeeping (§ 202.1101(a)):** For transactions subject to the rule (specific/general licenses, data brokerage with foreign persons, restricted transactions), *U.S. Persons* must keep a full and accurate record of each such transaction engaged in and keep the record available for at least 10 years after the date of such transaction.
- **Additional Recordkeeping for Restricted Transactions (§ 202.1101(b)):**
  - Keep a full and accurate record of **each restricted transaction** engaged in for at least 10 years after the date of such transaction, including documentation of:
    - Due diligence conducted to verify the data flow (types of data, identities of transaction parties, end-use of data).
    - Method of data transfer.
    - Dates of the transaction.
    - Any agreements or other records created in connection with the transaction.
  - Written policies on the data compliance program and security requirements.
  - The results of annual audits.
  - An annual certification by a responsible employee, officer, or executive responsible for compliance of the completeness and accuracy of the records documenting due diligence.
- **Reporting Requirements:**
  - **Annual Reports (§ 202.1103):** For restricted transactions involving cloud-computing services, and where a country of concern or covered person owns 25% or more of the U.S. person's equity interests (directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise).
  - **Proactive reports on rejected prohibited transactions (§ 202.1104):** Any *U.S. person* that rejects an offer to engage in a prohibited transaction must file a report within 14 days of rejecting such offer.
  - **Proactive reports on violations by a foreign person engaging in onwards data brokerage (§ 202.301):** Any *U.S. person* that becomes aware of a known or suspected violation of the contractual requirement to refrain from engaging in a subsequent data brokerage transaction with a *covered person* or *country of concern* must file a report within 14 days of becoming aware.
  - **Reports to be furnished on demand (§ 202.1102):** DOJ may demand "complete information relative to any act or transaction or covered data transaction, regardless of whether such act, transaction, or covered data transaction is effected pursuant to a license or otherwise."

Keep in Mind: *U.S. Persons* engaging in a transaction subject to a general or specific license may also have to comply with reporting requirements as a condition of those licenses.

The compliance program suitable for a particular U.S. person would be based on that person's individualized risk profile and would vary depending on a variety of factors, including the U.S. person's size and sophistication, products and services, customers and counterparties, and geographic locations. Depending on a U.S. person's individualized risk profile, a reasonable compliance program could include streamlined measures such as contractual safeguards and automated review of counterparties' technical indicators, such as IP address locations. – 90 Fed. Reg. 1696

DUE DILIGENCE & A DATA COMPLIANCE PROGRAM

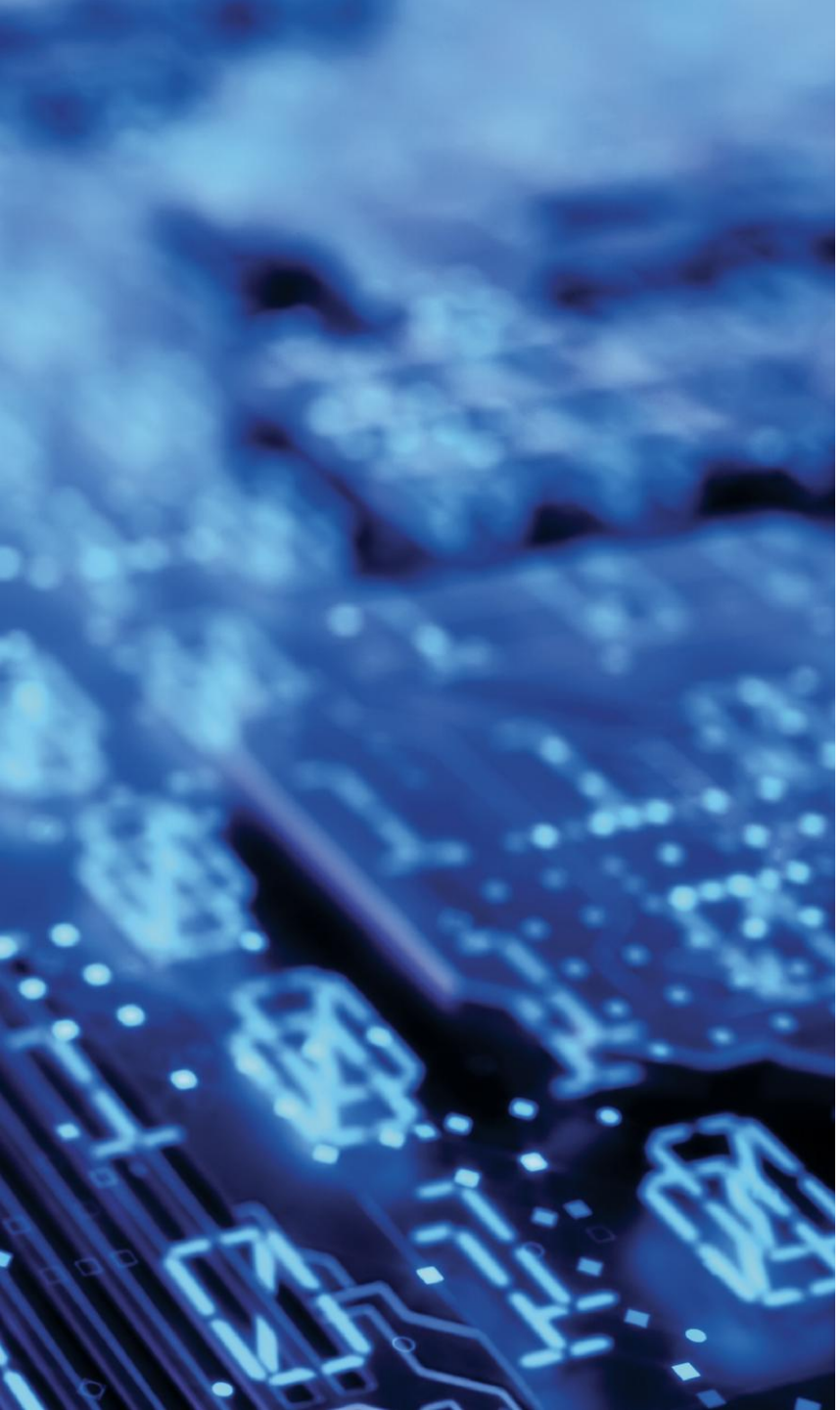
- **Applies to:** *U.S. Persons* engaging in any restricted transactions on or after October 6, 2025.
- **Key Requirements:**
  - **Risk-Based Verification (§ 202.1001(b)(1)):**
    - Verify and log data flows for restricted transactions **in an auditable manner**.
    - Capture:
      - Types and volumes of government-related or bulk U.S. sensitive personal data.
      - Identities of transaction parties (incl. ownership, citizenship, residence).
      - Data end-use and transfer methods.
  - **Vendor Verification (§ 202.1001(b)(2)):** Implement risk-based procedures to verify vendor identities.
  - **Written Policies & Certifications (§ 202.1001(b)(3-4)):**
    - Create a written policy detailing the data compliance program.
    - Create a written policy detailing implementation of the security requirements.
    - Annual certification of both policies by a responsible employee, officer, or executive.

AUDIT REQUIREMENTS (§ 202.1002)

- **Applies to:** *U.S. Persons* engaging in any restricted transactions.
- **Cadence:** Once for each calendar year in which the *U.S. Person* engages in any restricted transactions, covering the preceding 12 months.
- **Effective Date:** Because the audit requirement did not become effective until October 6, 2025, *U.S. Persons* will not have to audit restricted transactions before that date. However, based on the text of the rule, an audit would be required in 2025 for restricted transactions engaged in between October 6 and December 31, 2025. DOJ has not yet provided guidance on this issue.
- **Auditor Requirements (§ 202.1002(b)):**
  - Must be independent but does not have to be external.
  - Cannot be a *covered person* or *country of concern*.
  - Must be qualified to examine, verify, and attest to the *U.S. Person's* compliance with the security requirements and all other applicable requirements.
- **Audit Scope and Report (§ 202.1002(e-f)):**
  - The audit must cover the *U.S. Person's* restricted transactions, compliance program, security requirements, and required records.
  - The auditor must deliver an audit report to the *U.S. Person* (within 60 days) with an evaluation of the data compliance program and security requirements and recommendations for improvements.
  - The *U.S. Person* must retain the audit report for a period of 10 years.

Factors Relevant to Assessing Auditor "Independence"

- The specific internal organization of the U.S. company.
- The internal auditor's reporting relationship and accountability to the U.S. company's senior leadership and/or the board of directors.
- The training and expertise possessed by the internal auditor.



DEEP DIVE: AUDIT REPORT REQUIREMENTS (§ 202.1002(F)(2))?

🚫

Restricted Transactions:
Detail the nature of any **restricted transactions** the U.S. person engaged in.

🗺️

Audit Methodology:
Describe the **methodology** used, including documents, interviews, and systems examined.

✅

Program Effectiveness:
Describe the **effectiveness and implementation** of the U.S. person's data compliance program.

⚠️

Vulnerabilities & Deficiencies:
Describe any **vulnerabilities or deficiencies** that have affected or could affect the risk of **unauthorized access** to covered data.

❌

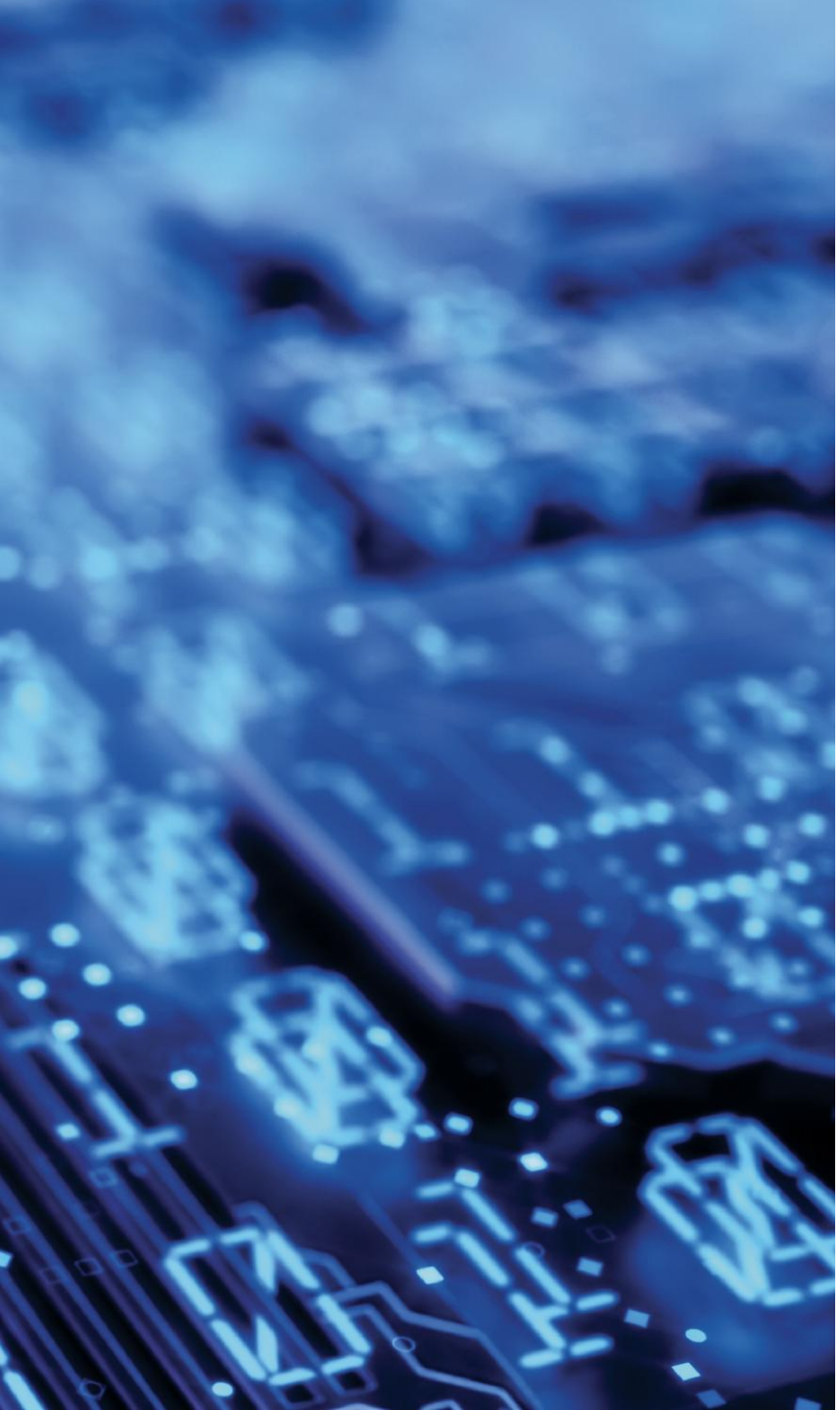
Failures:
Detail any **instances where security requirements failed** or were ineffective in mitigating the risk of **unauthorized access** by a country of concern or covered person.

💡

Recommendations:
Provide **recommendations** for improvements to policies, practices, or other aspects of the business to ensure compliance with the security requirements.

02

SCOPING THE AUDIT



SCOPING: WHAT IS "RESTRICTED" FOR YOU?

Coordination with Counsel:

- Partner with legal counsel to interpret the rule and validate scoping decisions.
- Confirm applicable exemptions and licensing arrangements.
- Limit scope to transactions governed by Subpart D – Restricted Transactions.

Transaction Identification:

- Map all transactions where covered data is accessible by covered persons or countries of concern.
- Include vendor, employment, and investment arrangements with potential data exposure.
- Document each logical and physical access pathway to define the audit universe.

OUR FOUR-PHASE AUDIT METHODOLOGY

01

Planning & Intake Phase

Comprehensive document requests, detailed system and data mapping, thorough risk profiling, and statistical sampling plan development.

02

Fieldwork Execution

Intensive control testing across all due diligence requirements, organizational controls, system-level protections, data-level safeguards, plus records and reporting verification.

03

Analysis & Risk Rating

Systematic deficiency severity assessment, comprehensive risk-of-access analysis, and development of targeted remediation recommendations with clear priorities.

04

Reporting & Closeout

Formal audit report issuance with executive summary, detailed findings, and complete evidence archive supporting 10-year retention requirements.

03

TESTING THE DATA COMPLIANCE PROGRAM

DUE DILIGENCE: CORE EXAMINATION AREAS

Data Flow Verification

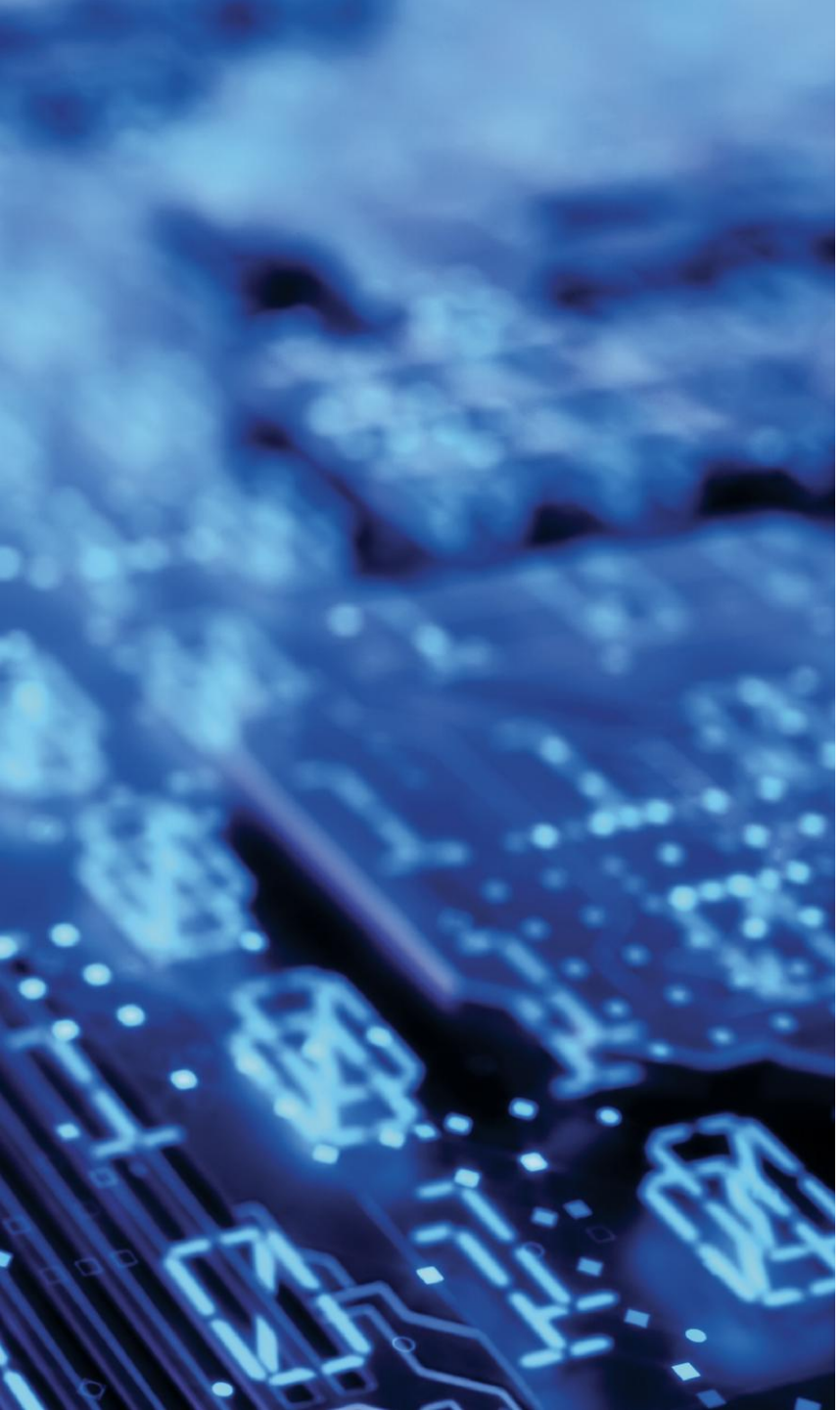
Risk-based verification of complete data flows in restricted transactions including data types, volumes, party identities, intended end-use purposes, and transfer methodologies with full audit trails.

Counterparty Screening

Comprehensive risk-based procedures to verify counterparty identities, ownership structures, and residency status.

Program Documentation

Written policies comprehensively describing the data compliance program structure and security-requirements implementation approach, supported by required annual executive certifications.



TEST PROCEDURES: DATA FLOW VERIFICATION

1

Transaction Sampling

Select representative sample of restricted transactions from the complete audit period using statistical sampling methodology for maximum coverage and confidence.

2

Comprehensive Tracing

For each selected transaction, trace and document all covered data types, volumes, involved parties, end-use purposes, and transfer methods with complete audit trail.

3

Evidence Reconciliation

Reconcile transaction logs to contracts, data maps, and system evidence including DLP logs, flow logs, and ETL job records for complete validation.

4

Auditability Assessment

Evaluate whether all records meet auditability standards: complete documentation, accuracy verification, and tamper-evident characteristics for regulatory compliance.

TEST PROCEDURES: COUNTERPARTY VETTING

Screening Procedures Review

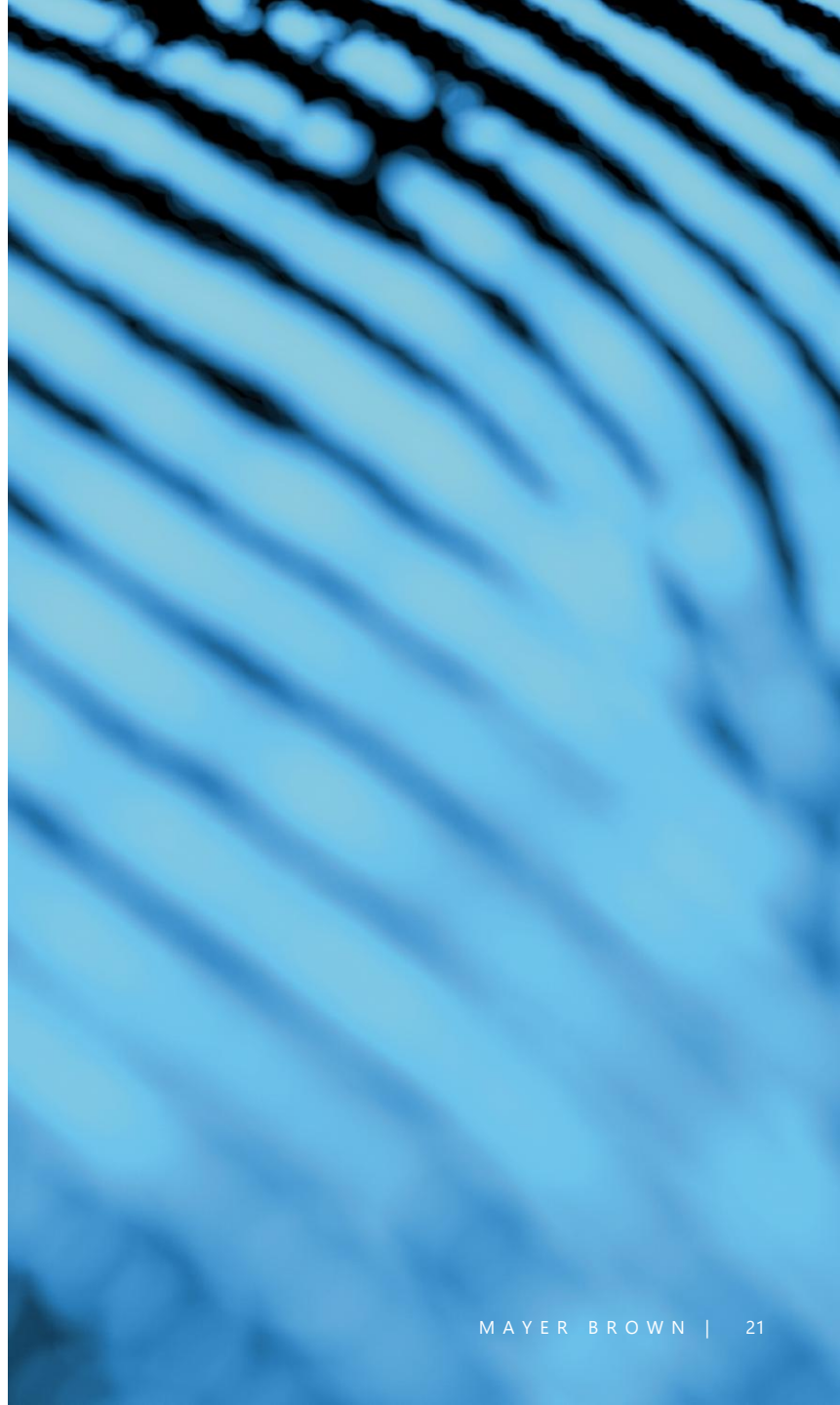
- Inspect comprehensive procedures and tools for covered-person screening including ownership thresholds ≥50%, organizational jurisdiction analysis, and designated individual identification.

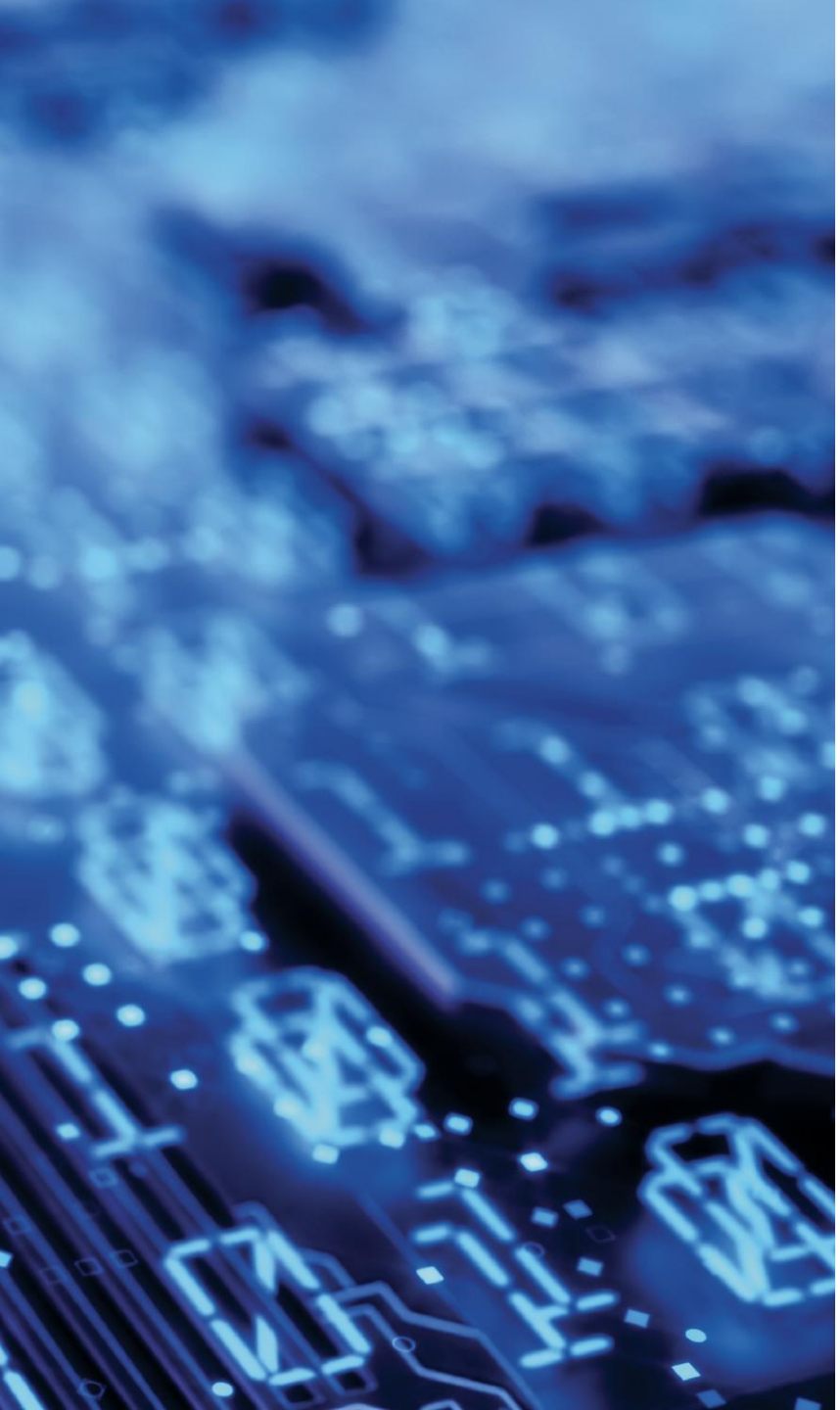
Evidence Validation

- Review screening evidence at onboarding and periodic intervals. Test sample transactions for proper match handling and complete escalation records.

Contractual Safeguards

- Confirm robust contractual protections are in place and enforceable:
  - Comprehensive representations and warranties.
  - Onward-transfer restriction clauses.
  - Termination rights for compliance violations.
  - Audit and monitoring provisions.





TEST PROCEDURES: POLICIES & CERTIFICATIONS

Policy Documentation

Verify existence, comprehensive scope, proper versioning, and clear ownership of both the data compliance program policy and security requirements implementation policy documents.

Annual Certifications

Confirm most recent annual certification by designated officer, executive, or responsible employee. Review attestations for completeness, accuracy, and appropriate scope coverage.

Practice Alignment

Assess alignment between documented policies and actual operational practices through structured interviews, process walkthroughs, and artifact examination.

04

TESTING THE SECURITY REQUIREMENTS

SECURITY REQUIREMENTS: ORGANIZATIONAL CONTROLS

Cybersecurity Governance

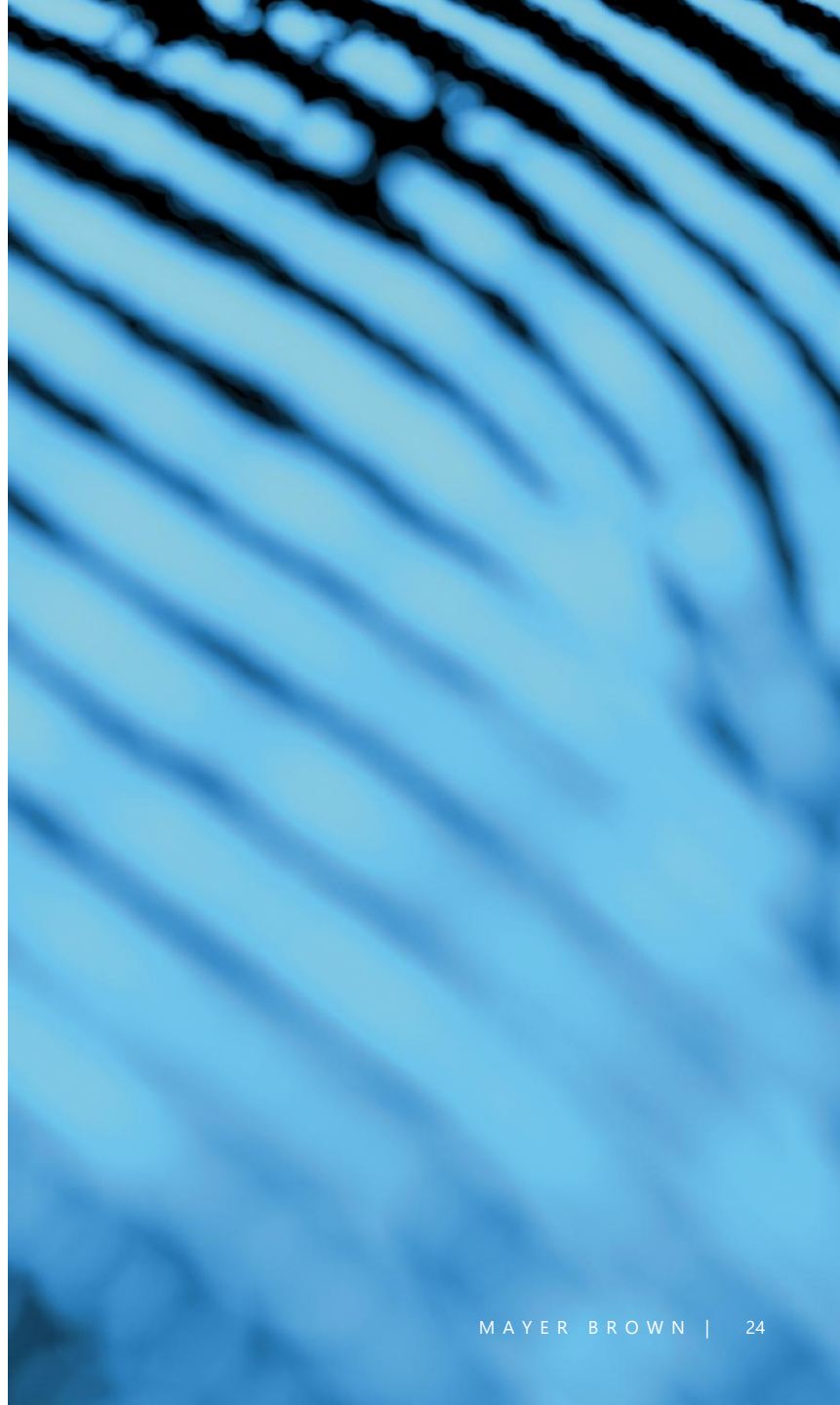
Comprehensive governance framework with clear accountability structures for cybersecurity oversight, secure asset management protocols, and standardized deployment and change management processes.

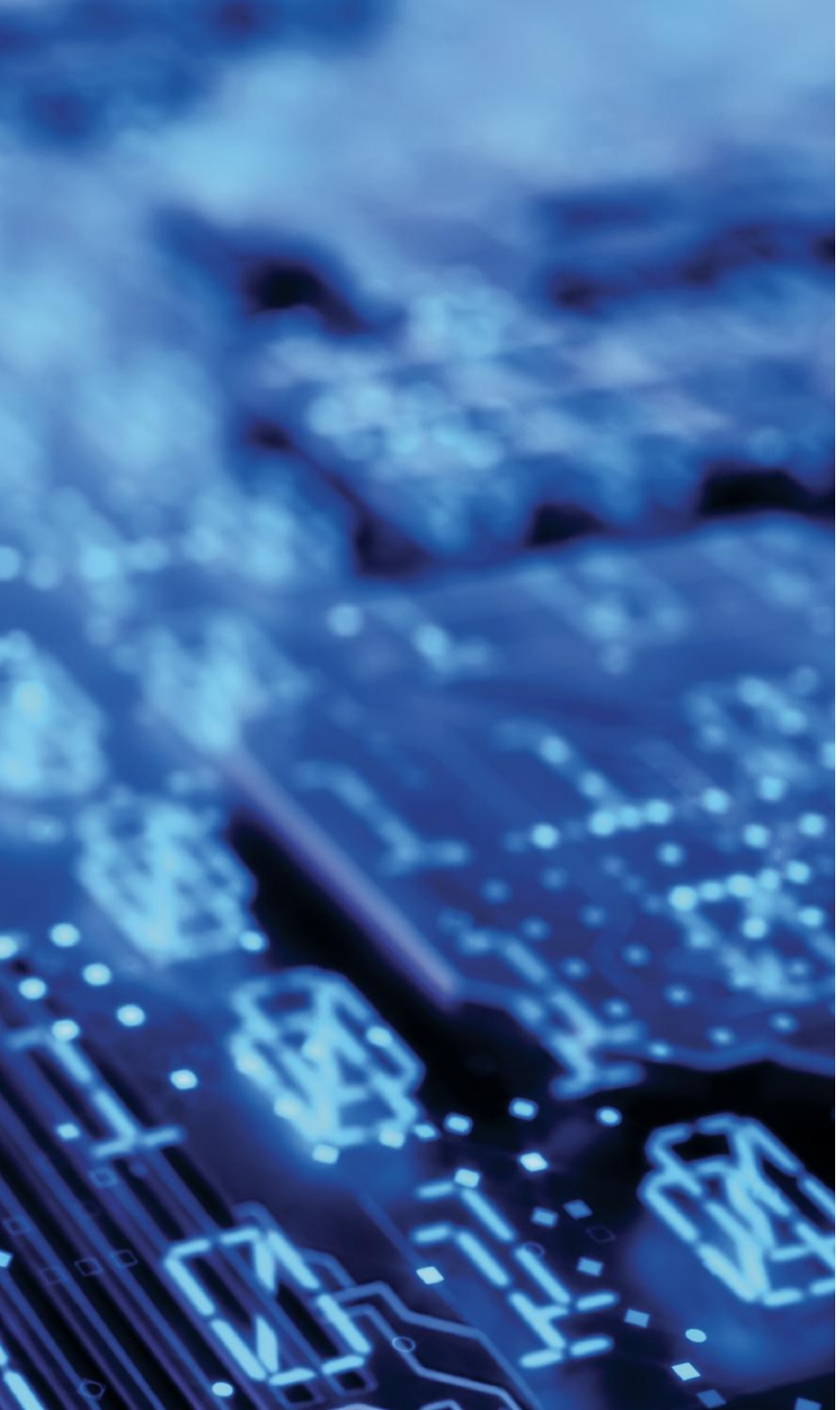
Vulnerability Management

Systematic vulnerability management program with timely remediation requirements (typically within 45 days), structured exception handling processes, and continuous monitoring capabilities.

Access Governance & Training

Comprehensive security training programs and role-based access governance frameworks tightly aligned to restricted transaction requirements and data protection obligations.





SECURITY REQUIREMENTS: SYSTEM-LEVEL CONTROLS

1

Identity & Access Management

Robust IAM implementation across all covered systems featuring multi-factor authentication (MFA that meets NIST SP 800-63B), least privilege principles, segregation of duties, and comprehensive session control mechanisms.

2

Security Monitoring & Logging

Comprehensive security logging and monitoring across authentication events, access attempts, and data movement activities with appropriate retention periods per organizational policy.

3

Network Segmentation

Technical segmentation strategies to prevent covered-person access paths including zero-trust architecture patterns where technically feasible and operationally appropriate.

SECURITY REQUIREMENTS: DATA-LEVEL CONTROLS

Data Minimization & Privacy Enhancing Technologies (PETs)

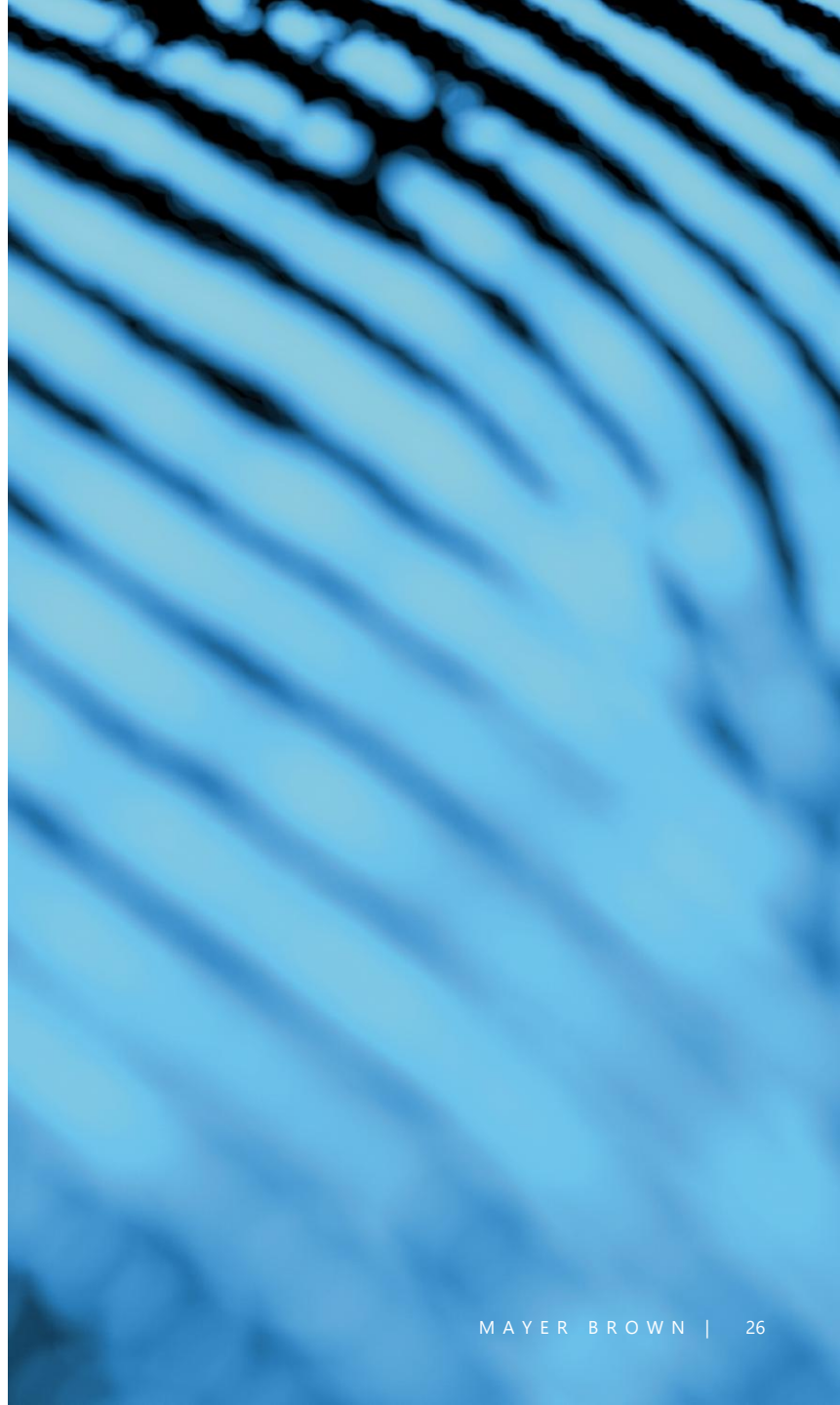
- Implementation of data minimization principles and Privacy Enhancing Technologies (PETs) to achieve effective de-identification and de-linking when access is necessary for restricted transactions.

Cryptographic Protection

- Strong cryptography for data at rest and in transit with protected key management systems. Ensure data remains unencryptable using commonly available technology.

Retention & Deletion

- Enforced retention and deletion schedules specifically for covered data with regular testing against actual datasets to ensure compliance effectiveness.



Security Risk Assessment (Data-Level)

Risk Assessment Evaluation

Evaluate documented risk assessment that justifies chosen mitigation strategies for each relevant transaction class and data category.

Likelihood Analysis

Assess comprehensive likelihood-of-disclosure and likelihood-of-harm analysis methodologies with annual review cycles and regular updates.

Mitigation Validation

Confirm that implemented mitigations, when properly combined, fully and effectively prevent all prohibited access outcomes.

SAMPLING METHODOLOGY & EVIDENCE STANDARDS

Risk-Based Sampling

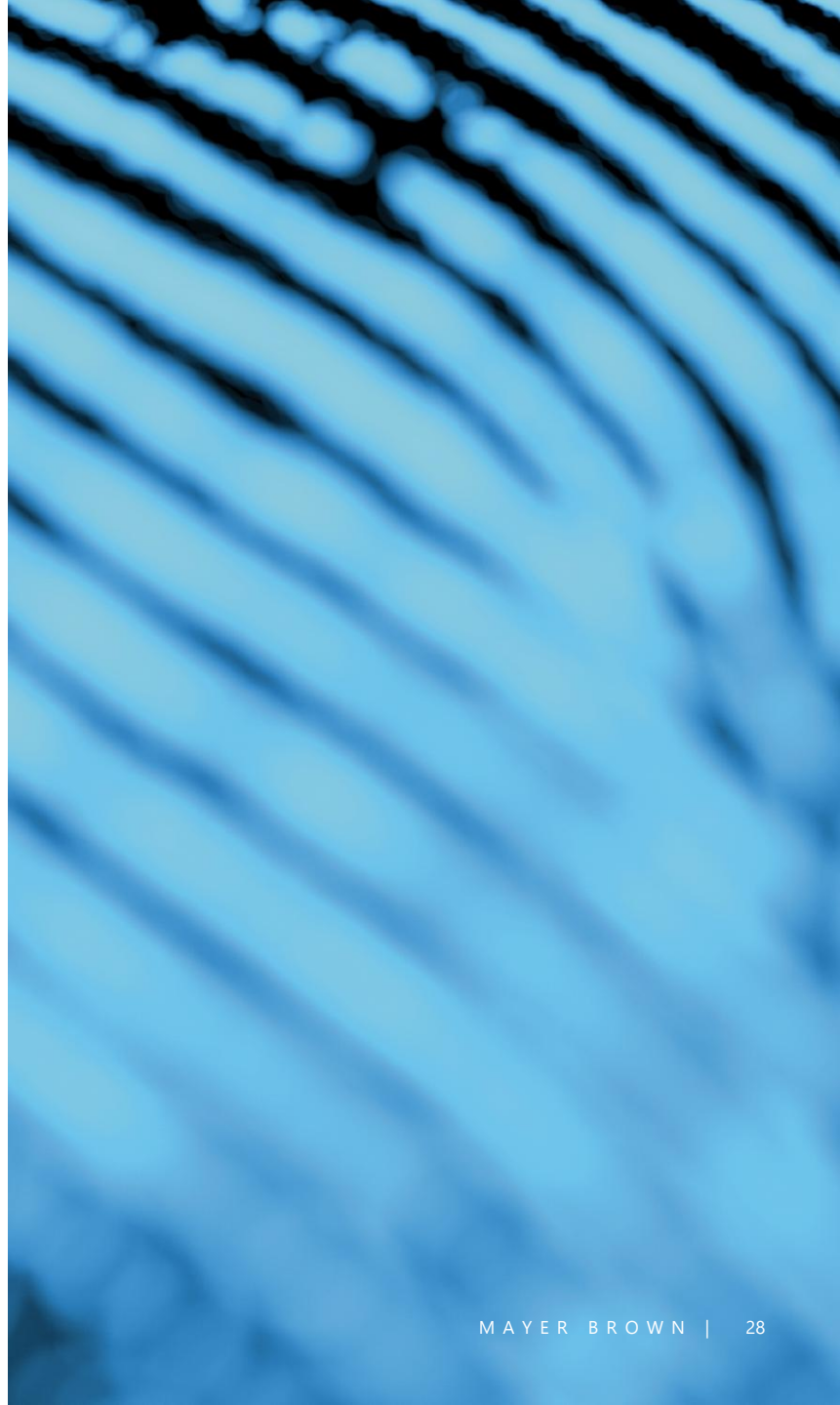
- Comprehensive risk-based sampling across each restricted-transaction pathway including vendor agreements, employment arrangements, and investment structures, plus coverage of each covered system environment.

Technical Corroboration

- All narrative assertions corroborated with technical artifacts: system configurations, security logs, key-management records, data-processing traces, and ticketing systems.

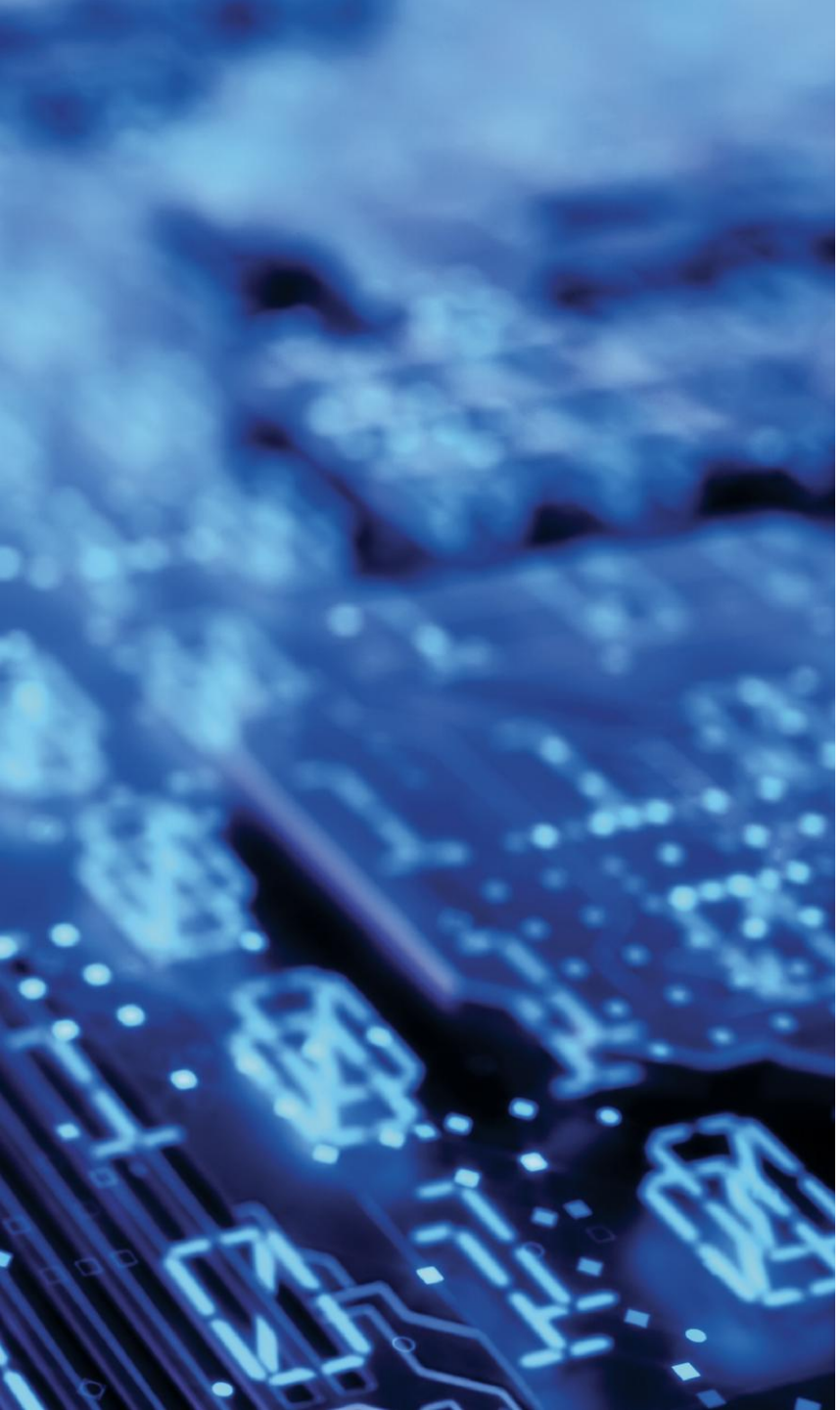
Evidence Chain of Custody

- Rigorous chain-of-custody procedures for all evidence collection and secure transmission protocols. Ensure complete reproducibility of all testing procedures for validation purposes.



05

DELIVERABLES, FINDINGS, AND REMEDIATION FRAMEWORK



DELIVERABLES, FINDINGS & REMEDIATION FRAMEWORK

Audit Deliverables

The written report—delivered within 60 days—documents the audit scope, restricted transactions examined, methods and evidence reviewed, and the overall effectiveness of the data-compliance and security programs. Includes management responses, remediation plans, and retest criteria.

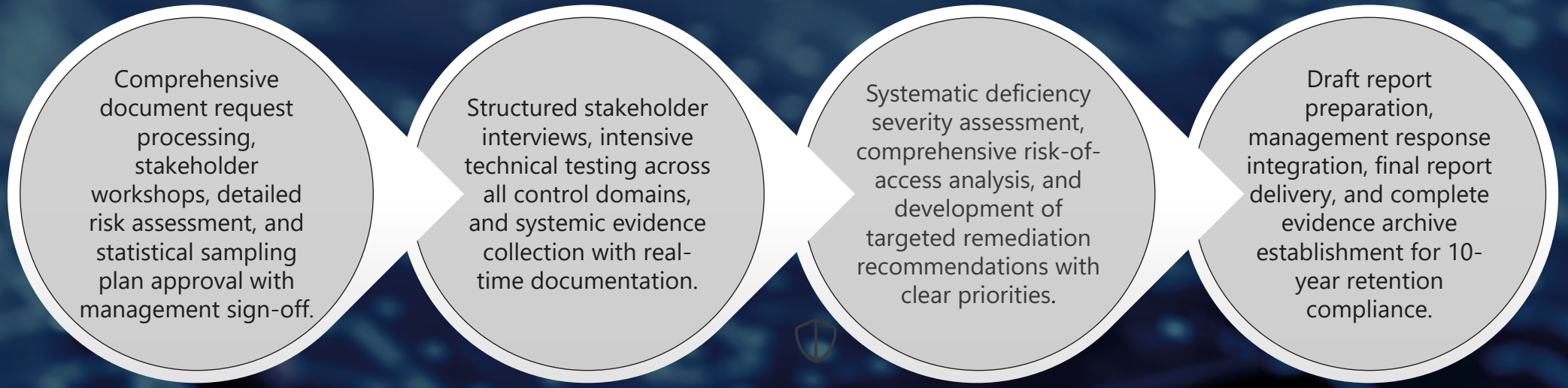
Findings & Ratings

All findings are mapped to specific DOJ Data Security Program provisions. Each issue is rated using a risk-based severity model—how likely it is that the weakness could lead to unauthorized access or disclosure of covered data to a country of concern or covered person.

Remediation & Validation

Actionable recommendations identify control fixes, owners, and due dates. Re-tests confirm closure. Documentation of remediation and follow-up becomes part of the auditable record under Subpart K.

Conceptual Project Timeline



07

Q&A

MAYER | BROWN