Performing Data Security Risk Assessments Checklist

by Practical Law Data Privacy Advisor

Checklists | **Maintained** | United States

A Checklist outlining key steps to take when planning and performing data security risk assessments. It addresses data security risk assessment requirements found in federal and state laws, industry standards, and best practices, such as the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, and the NIST Cybersecurity Framework. This Checklist is designed to be used with Practice Note, Data Security Risk Assessments and Reporting.

Identify Legal and Other Obligations

Consider whether the organization:

- Collects and uses customer or employee personal information (see Review Federal and State Guidance on Protecting Personal Information).
- Participates in an industry sector that is viewed as high risk or critical infrastructure (see Consider Sector-Specific Requirements).
- Offers securities as a publicly traded company (see Review Public Company Obligations).
- Needs to protect its own trade secrets or other internal or proprietary information (see Identify Trade Secrets or Other Internal or Proprietary Information).
- Wishes to demonstrate compliance with generally accepted industry standards for various legal and business purposes (see Review and Choose Applicable Industry Standards).
- Handles other organizations' information, subject to contract terms and conditions. If so, review contract terms to identify risk assessment requirements and standards applied (for example terms that customers commonly request, see Standard Clause, Data Security Contract Clauses for Service Provider Arrangements (Pro-Customer)).
- Accepts certain forms of payment, including credit cards, other payment cards, and direct payments from bank accounts. If so:
    - review the Payment Card Industry Data Security Standard (PCI DSS), which includes extensive program assessment requirements (see Practice Note, PCI DSS Compliance: Types of PCI DSS Validations and Assessments); and
    - review the NACHA Operating Rules, which set information security standards for processing automated clearing house network transactions.

Review Federal and State Guidance on Protecting Personal Information

- Review Federal Trade Commission (FTC) data security guidance resources and consent decrees for current standards and expectations (see Practice Note, FTC Data Security Standards and Enforcement).
- Consider whether state data security laws apply. States that have enacted data security laws to protect their residents' personal information typically require:
    - a written information security program (WISP) that includes risk assessments (see Standard Document, Written Information Security Program (WISP)); or
    - implementation of reasonable and appropriate security measures that are generally understood to include risk assessments (see Review and Choose Applicable Industry Standards).

For more details on legal obligations to protect personal information and conduct risk assessments, see Practice Notes, US Privacy and Data Security Law: Overview and Data Security Risk Assessments and Reporting: Personal Information.

Consider Sector-Specific Requirements

Consider whether the organization is:

- A financial institution subject to:
    - the Gramm-Leach-Bliley Act (GLBA) and must conduct risk assessments under the Safeguards Rule (see Practice Note, GLBA: The Financial Privacy and Safeguards Rules); and
    - state-level scrutiny (for example, see the New York State Department of Financial Services (NYDFS) Cybersecurity Regulations (23 NYCRR 500.0 to 500.23) and Practice Note, The NYDFS Cybersecurity Regulations).
- An insurance industry licensee subject to state data security obligations that mandate risk assessments (see Practice Note, NAIC Model Data Security Law and State-Specific Implementations).
- A broker-dealer or financial advisor subject to Securities and Exchange Commission (SEC) examination of their cybersecurity practices (for example, see Legal Update, SEC Publishes Cybersecurity and Resiliency Observations).
- A health care provider, health plan, or service provider subject to the Health Insurance Portability and Accountability Act (HIPAA) that must conduct a risk analysis under the Security Rule (see Practice Note, HIPAA Security Rule).
- An educational institution or service provider that must reasonably protect student information under the Family Educational Rights and Privacy Act (FERPA) and a growing body of state laws (see Practice Note, Student Privacy: Education Service Provider Requirements).

- An owner or operator of critical infrastructure subject to sector-specific regulations that requires it to perform data security risk assessments. For more details on critical infrastructure, including sector-specific examples, see Practice Note, The NIST Cybersecurity Framework.

Review Public Company Obligations

- Consider the SEC Division of Corporation Finance's 2011 guidance and February 2018 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, which expands and reinforces the 2011 guidance, on disclosure obligations related to cybersecurity risks and incidents, if the organization is a reporting company that must disclose material risks under SEC rules and regulations.

For more, see Legal Update, SEC Issues Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures.

Identify Trade Secrets or Other Internal or Proprietary Information

- Identify trade secrets or other internal or proprietary data, or categories of this data, that the organization must reasonably protect.
- Choose and apply appropriate information security industry standards to help demonstrate that the organization takes reasonable steps to preserve secrecy (see Review and Choose Applicable Industry Standards).

For more information on trade secret protection requirements under both federal and state laws, see Practice Note, Intellectual Property: Overview: Trade Secrets.

Review and Choose Applicable Industry Standards

- Review commonly used standards, including:
    - ISO/IEC 27001 and ISO/IEC 27002, which are internationally recognized information security program standards that also provide a basis for ISO certification (see ISO: ISO/IEC 27001 Information Security Management);
    - COBIT, which provides a broad set of IT audit controls that address information security issues (see ISACA: COBIT);
    - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations, which is primarily aimed at federal agencies and their contractors under the Federal Information Security Management Act of 2002 but provides extensive generally applicable guidance;
    - the Center for Internet Security's Critical Security Controls (for details, see Practice Note, Cybersecurity Tech Basics: Critical Security Controls: Overview); and

    - the NIST Cybersecurity Framework, which organizes these and other standards into a set of key functions (see Practice Note, The NIST Cybersecurity Framework).

- Choose one or more standards to apply in assessing the effectiveness and potential risks of the organization's information security program.
- Consider categorizing or mapping identified risks and results to chosen standards (see Report Assessment Results).

For more discussion, see Practice Note, Data Security Risk Assessments and Reporting: Generally Accepted Industry Standards.

Support Pre-Assessment Activities

- Identify and address legal and other obligations related to risk assessments (see Identify Legal and Other Obligations).
- Determine how to best protect any resulting sensitive risk assessment reports (see Protect Sensitive Risk Assessment Reports).
- Assist the organization's information security coordinator in:
    - identifying and engaging stakeholders who can help gather risk assessment information and manage any technical or non-technical risks identified;
    - determining appropriate channels for reporting results to the organization's leadership; and
    - seeking executive sponsorship to help prioritize assessment results.

For more discussion and examples of common stakeholders, see Practice Note, Data Security Risk Assessments and Reporting: Pre-Assessment Activities.

Define Assessment Timing, Scope, and Methods

- Determine the risk assessment's timing. For example, consider conducting:
    - a comprehensive risk assessment as frequently as required by applicable laws, regulations, and standards, but at least annually; and
    - targeted assessments when there are material changes or additions to business processes, systems, or the data that the organization collects and uses.
- Create alignment and simplify reporting by using any selected assessment timing cycle, such as conducting assessments annually, to help determine the time frame for estimating the likelihood that identified risks may be exploited (see Identify Risks and Compliance Gaps).
- Define the risk assessment's scope of review to:

  - comply with legal and other obligations (see Identify Legal and Other Obligations);
  - help avoid gaps; and
  - prevent mistaking a targeted review for an assessment of the organization's total risks.

- Select methods for conducting the assessment according to:
  - risk assessment objectives;
  - the organization's culture; and
  - available resources.

- Consider whether to employ one or more of the following risk assessment methods:
  - audits and certifications;
  - self-assessments;
  - penetration tests;
  - vulnerability scans;
  - assets scans; and
  - continuous monitoring.

- Document the timing, scope, and methods selected for any particular risk assessment with the assessment's results (see Report Assessment Results).

For more details on defining timing, scope, and methods for data security risk assessments, see Practice Note, Data Security Risk Assessments and Reporting: Define Timing, Scope, and Methods and Box, Common Forms of Data Security Risk Assessments.

Gather Information to Support Risk Identification

- Work with stakeholders to gather information based on the assessment's scope and selected methods. For example, assessment teams may need to:
  - collect documented policies, procedures, event logs, or other historical files;
  - interview key individuals;
  - gather current technical configurations and other system details;
  - document safeguards testing results; and
  - run automated scans.

- For service provider assessments:

    - distribute questionnaires or other self-assessment tools;
    - collect independent audit or certification results; and
    - gather incident reports provided as part of the relationship.

- For workforce risk and compliance reviews:
    - collect training records;
    - review reports produced by compliance management activities; and
    - test individuals on their current security awareness and compliance.

- In all cases, gather information to understand:
    - the organization's systems and data that fall within the assessment's scope;
    - the individuals or groups who may have access to systems and data, including the extent of their access and data use capabilities; and
    - the applicable network architecture, including integration points and communications paths.

For more guidance on gathering information to support data security risk assessments, see Practice Note, Data Security Risk Assessments and Reporting: Gather Information.

Identify Risks and Compliance Gaps

- Define and prioritize risks by identifying and combining the following key elements:
    - threats, which are generally considered to be any circumstance or event that can adversely impact an organization's IT assets or data;
    - vulnerabilities, which are weaknesses or other conditions within an organization that may be exploited by a threat to adversely affect data security;
    - the likelihood that a particular threat may occur or that a threat actor may exploit one or more vulnerabilities within a certain time frame, or the frequency of events that are almost certain to occur; and
    - the potential impact of a particular event.

    For detailed guidance on defining risks and their key elements, see Practice Note, Data Security Risk Assessments and Reporting: Key Concepts for Assessing Data Security Risks).

- Consider common areas of risk, including:
    - delays in removing access for terminated employees;

    - unsecured work areas;
    - failure to install current operating system or other software patches;
    - use of unencrypted laptops or other mobile devices to store personal information;
    - failure to limit access to customer information to employees with a need-to-know; and
    - default server configurations that include unnecessary services and vendor-supplied passwords.

- Provide a more comprehensive risk assessment by:
    - comparing the organization's performance to applicable laws, regulations, or generally accepted industry standards (see Review and Choose Applicable Industry Standards);
    - considering service provider and supply chain issues (see Practice Note, Data Security Risk Assessments and Reporting: Box, Service Provider and Supply Chain Risk Assessment); and
    - reviewing workforce awareness and compliance (see Practice Note, Data Security Risk Assessments and Reporting: Box, Workforce Risk Assessment).

- Document identified risks and compliance gaps for reporting and ongoing risk management purposes.

Report Assessment Results

- Before creating reports, determine how to best protect sensitive risk assessment results (see Protect Sensitive Risk Assessment Reports).
- Ensure that risk assessment reports:
    - focus on findings;
    - are factual; and
    - do not speculate or draw conclusions, especially regarding legal risk or regulatory compliance that others may later misinterpret or take out of context.

- Document the particular assessment's timing, scope, and methods used to provide context and avoid misinterpretation (see Define Assessment Timing, Scope, and Methods First).
- Categorize risks and compliance gaps to help simplify reporting and program management, for example, based on:
    - the group responsible for addressing the identified risk or compliance gap;
    - pertinent laws, regulations, standards, or other obligations;

  - costs to remediate;
  - time to remediate; or
  - the type of issue identified.

- Prioritize identified risks by analyzing likelihood and impact together, as shown in the table below, while considering the organization's unique circumstances and risk profile.

	Impact		
Likelihood	**High**	**Medium**	**Low**
High	High (Red)	High (Red)	Medium (Yellow)
Medium	High (Red)	Medium (Yellow)	Low (Green)
Low	Medium (Yellow)	Low (Green)	Low (Green)

For more details on reporting and prioritizing risks, see Practice Note, Data Security Risk Assessments and Reporting: Report Results, Prioritizing Risks, and Box, Communicating Risks.

Take Action to Manage Identified Risks and Compliance Gaps

- Timely respond to risk assessment reports by:
  - assigning clear ownership and accountability to reasonably address each identified risk; and
  - maintaining program management documents showing that the organization understands the identified risks, if any, and is responding appropriately.

- For each identified risk or compliance gap, consider:
  - the organization's risk tolerance level;
  - any applicable legal obligations and the potential costs of litigation or enforcement;
  - feasibility of remediation;
  - the costs and time frame required to remediate; and
  - the organization's culture.

- Choose an appropriate action to respond to each identified risk or compliance gap, for example:
  - accept the risk or gap;
  - mitigate but do not resolve the risk; or
  - remediate (resolve) the risk.

- Document each choice and track its implementation to completion, if applicable.
- When choosing to accept or mitigate rather than remediate a particular risk:

- record any analysis or rationale; and
- set a time frame for follow up review, if circumstances change.

For more guidance on managing risks and compliance, see Practice Note, Data Security Risk Assessments and Reporting: Manage Risks and Compliance.

Protect Sensitive Risk Assessment Reports

Protect risk assessment reports and supporting documents by:

- Applying attorney-client privilege or the work product doctrine or both, if applicable.
- Assigning the organization's most protective information classification level.
- Using extensive administrative, physical, and technical safeguards.
- Educating risk assessment participants on the need to protect reports.

For more details on the sensitive information typically included in risk assessment reports and protection methods, see Practice Note, Data Security Risk Assessments and Reporting: Protecting Risk Assessment Reports.

Recognize and Address Risk Assessment Limitations

- Treat risk assessment as a cyclical process rather than a one-time event.
- Include different individuals with a variety of backgrounds, skills, and perspectives on assessment teams.
- Use multiple tools for automated reviews where feasible.
- Implement continuous monitoring to detect and help address data security risks in near real-time (see Practice Note, Data Security Risk Assessments and Reporting: Box, Common Forms of Data Security Risk Assessments).
- Engage one or more independent third-party auditors or assessors.

For more discussion on risk assessment limitations, see Practice Note, Data Security Risk Assessments and Reporting: Risk Assessment Limitations.

Explore the Benefits of Cybersecurity Information Sharing

- Consider whether the organization is willing and able to share information.
- Identify and join one or more appropriate cybersecurity information security communities.
- Define processes to avoid disclosing sensitive information to information sharing communities, for example:

- the organization's status or specific risk assessment results; or
- personal information, unless necessary to describe a cyber threat.

- Routinely incorporate information received from information sharing communities into the organization's risk assessment and risk management processes.

For more details on cybersecurity information sharing programs, including supporting laws and additional resources, see Practice Note, Data Security Risk Assessments and Reporting: Box, Cybersecurity Information Sharing Programs.

END OF DOCUMENT

RESOURCE HISTORY

SEC Announces New Cybersecurity Disclosure Guidance.

We have updated the Review Public Company Obligations section to reflect the updated cybersecurity disclosure guidance that the Securities and Exchange Commission (SEC) published on February 21, 2018.

Related Content

Topics

Privacy

Practice note: overview

State Data Security Laws: Overview • Maintained
US Privacy and Data Security Law: Overview • Maintained

Practice notes

Managing Privacy and Data Security Risks in Vendor Relationships • Maintained
Cyberattacks: Prevention and Proactive Responses • Maintained
Developing Information Security Policies • Maintained
FTC Data Security Standards and Enforcement • Maintained
The NIST Cybersecurity Framework • Maintained
Data Security Risk Assessments and Reporting • Maintained

Standard documents

Information Security Policy • Maintained
Written Information Security Program (WISP) • Maintained

Checklists

Common Gaps in Information Security Compliance Checklist • Maintained

Toolkit

Information Security Toolkit • Maintained
Data Breach Toolkit • Maintained
Cybersecurity Tech Basics Toolkit • Maintained

