THOMSON REUTERS
PRACTICAL LAW™

Data Security Risk Assessments and Reporting

by Practical Law Data Privacy Advisor

Status: **Maintained** | Jurisdiction: **USA (National/Federal)**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-002-2323**
Request a free trial and demonstration at: **https://legal.thomsonreuters.com/en/products/practical-law#free-trial**
This resource was downloaded July 29, 2021. Please view current online version for any changes since then.

A Practice Note explaining how to plan, perform, and report on data security risk assessments as required by federal and state laws, including the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), industry standards, and best practices. It also addresses common forms of cyber risk assessments and their role in any organization's overall information security program.

Risk assessments play a crucial role in maintaining information security.

Information security programs protect the confidentiality, integrity, and availability of data and information technology (IT) assets. However, technology and the cybersecurity threat climate constantly change. Effective information security programs:

- Recognize the dynamic nature of data security risks.
- Treat risk assessment as a cyclical process.

Current laws that call for performing data security risk assessments typically are not prescriptive. For example, many federal and state laws require organizations to identify reasonably foreseeable internal and external risks that affect data security. Within those broad standards, organizations may choose their risk assessment methods. This note explains key concepts and the core process steps organizations generally follow when conducting data security risk assessments.

Specifically, it:

- Describes the legal issues to consider when planning and performing assessments.
- Explains the key concepts necessary for recognizing, defining, and managing data security risks.
- Defines the risk assessment process.
- Reviews issues and methods related to protecting risk assessment reports.
- Cautions counsel regarding risk assessment limitations.

Risk Assessments and Counsel's Role

Risk assessments are inherently operational, but counsel plays an important role in this vital information security activity. Data security laws, regulations, and typical contract obligations often use a reasonableness standard. Organizations look to counsel for advice on what is reasonable practice. To provide effective advice, counsel must understand common data security risk assessment terminology, processes, and standards.

Information security practitioners and data security laws and regulations often use the term "risk assessment" to refer to different activities. Risk assessments typically focus on:

- Identifying reasonably foreseeable internal and external risks to data security.
- **Reviewing an organization's current information security program for:**
  - Compliance against a specified set of standards
  - General effectiveness
  - Both

Organizations may consider these two perspectives separately or together. However, to maintain a sound information security program, organizations need to regularly review:

- Their own unique risk profiles.
- Their performance against applicable standards of practice.

- Risks that their third-party service providers or vendors create.
- Information security awareness and compliance across their workforce members, including employees, contractors, volunteers, and any others who access or use their data and IT assets.

Common risk assessment methods vary in scope, technical detail, and resource requirements. Some organizations choose to periodically engage one or more independent third-party auditors or assessors, regardless of whether they must do so by law or other obligations. For more details on different types of risk assessments, see Box, Common Forms of Data Security Risk Assessments.

Based on legal obligations and best practices, some organizations document their information security activities in a written information security program (WISP), including their commitment to conduct periodic risk assessments. For more details on developing, implementing, and maintaining a WISP, see Standard Document, Written Information Security Program (WISP).

Organizations should also address risk management activities, including risk assessment, in their information security policies. For guidance on developing workforce-facing information security policies and a sample policy, see Practice Note, Developing Information Security Policies and Standard Document, Information Security Policy.

Legal Considerations

Various data security laws, regulations, and industry standards state or at least imply an obligation to perform risk assessments. For example, laws and regulations often call for reasonable and appropriate data security measures. Reasonable data security measures are generally understood to include performing risk assessments, at least in part, because organizations cannot determine appropriate measures unless they assess risks. Common scenarios that drive organizations to support risk assessments include:

- Collecting and using **personal information** for customers and employees (see Personal Information).
- Participating in a high risk or critical infrastructure industry sector (see Sector-Specific Requirements).
- Offering securities as a publicly traded company (see Public Company Obligations).
- Protecting their own trade secrets and other internal or proprietary information (see Trade Secrets and Other Internal or Proprietary Information).
- Handling other organizations' information, subject to contract terms and conditions (see Contract Obligations).
- Accepting certain forms of payment, including credit cards, other payment cards, and direct payments from bank accounts (see Payment Processing Standards).
- Demonstrating compliance with generally accepted industry standards for various legal and business purposes (see Generally Accepted Industry Standards).

Personal Information

Almost every organization collects, uses, and maintains personal information. While a comprehensive review of privacy and data security laws is beyond this note's scope, certain federal and state laws require data security risk assessments. For more details on U.S. laws protecting personal information, see Practice Note, U.S. Privacy and Data Security Law: Overview.

For example, under its authority to address unfair or deceptive trade practices, the Federal Trade Commission (FTC) takes enforcement action against businesses that fail to:

- Keep their data security commitments, including promises to follow industry standards.
- Implement reasonable safeguards.

The FTC's data security guidance resources call for risk assessment (see Box, Additional Resources). FTC data security investigations often result in consent decrees that mandate regular security assessments, including independent third-party program reviews (see Practice Note, FTC Data Security Standards and Enforcement: Consent Decrees and Settlements).

Some states require organizations that maintain their residents' personal information to implement a WISP that calls for performing periodic risk assessments. Other states require that organizations implement reasonable and appropriate measures to protect personal information. For more examples and information on state-level data security laws, see Practice Note, State Data Security Laws: Overview. For a model WISP, see Standard Document, Written Information Security Program (WISP).

Organizations that handle personal information that originates outside the U.S. may have additional data security obligations, for example, under EU laws. For more details, see GDPR Resources for U.S. Practitioners Toolkit.

Sector-Specific Requirements

Sector-specific data security laws and regulations require organizations to protect certain systems and data types, especially sensitive or high-risk assets. **These mandates often explicitly address risk assessments. Examples include:**

- Financial institutions subject to the **Gramm-Leach-Bliley Act** (GLBA) must conduct risk assessments under the Safeguards Rule (see Practice Note, GLBA: The Financial Privacy and Safeguards Rules).
- Broker-dealers and financial advisors are subject to **Securities and Exchange Commission** (SEC) examination of their cybersecurity practices.
- The financial services sector is increasingly subject to state-level scrutiny. For example, the New York Department of Financial Services (NYDFS) has promulgated extensive cybersecurity regulations (for details, see Practice Note, The NYDFS Cybersecurity Regulations and Complying with the NYDFS Cybersecurity Regulations Checklist).
- Health care providers, health plans, and their service providers subject to the **Health Insurance Portability and Accountability Act** (HIPAA) must conduct a risk analysis under the Security Rule (see Practice Note, HIPAA Security Rule).
- Educational institutions and their service providers 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).
- Insurers in a growing set of states are subject to laws modelled on the National Association of Insurance Commissioners (NAIC) Model Data Security Law (see Practice Note, NAIC Model Data Security Law and State-Specific Implementations).
- Organizations that own or operate critical infrastructure may be subject to sector-specific regulations that require them to perform data security risk assessments. Some sector-specific agencies regulate cybersecurity practices, while others depend on voluntary activities and industry self-regulation. For more details on the critical infrastructure sectors and the federal response to increasing information security risks, see Practice Note, The NIST Cybersecurity Framework: Cybersecurity Risk and Federal Government Response.

Public Company Obligations

Current SEC rules and regulations do not explicitly address data security and risk assessments. However, existing rules require **reporting companies** to disclose material risks. **Unless they perform regular data security risk assessments, companies may:**

- Fail to identify material risks.
- Subject themselves to enforcement activities, especially if a data breach or other cybersecurity incident occurs.
- In late 2011, the SEC Division of Corporation Finance issued guidance on cybersecurity risk and incident disclosure obligations. In February 2018, the SEC released a Commission Statement and Guidance on Public Company Cybersecurity Disclosures (83 Fed. Reg. 8166-01 (Feb. 26, 2018)), which expands and reinforces the 2011 guidance.

Trade Secrets and Other Internal or Proprietary Information

Companies often consider their internal information to be proprietary confidential information or trade secrets. The **Defend Trade Secrets Act of 2016** (DTSA) creates a federal civil remedy for trade secret misappropriation that supplements but does not preempt state law. For more details on the DTSA and state trade secrets protection, see Practice Note, Intellectual Property: Overview: Trade Secrets.

Organizations must generally make reasonable efforts to preserve secrecy to receive trade secret protection under existing law (see Generally Accepted Industry Standards).

Contract Obligations

Organizations that handle other companies' information or access their IT systems may be subject to contract terms requiring them to:

- Perform regular risk assessments, including audits and certifications.
- Comply with specific data security regulations or industry standards.

Just as they assess their service providers and vendors, organizations should expect their customers to seek assurances that they have identified and are reasonably managing data security risks (see Box, Service Provider and Supply Chain Risk Assessment).

Payment Processing Standards

Businesses that process payments made using credit cards, other payment cards, and direct payments from bank accounts are typically subject to data security standards, often through transaction servicing agreements, including:

- 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).
- The NACHA Operating Rules, which set information security standards for processing automated clearing house network transactions.

Generally Accepted Industry Standards

Organizations often seek to demonstrate their compliance with generally accepted industry standards of information security practice to:

- Support insurance application and underwriting processes (see Practice Note, Cyber Insurance: Insuring for Data Breach Risk: Applying for Cyber Coverage).
- Minimize legal risk if a data breach or other cyber incident occurs that results in litigation or regulatory enforcement action.
- Provide information for due diligence purposes.
- Bolster their negotiating position with potential customers, business partners, investors, or others.

Program reviews against widely recognized information security standards support these efforts, including audits, certifications, and less formal assessments (see Box, Common Forms of Data Security Risk Assessments).

Some common standards include:

- ISO/IEC 27001 and ISO/IEC 27002, which are internationally recognized information security program standards that also provide a basis for ISO certification.
- COBIT 5, which provides a broad set of IT audit controls that address information security issues.
- 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 (see Practice Note, Cybersecurity Tech Basics: Critical Security Controls: Overview).
- NIST's Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework), which organizes these and other standards into a set of key functions (see Practice Note, The NIST Cybersecurity Framework).

Key Concepts for Assessing Data Security Risks

Current laws and regulations that mandate data security risk assessments generally do not directly define risks or prescribe specific methods for identifying them. Industry standards offer further guidance and provide examples. For instance, the NIST Cybersecurity Framework lists activities associated with risk assessments and others related to an organization's risk management strategy (see Generally Accepted Industry Standards and Box, Additional Resources).

Organizations ultimately must define, identify, and manage their own data security risks. Counsel must understand key concepts and risk assessment methods to advise clients on what is reasonable practice.

Data security risks are defined and prioritized by combining several elements, including:

- Threats to an organization's IT environment or data, whether internal or external, human or otherwise (see Threats).
- Vulnerabilities or weaknesses that exist in the organization's environment (see Vulnerabilities).
- The likelihood or probability that a particular threat or threat actor will exploit one or more vulnerabilities (see Likelihood).
- The impact or harm likely to result from a particular event (see Impact).

Identifying data security risks requires organizations to consider each of these elements and apply them to their environments. For example, a particular event may occur when a threat exploits one or more vulnerabilities, such as an external hacker who takes advantage of an organization's outdated software to obtain unauthorized access to sensitive data. That potential event identifies a risk that the organization can further characterize by its likelihood and impact.

Different organizations are often subject to similar data security risks and so may benefit from sharing information (see Box, Cybersecurity Information Sharing Programs).

However, each organization's total risk profile is unique because:

- IT environments and the data organizations store differ.
- The number and character of vulnerabilities varies, according to an organization's policies and how diligently it configures and maintains its IT assets.
- Some organizations are more likely to be cyberattack targets because of their sector, business role, or data's value. Organizations should nonetheless avoid downplaying their likelihood of being targeted. Hackers increasingly attack small businesses or others they perceive as easy targets, and rogue or disgruntled employees may exist anywhere. Nation-state and other sophisticated cyberattackers often seek out weaker entry points to their ultimate targets, such as service providers, contractors, software or hardware suppliers, or other supply chain members.
- The potential impact of particular risks varies based on an organization's preparedness and ability to contain events.
- Organizations should view risk assessment as an ongoing process and expect their risks to change as threats change and their programs evolve (see Risk Assessment Process).

Threats

A threat is generally any circumstance or event that can adversely impact an organization's IT assets or data. For example, the Cybersecurity Information Sharing Act of 2015 (CISA) broadly defines cybersecurity threats as any actions that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of systems or data (6 U.S.C. § 1501(5)).

Threats are often characterized as attacks or attack types and may also be defined from several perspectives, including:

- **Sources or threat actors, such as:**
  - Negligent or malicious employees who create internal threats
  - Nation-state actors or hackers or other criminals who create external threats
- **Events or scenarios, such as:**
  - Data loss or theft, including data exfiltration
  - Errors or omissions
  - Malicious software (**malware**) infections
  - Hacking, including computer or network intrusions
  - Unauthorized access to data
  - Physical equipment loss or theft
  - Credential theft
  - Social engineering, for example, email-based attacks like phishing
  - A combination of sources and events.
  - **To identify threats, organizations should:**
  - Consider previous events they or similarly situated organizations have experienced.
  - Consult reliable information sharing sources.
  - Monitor current cyberattack trends.
  - Start simply with basic threat scenarios and build sophistication.

Organizations should also consider natural disasters or human-caused events that may threaten information confidentiality, integrity, or availability, such as fires, floods, other major weather events, terrorist attacks, and power outages. Because these environmental threats have potentially far-reaching effects, organizations may choose to address them separately in a formal disaster preparedness or business continuity and disaster recovery planning process. See Box, Additional Resources for more guidance and examples.

Vulnerabilities

Vulnerabilities are weaknesses or other conditions within an organization that threat actors exploit to adversely affect data security. CISA broadly defines security vulnerabilities as any attribute of hardware, software, process, or procedure that could enable or help defeat a security control (6 U.S.C. § 1501(17)).

Unlike threats, organizations can often directly control their vulnerabilities and therefore minimize risks.

Organizations typically find vulnerabilities in their:

- **People.** Due to a lack of training or awareness, individuals may be prone to mistakes or unaware of steps they should or should not take to protect data. Granting individuals access to more information or capabilities than they need to complete their assigned duties also creates unnecessary vulnerabilities.
- **IT assets.** Allowing individuals to introduce unauthorized IT assets into the organization's environment creates vulnerabilities, because the

organization cannot protect hardware and software that it does not know exists. **An organization's hardware, software, and network components may also be subject to:**

  - Inadvertent manufacturing or development defects
  - Intentionally placed backdoors
  - Insecure configurations or unnecessarily enabled services

- For more information on managing cyber vulnerabilities, see Practice Note, Cybersecurity Tech Basics: Vulnerability Management: Overview.
- **Policies.** An organization's information security policies or lack of policies may create vulnerabilities. For example, many organizations allow workforce members to use their own mobile devices. These Bring Your Own Device to Work (BYOD) policies may benefit the organization and individuals. However, connecting personal devices to the organization's systems creates vulnerabilities, unless the organization limits them with appropriate security controls. For details on developing policies, see Practice Note, Developing Information Security Policies.
- **Processes and procedures.** Gaps in business processes and procedures may create security vulnerabilities. For instance, human resources processes should deactivate systems access immediately when organizations terminate employees. Lapses in IT maintenance procedures, such as failing to apply vendor-supplied patches, and other information security gaps also create vulnerabilities (for more examples, see Common Gaps in Information Security Compliance Checklist).
- **Facilities.** Physical security gaps may create data security vulnerabilities. **For example, organizations should:**
  - House servers and other IT assets in secure locations
  - Develop, implement, and maintain backup and redundancy plans according to data sensitivity and business needs

To identify vulnerabilities, organizations should:

- Maintain a current IT asset inventory, including the hardware and software versions they use.
- Regularly review configurations.
- Establish strong vendor relationships to ensure they receive immediate notice of any newly identified flaws and defensive measures (see Box, Service Provider and Supply Chain Risk Assessment).
- Consult reliable information sharing sources. For example, the **Department of Homeland Security** (DHS) Cybersecurity and Infrastructure Security Agency (CISA) provides notice of newly identified technical vulnerabilities using standardized naming and severity level scoring through its National Cyber Awareness System.
- Routinely review their policies, processes, and procedures, especially when making material changes to business processes or IT systems.
- Consider previous assessment results.
- Conduct post-incident reviews if a data breach or other information security incident occurs (for more guidance on preparing for and managing cyber incidents, see Practice Note, Breach Notification and Standard Document, Cyber Incident Response Plan (IRP)).
- Consider implementing continuous monitoring to identify vulnerabilities on an ongoing basis (see Box, Common Forms of Data Security Risk Assessments).
- Regularly collect and analyze service provider questionnaires or other assessment or certification results (see Box, Service Provider and Supply Chain Risk Assessment).
- Consider using testing or other active workforce assessment techniques (see Box, Workforce Risk Assessment).

See Box, Additional Resources for more guidance and examples.

Likelihood

A data security risk's likelihood estimates the probability that a given threat will both:

- Exploit a particular vulnerability or set of vulnerabilities.
- Result in an event that adversely affects data security.

Organizations should consider likelihood based on:

- A particular time frame, such as within the next quarter, the next year, or another set interval.
- The likely frequency if an event is almost certain to occur within the chosen time frame.
- A combination of set time frame and frequency.

Depending on the organization's preferences and experience in conducting risk assessments, it may determine likelihood:

- Qualitatively, using categories such as high, medium, and low, or more refined distinctions.
- Quantitatively, using a scoring scale such as one to

ten or 1 to 100, resulting in an estimated percentage likelihood.

When determining likelihood, organizations should also consider their exposure to a particular risk. Despite a vulnerability, if the organization lessens its exposure by applying security controls, then the likelihood of the risk is lower. For example:

- Employees are almost certain to lose laptops that contain confidential information. If the organization applies and maintains access controls and encryption, then the likelihood of data loss is low.
- Hackers are highly likely to exploit serious software flaws that occur on internet-facing web servers. **Organizations can decrease their exposure and lessen the likelihood of damaging attacks by:**
  - Timely applying any available software patches
  - Using alternative configurations
  - Increasing monitoring

Impact

A risk's impact type and level characterize the likely consequences if a threat successfully exploits one or more vulnerabilities. **NIST provides five examples of potential impact types, including harm to:**

- An organization's operations.
- An organization's assets.
- Individuals, who might include customers, employees, or others.
- Other organizations, such as business partners, clients, or customers.
- The community or nation, for example, if the organization is a government agency or provides critical infrastructure or services.

(See NIST SP 800-30, Guide for Conducting Risk Assessments, Appendix H, Table H-2.)

To determine impact level, organizations should consider a risk's seriousness. Organizations may characterize a risk's potential impact qualitatively or quantitatively, similar to likelihood.

For simplicity, organizations often combine the impact type and level analyses to categorize risks simply as high, medium, or low impact.

Implementing security controls may also diminish a risk's potential impact. For example, network and data segmentation help isolate assets so that successful attacks are less likely to cause widespread harm to the organization.

Risk Assessment Process

Data security risk assessment is a cyclical process and not a one-time event. **Organizations should expect their risk profiles to change as:**

- Their business processes and the technologies they use change.
- Threats and attack trends evolve.
- They address identified risks and eliminate known vulnerabilities.
- They build experience in conducting assessments and identify more risks.

Each iteration of the risk assessment cycle includes five basic steps to:

- Determine the assessment's timing, scope, and methods.
- Gather pertinent information.
- Identify risks and assess program compliance and effectiveness.
- Report results.
- Manage risks and compliance.

An organization may have multiple risk assessments underway at any given time based on scope and assessment type (see Box, Common Forms of Data Security Risk Assessments).

An organization's information security coordinator or other individual designated as responsible for information security typically owns and manages the risk assessment process. For more details on assigning information security accountability, see Standard Document, Written Information Security Program (WISP): Drafting Note: Information Security Coordinator.

Pre-Assessment Activities

Before an organization conducts any data security risk assessments, counsel should assist information security coordinators with:

- Identifying and addressing any legal obligations (see Legal Considerations).

- Determining how to best protect sensitive risk assessment reports (see Protecting Risk Assessment Reports).

Other pre-assessment activities, typically completed by the information security coordinator or risk assessment team, include:

- Identifying and engaging stakeholders who can help gather information and manage any technical or non-technical risks identified. While each organization is unique, common stakeholders include:
  - Business unit and program groups
  - IT
  - Legal
  - Ethics and compliance
  - Human resources
  - Privacy
  - Procurement, especially vendor or service provider relationship management
  - Physical security
  - Disaster preparedness or business continuity and disaster recovery
- Determining appropriate channels for reporting results to the organization's leadership.
- Seeking executive sponsorship to help prioritize results.

Define Timing, Scope, and Methods

Objectives for risk assessments vary (for more details on objectives and drivers, see Risk Assessments and Counsel's Role and Legal Considerations). However, as the first step in any assessment, counsel should help risk assessment teams define their timing, scope, and methods. Organizations should always document their selected timing, scope, and methods with the assessment's results to provide context and avoid misinterpretation (see Report Results).

Determine Timing

Organizations should conduct:

- A comprehensive risk assessment as required by applicable laws, regulations, and standards, but at least annually.
- Targeted assessments when there are material changes or additions to business processes, systems, or the data that the organization collects and uses.

An assessment's timing helps to determine the time frame used in defining likelihood (see Likelihood). For example, if an organization conducts a comprehensive risk assessment annually, then similarly defining the time frame for estimating risk likelihood as one year creates alignment and simplifies reporting.

Define Scope

Organizations must carefully define and communicate any risk assessment's scope. Comprehensive risk assessments are time-consuming and resource-intensive. Organizations often choose to perform targeted assessments, for example, focusing on:

- Compliance with specific federal and state laws and regulations, such as those that regulate personal information or other activities (see Legal Considerations).
- Internet-facing systems.
- High-value data.
- New products, services, or programs.
- Systems or groups that have recently experienced a cyber incident.

Organizations may derive significant benefits from these activities. However, data security risks may still exist in other areas, and connections between systems may create additional risks. **Carefully considering and defining the scope of each risk assessment:**

- Helps avoid gaps.
- Prevents mistaking a piecemeal view for the organization's total risk profile.

Multiple assessments, if thoughtfully planned and coordinated, can provide comprehensive risk assessment coverage despite limited resources.

To avoid duplication, counsel and risk assessment teams should also consider other related activities that the organization may support, including:

- Enterprise risk management.
- Records management reviews.
- Privacy impact assessments (for more information on the privacy impact assessment process, see Practice Note, Conducting Privacy Impact Assessments).
- Disaster preparedness or business continuity and disaster recovery planning.

Select Methods

Current laws that call for performing data security risk assessments generally are not prescriptive (see Legal Considerations). Organizations:

- Can define their own detailed risk assessment methods.
- **Have flexibility regarding:**
  - The tools they use
  - Their level of formality
- **Should choose methods according to their:**
  - Risk assessment objectives
  - Culture
  - Available resources

Organizations should also identify applicable standards to assess compliance (see Generally Accepted Industry Standards and Box, Additional Resources).

Gather Information

Risk assessment teams work with stakeholders to gather pertinent information based on the assessment's scope. For example:

- **Assessments that seek to compare an organization's current information security program to industry standards and best practices may call for:**
  - Collecting documented policies, procedures, event logs, or other historical files;
  - Interviewing key individuals
  - Gathering current technical configurations and other system details
  - Documenting safeguards testing results
- Assessments that target particular systems or technical controls may require running automated scans or using other tools in the organization's IT environment.
- Service provider assessments typically use questionnaires or other vendor self-assessments but may also include:
  - Collecting independent audit or certification results
  - Running agreed on scans or other technical reviews
  - Gathering any incident reports, periodic service level metrics, or other routinely provided reports
- **Workforce assessments often include:**
  - Collecting training records, including results from compliance certification tests
  - Reviewing reports produced by compliance management activities, such as user logs and project reviews
  - Testing individuals on their current security awareness and compliance, for example, for phishing susceptibility

In all cases, the risk assessment team must 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.
- **The applicable network architecture, including:**
  - Any integration points between systems
  - Communications paths that permit external access, such as for customers, service providers, or employees who work remotely

Organizations should use their IT asset inventories to support risk assessment. An organization's inventory should include any equipment that stores or handles information, such as copiers and telephone systems, in addition to computing and network hardware and software. Data mapping activities also support risk assessments by linking the data an organization collects and systems it uses to particular business processes.

Identify Risks and Compliance Gaps

The risk assessment team next uses the information gathered to:

- Provide context.
- **Identify risk elements, including:**
  - Threats
  - Vulnerabilities
  - Likelihood
  - Impact

(See Key Concepts for Assessing Data Security Risks.)

The risk assessment team combines the identified risk elements to define and characterize current risks. Risks may cover a wide range of administrative, physical, and technical issues and are typically reported as potential events. **Some common risk examples include:**

- Delays in removing access for terminated employees may allow prior employees or others to gain unauthorized access to confidential systems and data.

- Unsecured work areas may allow unauthorized employees or others to gain access to desktop computers the organization uses to handle personal information.
- Unencrypted laptops that store personal information may cause a data breach if lost, stolen, or accessed by unauthorized parties.
- Failure to limit access to customer information to only those employees who need to know may allow unauthorized individuals to steal or misuse data.
- Using default server configurations that include unnecessary services and vendor-supplied passwords may allow hackers to compromise systems, steal data, or infiltrate the company's network.

To provide a more comprehensive assessment, along with identifying risks, organizations should:

- Compare their information security program's performance to applicable laws, regulations, standards, or other obligations (see Legal Considerations).
- Consider service provider and supply chain issues (see Box, Service Provider and Supply Chain Risk Assessment).
- Review workforce awareness and compliance (see Box, Workforce Risk Assessment).

Identified risks and program gaps often overlap. For example, a lack of access controls to protect sensitive information based on need-to-know both:

- Creates risks.
- Is contrary to laws that protect personal information.

Assessment teams should document risks and compliance gaps for reporting and ongoing risk management purposes.

Report Results

Counsel should work with risk assessment teams to determine how to best protect sensitive reports, preferably before conducting an assessment or generating a report (see Protecting Risk Assessment Reports).

Risk assessment reports should:

- Focus on findings.
- Be factual.
- Avoid speculative or conclusory statements that others may later misinterpret or take out of context, especially regarding legal risk or regulatory compliance.

To provide context and avoid misinterpretation, risk assessment reports should always document the timing, scope, and methods with the results (see Define Timing, Scope, and Methods).

Organizations may identify many data security risks and compliance gaps, though they can often address most of them with reasonable policies, practices, and safeguards. For guidance on developing policies and addressing gaps, see Practice Note, Developing Information Security Policies and Common Gaps in Information Security Compliance Checklist.

Categorizing risks and compliance gaps helps simplify reporting and program management. **Some common approaches include categorizing issues according to:**

- The group responsible for addressing the risk or compliance gap, such as a particular IT function, human resources, legal, or others.
- Pertinent laws, regulations, standards, or other obligations.
- Costs to remediate.
- Time to remediate.
- **The type of issue identified, such as:**
  - Data collection
  - Access control
  - Server maintenance
  - Network configuration
  - Application software
  - End user devices
  - Vendor management
  - Others

Some organizations choose to distinguish between technical and non-technical risks. For instance, IT groups often manage technical risks, while other stakeholders, such as human resources, legal, privacy and compliance groups, and business leadership, address non-technical issues. However, organizations should not lose sight of their total risk profile and the potential interaction between technical and non-technical risks.

Prioritizing Risks

Prioritizing risks helps focus attention and resources on those issues most likely to harm the organization. Organizations may prioritize risks by analyzing likelihood and impact together (see Likelihood and Impact), as shown in the table below. For example, a highly likely to

occur risk with medium level potential impact is treated as a high priority risk. The table provides basic guidance, but organizations should consider their unique circumstances and risk profiles when prioritizing risks. Some organizations color code risk priorities to help stakeholders focus on key issues.

	Impact		
Likelihood	**High**	**Medium**	**Low**
High	**High**	**High**	**Medium**
Medium	**High**	**Medium**	**Low**
Low	**Medium**	**Low**	**Low**

NIST provides a more detailed risk assessment scale that combines likelihood and impact using five categories (see NIST SP 800-30, Appendix I, Table I-2).

For more reporting guidance, see Box, Communicating Risks.

Manage Risks and Compliance

To ensure overall data security and avoid any appearance that they are downplaying risks, organizations should timely respond to risk assessment reports by:

- Assigning clear ownership and accountability to reasonably address each identified risk.
- Maintaining program management documents that show the organization understands identified risks and is responding appropriately.

Organizations typically respond to identified risks and compliance gaps by choosing among:

- Accepting the risk.
- **Mitigating but not resolving the risk by implementing compensating controls or other measures to:**
  - Limit the risk's likelihood of being exploited
  - Minimize the risk's potential impact, if exploited
  - Both
- Remediating the risk.

Cyber insurance can help organizations protect themselves by transferring the costs when they accept some risks. For more information on cyber insurance and typical coverage, see Practice Note, Cyber Insurance: Insuring for Data Breach Risk.

Factors that may influence an organization's decisions for how to address each risk include:

- Its risk tolerance level.
- Applicable legal obligations and the potential costs of litigation or enforcement.
- Feasibility, for example, remediation may be cost-prohibitive or not an option in the organization's current IT environment.
- The costs and time frame required to remediate.
- The organization's culture, especially if remediation requires changes in business processes or workflow.

Organizations should document their choices and track their activities to completion, if applicable. **For example, if an organization chooses to accept or mitigate rather than remediate a particular risk, it should:**

- Record its analysis and rationale.
- Set a time frame for follow up review, if circumstances change.

Protecting Risk Assessment Reports

Risk assessment reports and supporting documents typically contain highly confidential and sensitive information. **For example, risk assessment reports may detail:**

- **Specific cybersecurity vulnerabilities in the organization's IT environment.** Internal or external cyberattackers may exploit vulnerability information to gain unauthorized access to data or damage the organization's systems.
- **Gaps in regulatory compliance.** Identified risks may directly or indirectly show that the organization currently fails to comply with applicable data security laws and regulations.
- **Breaches of contract terms and conditions.** Assessments may identify practices or procedures that are contrary to the organization's contractual commitments.
- **Various circumstances that taken together could demonstrate unreasonable data security practices.** Maintaining a strong information security program requires constant vigilance. Even diligent organizations with sophisticated programs may experience periodic lapses in their controls. Risk assessments highlight these issues and provide an opportunity to address them. However, litigants, regulators, or others may use risk assessment reports that identify a large number or pattern of unaddressed gaps to claim that the organization fails to support reasonable data security practices. Reports that fail to identify or downplay material risks invite questions regarding the organization's practices.

Counsel should identify methods for protecting risk assessment reports and supporting documents, which may include:

- **Applying attorney-client privilege, the work product doctrine, or both.** Reports may be subject to attorney-client privilege, the work product doctrine, or both, according to timing and the reasons for initiating particular risk assessments. However, assessments conducted to meet regulatory obligations or in the ordinary course of business, such as to comply with company policy, are less likely to qualify for protection. **Counsel should examine the circumstances surrounding each particular risk assessment and not assume that reports are protected simply because an attorney is involved.**

  For example:

  - Attorney-supervised risk assessments conducted in anticipation of litigation, such as during a data breach investigation, may qualify as attorney work product
  - Risk assessments conducted by counsel specifically to support a client's request for legal advice may fall under the attorney-client privilege

- For more guidance, especially regarding risk assessments that an organization performs following a data breach, see Practice Note, Data Breaches: the Attorney-Client Privilege and the Work Product Doctrine.
- **Assigning the organization's most protective information classification level.** Organizations typically define an information classification model in their information security policies and apply safeguards accordingly (see Practice Note, Developing Information Security Policies: Data: Information Classification and Risk-Based Controls). Organizations should generally apply their highest level of information sensitivity, for example, Highly Confidential Information, and commensurate safeguards to risk assessment reports.
- **Using extensive administrative, physical, and technical safeguards.** Assigning the organization's most protective information classification level should provide strong safeguards. Counsel should also consider applying specific controls to risk assessment reports. **For example:**
  - Limiting distribution on a strict need-to-know basis, which may include sharing identified risks individually with those assigned to address them rather than distributing entire reports
  - Prohibiting further distribution or sharing of reports without prior approval
  - Using strict access controls, encryption, and data loss or data leakage prevention software to limit electronic access, copying, emailing, and printing
  - Minimizing the use of paper copies, including tracking and collecting any copies distributed at the end of review meetings
  - Ensuring proper disposal of electronic and paper copies, according to the organization's records retention policy
- **Educating risk assessment participants on the need to protect reports. Counsel should specifically remind risk assessment participants of:**
  - The legal risks, sensitivity, and potential misuses or

abuses of reports

- Protocols for maintaining attorney-client privilege and work product doctrine protection, including their limits, if applicable
- How to support and avoid defeating safeguards, even inadvertently
- The need to keep reports and supporting documents factual and avoid speculative or conclusory statements, especially any regarding legal risk or regulatory compliance that others may later misinterpret or take out of context

Risk Assessment Limitations

Organizations and their counsel must recognize that while crucial to an effective information security program, risk assessments are also inherently limited because:

- They depend on the accuracy and completeness of gathered information.
- Individuals who perform any particular assessment may lack necessary skills, expertise, and thoroughness.
- Automated review tools may have gaps or defects.
- **They provide a snapshot of risks at a given moment in time, but:**
  - The organization's business processes and priorities are subject to change
  - Hardware, software, and network components change
  - Cyber threats constantly evolve
  - Novel attacks regularly emerge
  - Newly identified or reintroduced vulnerabilities increase the organization's exposure

Organizations can address these limitations by:

- Treating risk assessment as a cyclical process and not a one-time event (see Risk Assessment Process).
- Including different individuals with a variety of backgrounds, skills, and perspectives on assessment teams.
- Using multiple tools for automated reviews, where feasible.
- Implementing continuous monitoring to identify and respond to potential risks on an ongoing basis.
- Periodically engaging one or more independent third-party auditors or assessors, regardless of whether they must do so by law or other obligations.

Common Forms of Data Security Risk Assessments

Common risk assessment methods vary in scope, technical detail, and resource requirements.

Audits and Certifications

These formal reviews compare current information security practices against selected standards. Information security standards typically cover administrative, physical, and technical safeguards. Auditing or other assessment standards may use the term "audit controls." Organizations often hire independent third-party auditors according to contract or other legal obligations (for details on requirements and example standards, see Legal Considerations).

To identify compliance gaps and risks, audits generally include:

- Examining current policies and procedures documents.
- Interviewing key individuals.
- Evaluating technical configurations.
- Reviewing event logs or other historical files.
- Testing safeguards.

External auditors may provide the organization with a certification or other attestation for sharing with customers, regulators, or other stakeholders.

Assessments

Less formal than audits, these reviews:

- Take a broad look at some or all of an organization's IT environment.
- Identify data security risks.
- Compare current policies, procedures, and safeguards to applicable standards.

Organizations should consider performing regular self-assessments to:

- Recognize new or changed risks.
- Identify potential compliance gaps (see Legal Considerations).
- Prepare for more costly and time-consuming audits and certifications.

Penetration Tests

During a penetration test (pen testing), technically skilled trusted individuals try to hack into or otherwise compromise an organization's IT systems using various attack methods. **Pen tests mimic the likely actions of malicious attackers and may be:**

- Externally initiated from outside an organization's internet or other network perimeter.
- Internally initiated using some knowledge of the organization's IT environment.
- A combination.

Vulnerability Scans

These reviews typically use automated tools to determine whether particular computers or other IT assets are subject to known technical vulnerabilities, especially those that hackers can easily exploit. **For example, vulnerability scans can identify:**

- Outdated software or missing patches.
- Insecure hardware or software configurations or settings.
- Unexpected or unnecessary files or services.

Asset Scans

Maintaining a current IT asset inventory is crucial for assessing and managing data security risks. Asset scans use tools to help organizations recognize network connections from desktops, laptops, mobile devices, and other computing and network equipment so that they can:

- Inventory, track, and assess risks for authorized assets.
- Discover and flag unauthorized assets for further investigation.

Continuous Monitoring Programs

Similar to other assessment activities but operating on an ongoing basis, these programs deploy software to continually:

- Monitor security controls.
- Identify vulnerabilities.
- Verify hardware and software configurations.
- Flag suspicious activities.

The tools that support continuous monitoring automatically correlate and present results to IT staff for further action. Some continuous monitoring tools include automated update features to close gaps, such as blocking suspicious network traffic, applying software patches, or changing configurations. Organizations must apply these automated remediation techniques carefully to avoid inadvertent business impact.

Service Provider and Supply Chain Risk Assessment

Service providers and other contractors can create significant data security risk because they often:

- Have direct access to the organization's IT environment.
- Provide services that create, collect, use, or maintain personal or other sensitive or confidential information on the organization's behalf.

Organizations typically assess service provider risk using a combination of:

- Pre-engagement due diligence to ensure service providers have a reasonable information security program and practices in place.
- Contract provisions that obligate service providers to maintain reasonable data security controls, often based on one or more specified standards (for example clauses, see Standard Clauses, Data Security Contract Clauses for Service Provider Arrangements (Pro-Customer)).
- Regular information security oversight throughout the relationship. **For instance, common methods of ongoing service provider risk assessment include:**
  - Regularly collecting and analyzing service provider questionnaires or other self-assessment reports
  - Specifying the use of particular safeguards, such as encryption, continuous monitoring, and data loss or data leakage prevention software
  - Periodically requiring third-party independent audits or certifications

An organization's supply chain can similarly affect data security risk. **For example, the vendor-supplied hardware and software an organization uses in its IT environment may:**

- Be subject to particular attacks.
- Introduce specific vulnerabilities, especially if vendors fail to prioritize cybersecurity or lack technical sophistication.

- Include backdoors or other channels, whether intentional or inadvertent, that could allow unauthorized parties to access the organization's data or IT environment.

Organizations should assess and manage supply chain risks by:

- Maintaining a current IT asset inventory, including hardware and software versions, to track vendors and enable risk assessment.
- Performing up front due diligence, including conducting appropriate product reviews and security testing.
- **Demanding specific contract provisions and supplier warranties regarding:**
  - Information security standards of practice, including those of third-party suppliers or subcontractors
  - Periodic audits and certifications
  - Expectations for vendors to communicate and timely address newly identified vulnerabilities
- Performing ongoing oversight to monitor vendor information security practices and manage vulnerabilities.

For more on identifying and managing service provider risks, see Practice Note, Managing Privacy and Data Security Risks in Vendor Relationships. For information on generally managing cyber vulnerabilities, see Practice Note, Cybersecurity Tech Basics: Vulnerability Management: Overview.

Workforce Risk Assessment

Organizations may choose to assess workforce awareness, training, and compliance with their information security standards separately or in their other assessments. Verifying workforce capabilities helps ensure information security. **As organizations implement technical safeguards and they evolve, people often become the weak link because:**

- **They make mistakes. For example, people:**
  - Allow themselves to be duped by attackers into sharing their passwords or downloading malware
  - Use outdated software
  - Lose or improperly discard paper files
  - Store sensitive data on easily lost or stolen unencrypted mobile devices
- **Bad actors increasingly target individuals.** Attacks on individuals like phishing, other forms of social engineering, user credential theft, and targeted malware infections are common and likely to increase as improved technical safeguards frustrate attackers.
- **Well-meaning workforce members circumvent controls.** Individuals misunderstand data security risks
  and mistakenly believe they or their organizations can benefit from bypassing controls.

Assessing workforce risk can be challenging. Counsel should consider any limits that applicable labor or other contracts or employment laws impose when selecting workforce risk assessment methods, especially those that involve testing. **Several common approaches combine risk assessment with education and include:**

- **Providing training with quizzes or other assessment tools.** Using assessment tools in their training, such as online quizzes or compliance certification tests, helps organizations determine whether workforce members understand information security policies and sound practices.
- **Testing workforce members for phishing susceptibility.** Organizations can design email messages using common attack methods and track how workforce members interact with them. Organizations can use aggregated results for general awareness messages, while identifying susceptible individuals for specific training. However, organizations must be careful not to misinterpret results. For instance, some email preview functions give messages the appearance of being opened or read even when users choose not to interact with them.
- **Using scanning and continuous monitoring results for coaching purposes.** Risk assessment tools identify individuals who download unauthorized software, change settings, or otherwise create data security risks. Organizations can use individual results to support specific coaching or take enforcement action. Aggregated results gauge general workforce compliance and may help identify and prioritize additional training needs.
- **Performing detailed reviews and testing for high priority projects.** Significant gaps indicate a lack of understanding or appreciation for data security risks. Conducting risk assessments early in the development phase provides an opportunity to further train team members and remediate issues before deployment.

Cybersecurity Information Sharing Programs

Each organization's data security risk profile is unique. However, many can benefit from sharing information on the threats they detect and the defensive measures they take with a like-minded community. Organizations can share valuable information regarding threats and defensive measures without disclosing their status or risk assessment results. Liability concerns still unfortunately limit some companies' willingness to share information. Some government agencies, like CISA, collect risk and threat details and foster public-private information sharing.

Several federal actions support information sharing, including:

- **The National Cybersecurity Protection Act of 2014, which codifies the DHS-led National Cybersecurity and Communications Integration Center (NCCIC) as:**
  - The federal civilian cybersecurity situational awareness, incident response, and event management center
  - A hub for sharing cybersecurity information among the public and private sectors
- (6 U.S.C. § 659.)
- **Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing (issued Feb. 13, 2015), which directs DHS to encourage the development of public-private information sharing and analysis organizations (ISAOs) by:**
  - Working through the NCCIC to coordinate information sharing
  - Consulting with other federal agencies that have cybersecurity responsibilities, including sector-specific regulators
  - Designating a standards organization to set voluntary standards and guidelines for ISAOs
  - Ensuring that information sharing activities incorporate privacy and civil liberties protection
- **The Cybersecurity Information Sharing Act of 2015, which encourages companies to timely share information about cybersecurity threats, incidents, vulnerabilities, and defensive measures by:**
  - Directing DHS to create an online portal and related guidelines to support information sharing
  - Requiring private entities that share information with DHS to first remove any personal information that is not directly related to a cybersecurity threat
  - Clarifying that sharing information in accordance with the Act will not violate antitrust laws or waive any applicable privilege or protection provided by law, including trade secret protection
  - Prohibiting agencies from using shared information for regulatory purposes, including enforcement actions, other than to inform the rulemaking process
  - Stating that the Act does not create a duty to share, warn about, or act on cybersecurity threats or defensive measures
  - Establishing liability protection for private entities that monitor information systems or share cybersecurity information in accordance with the Act
- (6 U.S.C. §§ 1501 to 1510.)

Organizations should consider participating in information sharing programs when developing their data security risk assessment process. Benefits include:

- Rapidly receiving information regarding new threats and recommended defensive measures, often before cyberattackers target them.
- Learning from a broad set of others' experiences.
- Sharing information in a vetted community.
- Helping strengthen information security across the public and private sectors.

For more on information sharing programs and links to the DHS portal and other resources, see Box, Additional Resources.

Communicating Risks

Just as current laws, regulations, and standards allow organizations to choose their risk assessment methods, reporting approaches also vary. **Organizations should select one or more means for recording and communicating identified risks and compliance gaps that:**

- Standardize reporting to ease comparison and data aggregation.
- Offer sufficient details for accountable parties to take action.

- **Provide summaries or other easy-to-read views for executives, such as:**
  - Dashboards
  - Top ten lists
  - Business unit or program-specific scorecards
  - Support strict access controls to protect sensitive assessment data (see Protecting Risk Assessment Reports).

Using familiar tools may lower costs and simplify communications. Some common examples include:

- Tables or spreadsheets.
- Project management tools.
- IT ticketing systems.

For each identified risk, reports should at minimum include:

- Risk priority, if applied (see Report Results).
- Any category or risk type.
- A description of the risk as a potential event (for examples, see Identify Risks and Compliance Gaps).
- Likelihood.
- Potential impact.
- The date identified.
- Identification method.
- The owner or accountable party.
- The action to be taken (see Manage Risks and Compliance).
- The planned or actual completion date.
- Any applicable law, standard, or other related obligation.
- Notes or additional information.

Risk assessment teams should regularly update reports until applicable actions are complete. **Counsel should advise those who create, receive, or maintain risk assessment reports on the need to:**

- Keep reports and supporting documents factual.
- Avoid speculative or conclusory statements, especially any regarding legal risk or regulatory compliance that others may later misinterpret or take out of context.

(See Protecting Risk Assessment Reports.)

Mapping results to industry standards can help gauge compliance and improvements made over time. For instance, the NIST Cybersecurity Framework encourages organizations to use its profiles to track their alignment in terms of a current state and a desired target state (for more information on the Framework, see Practice Note, The NIST Cybersecurity Framework).

Additional Resources

Industry standards and other resources provide further guidance on performing data security risk assessments. See Generally Accepted Industry Standards for common standards that organizations may use to assess current program effectiveness.

Other helpful resources include:

- For general data security risk assessment guidance, see:
  - NIST SP 800-30, Guide for Conducting Risk Assessments
  - ISO 27005
  - The Center for Internet Security's Risk Assessment Method
  - FTC data security guides, which address risk assessment and safeguards (see Practice Note, FTC Data Security Standards and Enforcement: FTC Data Security Guidance)
  - CISA's Cyber Resilience Review materials
  - For examples of sector-specific risk assessment guidance, see:
  - In the financial services sector, Practice Note, GLBA: The Financial Privacy and Safeguards Rules: Box, Interagency Guidelines and Bank Examinations
  - In the healthcare sector, the Security Risk Assessment Tool provided by the **Department of Health and Human Services** to assist covered entities with their HIPAA-required risk analyses
  - For information on CISA implementation and cybersecurity information sharing, see:
  - U.S.-CERT's Automated Indicator Sharing (AIS) tools and resources
  - The ISAO Standards Organization publications available on its website

- NIST SP 800-150, Guide to Cyber Threat Information Sharing
- Sector-specific information sharing groups, such as the Financial Services Information Sharing and Analysis Center, the Multi-State Information Sharing and Analysis Center, the Information Technology Information Sharing and Analysis Center, and others that together have formed the National Council of ISACs
- For detailed attack (threat) examples, see the Common Attack Pattern Enumeration and Classification (CAPEC) website.
- For a broad set of regularly-updated vulnerability reports and other current information, see CISA's National Cyber Awareness System.