REUTERS / Kacper Pempel

Developing Your Information Security Program: WISPs, Policies, and More

August 11, 2016

Panelists:

Melissa Krasnow, Partner, *Dorsey & Whitney LLP*
Ivan Rothman, Of Counsel, *Squire Patton Boggs (US) LLP*
Mel Gates, Senior Legal Editor, *Practical Law Intellectual Property & Technology (Moderator)*

DORSEY™ always ahead

SQUIRE PATTON BOGGS

The intelligence, technology and human expertise
you need to find trusted answers.

the answer company™
THOMSON REUTERS®

Agenda

Introduction

Presentation: *Developing Your Information Security Program: WISPs, Policies, and More*

- Key Issues in Developing Your Organization's Information Security Program
- Written Information Security Programs (WISPs)
  - Legal obligations and issues
  - Key WISP elements and best practices
- Information Security Policies
  - Legal obligations and issues
  - Key policy elements and best practices
- Risk Assessment and Preventing Cyber Incidents

Quick Review of Practical Law Related Resources

Q&A Session

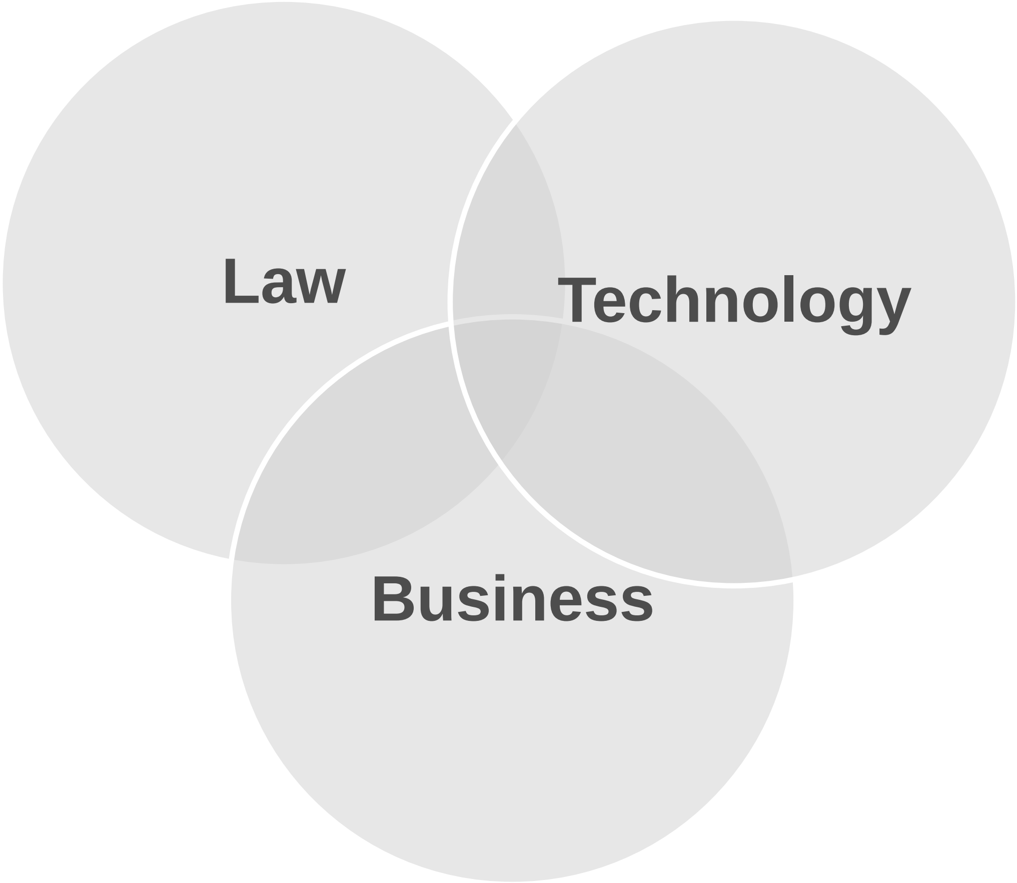
Conclusion

Key Issues in Developing Your Organization's Information Security Program

Why Information Security?

Privacy and information security operate at the intersection of law, technology, and business.

- Just a few of the challenges include:
  - increasing threats;
  - heightened expectations from:
    - customers,
    - shareholders,
    - employees,
    - business partners, and
    - regulators;
  - lack of communication among legal, IT, and business leadership; and
  - the demands of changing technology and ongoing risk management.



A Growing Body of Law Demands Counsel's Attention

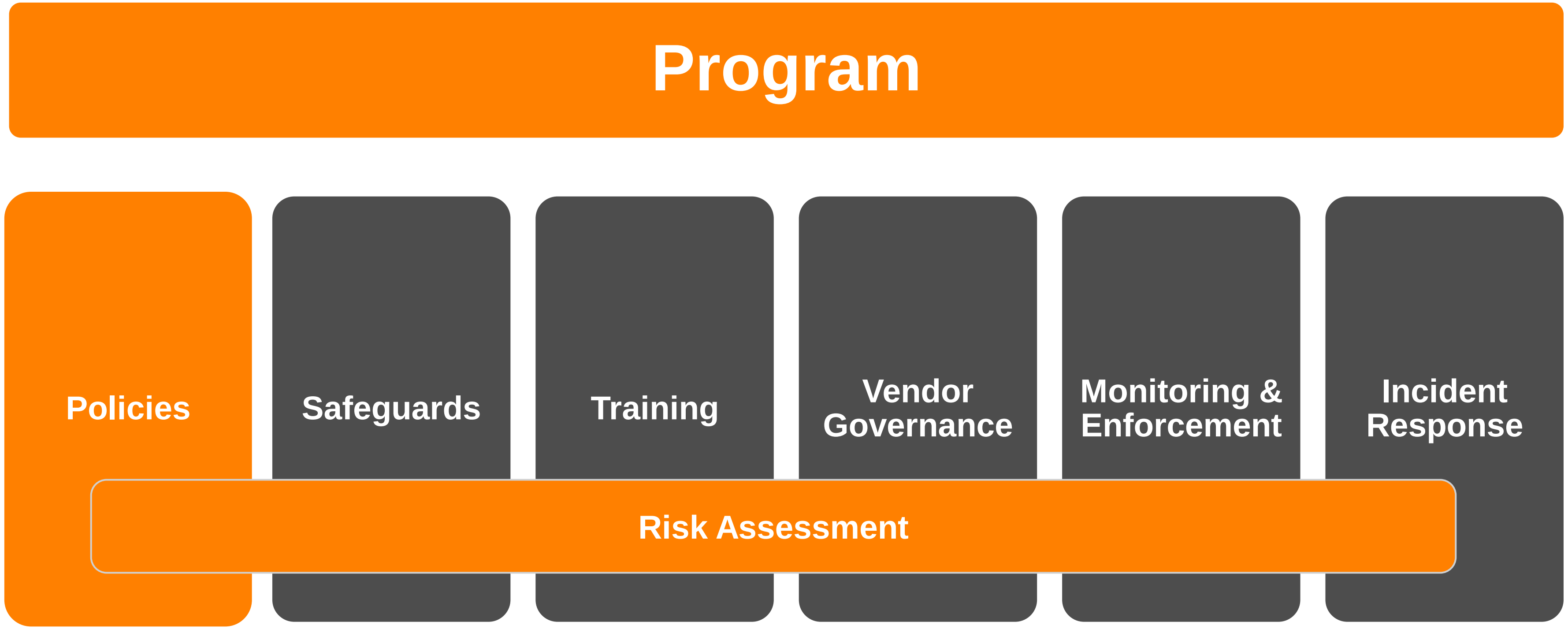
Common business scenarios create legal obligations to develop, implement, and maintain a reasonable information security program.

- Some examples include:
  - collecting and using personal information of customers, employees, or others;
  - participating in an industry sector that is considered high risk or critical infrastructure;
  - offering securities as a public company;
  - protecting trade secrets and other internal or proprietary information;
  - handling other organizations' information, subject to contract terms and conditions;
  - accepting certain forms of payment, such as credit cards, other payment cards, or direct payments from bank accounts; and
  - aiming to demonstrate compliance with generally-accepted industry standards for various legal and business purposes.

Building an Information Security Program

Information security programs combine multiple elements to protect the confidentiality, integrity, and availability of systems and data.

- Effective programs rely on:
  - policies;
  - processes;
  - people; and
  - tools.



Program

Policies

Safeguards

Training

Vendor Governance

Monitoring & Enforcement

Incident Response

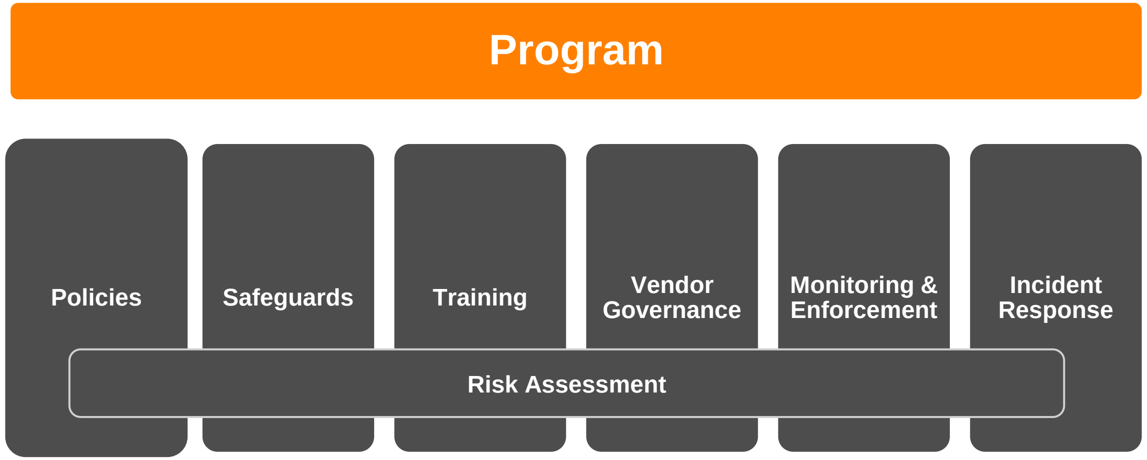
Risk Assessment

Written Information Security Programs (WISPs)

A Written Information Security Program (WISP) Documents the Measures an Organization Takes to Protect its Systems and Data

A WISP consists of high-level program descriptions and makes organizational commitments.

- WISPS are:
  - targeted to organizational leadership and stakeholders;
  - concise since policy and implementation details reside in related documents; and
  - required by some federal and state laws.



Program

Policies

Safeguards

Training

Vendor Governance

Monitoring & Enforcement

Incident Response

Risk Assessment

State Data Security Laws Protect Personal Information

State data security laws focus on those who handle personal information, including customer and employee data.

- Data security laws vary by state, but where enacted, may require businesses to:
  - maintain appropriate security policies, procedures, and safeguards;
  - train employees;
  - oversee service providers;
  - periodically assess risks; and
  - monitor their programs.

State Data Security Laws Protect Personal Information

- Massachusetts, Oregon, and Rhode Island require an **information security program**.
- Massachusetts requires a **written information security program**.
  - M.G.L. c. 93H; Mass. Regs. Code tit. 201 § 17.01-17.05
  - Or. Rev. Stat. § 646A.622
  - R.I. Gen. Laws §§ 11-49.3-1 through 11-49.3-6

State Data Security Laws Protect Personal Information

- Others states require **reasonable security measures** to protect personal information. Some examples include:
  - Ark Code Ann. § 4-110-104(b).
  - Cal. Civ. Code § 1798.81.5.
  - Fla. Stat. § 501.171(2).
  - 815 Ill. Comp. Stat. § 530/45 (as amended by H.B. 1260, effective Jan. 1, 2017).
  - Ind. Code Ann. § 24-4.9-3-3.5.
  - Md. Code Ann., Com. Law § 14-3503.
  - Nev. Rev. Stat. §§ 603A.210, 215 (including payment cards data standards).
  - Tex. Bus. & Com. Code Ann. § 521.052(a).
  - Ut. Stat. § 13-44-201(1)(a).

State Data Security Laws Protect Personal Information

- California AG guidance sets a **baseline** for reasonable security practices:
  - details appear in her Data Breach Report 2012-2015;
  - published in Feb. 2016, see https://oag.ca.gov/breachreport2016; and
  - leverages the Center for Internet Security's 20 Critical Security Controls.

Federal Law Focuses on FTC Enforcement and Sector-Specific Requirements

The Federal Trade Commission (FTC) takes data security enforcement actions under its authority to address unfair or deceptive trade practices.

- Actions focus on businesses that fail to:
  - keep their data security commitments, including promises to follow industry standards; or
  - implement reasonable safeguards to protect personal information.
- FTC follows a **reasonableness standard**.

- Federal sector-specific data security laws include:
  - HIPAA/HITECH (healthcare);
  - GLBA (financial services);
  - COPPA (children’s online privacy);
  - FERPA (student information); and
  - those applicable to telecommunications and other sectors.

WISP Benefits

Even when not explicitly required by law, WISPs may provide risk management benefits to organizations.

- Some **potential benefits** include:
  - prompting the organization to proactively assess risk and implement safeguards;
  - educating employees and other stakeholders;
  - communicating information security expectations and practices to leadership, customers, and other interested parties, including regulators; and
  - establishing that the organization takes **reasonable steps**, especially in the event of a data breach or other security incident where litigation or enforcement action could occur.

Issues to Consider Before Developing a WISP

Counsel should consider key issues regarding applicable laws, data collected, and the organization's culture before creating a WISP.

- How is personal information defined?
- What types of personal information does the organization collect, use, store, or share?
- Where do affected individuals reside?
- What laws and regulations apply?
- Does the organization have other information security obligations, such as any imposed by contracts?
- For what purposes does the organization collect, use, store, or share personal information?
- What other sensitive or confidential information (if any) should the WISP address?
- How is information collected, stored, and managed (including any safeguards)?

Issues to Consider Before Developing a WISP

- Who are the organization's third-party service providers and other business partners?
- What is the WISP’s relationship to the organization’s other policies and obligations?
- What resources are available to develop, implement, and maintain the WISP and any supporting policies, procedures, or other program elements?
- Who will own the WISP and be accountable for information security matters?

- Should the WISP:
  - be state-specific or nationwide (or global) in scope?
  - apply to part or all of the organization?
  - address a specific law (separate) or different laws (combined)?

Common WISP Elements

Common WISP elements demonstrate accountability.

- WISPs typically include:
  - Purpose.
  - Scope.
  - Information security coordinator designation and responsibilities.
  - Training.
  - Commitments to:
    - conduct periodic risk assessments and address identified issues;
    - develop, maintain, and distribute appropriate information security policies and procedures;
    - develop, implement, and maintain reasonable administrative, physical, and technical safeguards;
    - oversee service providers;
    - regularly test, monitor, and update the program; and
    - establish and maintain incident response policies and procedures.
  - Enforcement and sanctions for violations.
  - Periodic (annual) program review and documentation.

State-Specific Requirements

Some state laws and regulations dictate detailed program elements and safeguards.

- Several states require organizations to impose **contractual obligations on service providers** to implement and maintain similar reasonable security measures.

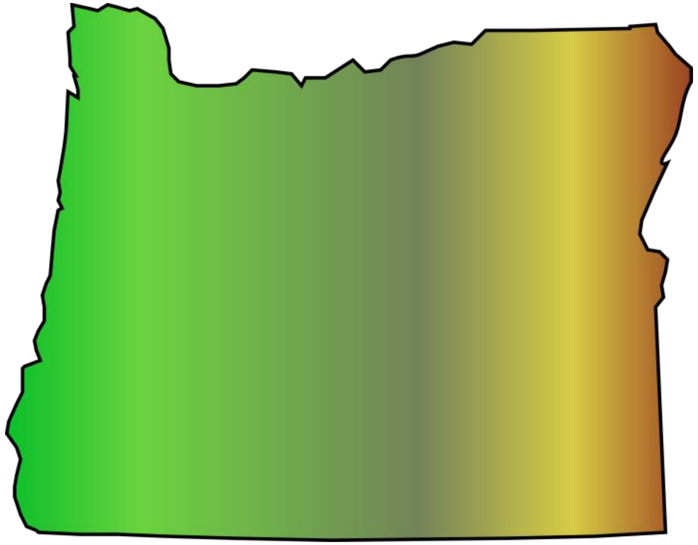
- Massachusetts and Oregon call for **risk assessments** that pay particular attention to:
  - ongoing employee training, including training for temporary and contract employees;
  - employee compliance with policies and procedures; and
  - means for detecting and preventing security system failures.

State-Specific Requirements

- Massachusetts regulations also emphasize:
  - the need to prevent **terminated employees** from accessing personal information;
  - **incident response and post-incident analysis** and follow up documentation;
  - particular **safeguards** (security system elements), including:
    - secure user authentication protocols;
    - secure access control measures;
    - encryption; and
    - monitoring, network perimeter, and anti-malware controls.

State-Specific Requirements

- Oregon calls for focusing on **risk assessment and management** by:
  - assessing risks in:
    - network and software design;
    - information processing, transmission, and storage; and
    - information storage and disposal.
  - detecting, preventing, and responding to attacks or system failures;
  - testing and monitoring the effectiveness of key controls, systems, and procedures;
  - detecting, preventing, and responding to intrusions;
  - protecting against unauthorized access to or use of personal information; and
  - securely disposing of personal information after it is no longer needed.



State-Specific Requirements

- Rhode Island highlights **records management issues**, requiring that personal information:
  - Be retained no longer than is required:
    - to provide requested services;
    - to meet the purposes for which the personal information was collected;
    - in accordance with a written retention policy; or
    - by law.
  - Be securely disposed of after it is no longer needed.

Practice Tips: Effective WISPs

Taking some simple steps can improve a WISP's effectiveness.

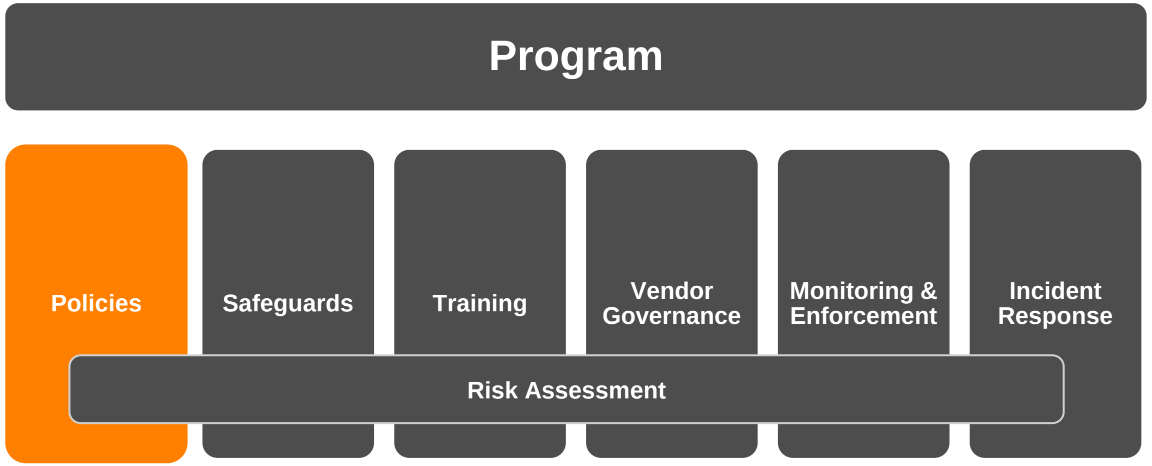
- Identify specific reasons for adopting a WISP.
- Define objectives.
- Establish a clear scope.
- Engage pertinent stakeholders.
- Assign accountability for developing, implementing, and maintaining information security program elements detailed in the WISP.
- Set reasonable expectations for related policies and other documents.
- Periodically review and seek feedback on the WISP, especially when business practices change.

Information Security Policies

Workforce-Facing Information Security Policies Establish Accountability and Standards of Behavior

Policies assign detailed program responsibilities but also address the weak link in information security: people.

- As one element of an organization’s information security program, a robust policy helps minimize risks by:
  - establishing information security as a core value;
  - laying out clear rules for using and protecting information assets;
  - helping workforce members understand and manage information security risks;
  - providing a basis for training; and
  - fostering communication among workforce members and the information security team.



Legal Requirements for Information Security Policies Address Personal Information and More

Federal and state laws and regulations, industry standards, and best practices require information security policies.

- WISP laws call for policies.
- Reasonable security practices are generally understood to include policies and related training.
- The need to implement reasonable security practices, including policies, addresses protecting personal information and more, including:
  - sector-specific regulations;
  - critical infrastructure obligations;
  - public company risk disclosures;
  - trade secrets protection;
  - contract obligations, including payment processing; and
  - litigation and enforcement risk management, especially if a data breach or other security incident occurs.

Issues to Consider Before Developing a Policy

As with WISPs, counsel should consider key issues regarding applicable laws, data collected, and the organization's culture before creating a policy.

- What laws and regulations apply?
- What industry standards and best practices has the organization adopted (or plans to adopt)?
  - for example,
    - generally applicable standards such as those collected in the NIST Cybersecurity Framework;
    - sector-specific standards and best practices; and
    - activity-related standards, such as the Payment Card Industry Data Security Standard (PCI DSS).

- Does the organization prefer a single workforce-facing policy or multiple policy documents, such as those that address:
  - acceptable use; and
  - bring your own device to work (BYOD)?

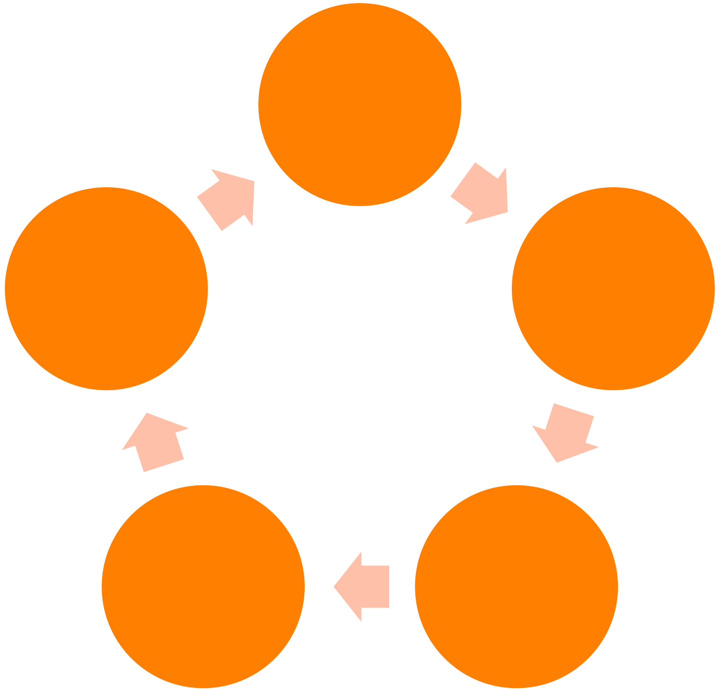
Issues to Consider Before Developing a Policy

- Will the organization’s culture and characteristics support the policy and specific policy decisions contained in it?
- Is the scope realistic?
- Does leadership value information security and will they support the policy by modeling good practices?
- Will the information security coordinator have real enforcement authority?
- Are sufficient resources available to implement and maintain the policy, including compliance monitoring?
- How technically savvy are most workforce members?
- How much (if any) control do users need over the desktops, laptops, and mobile devices they use?
- Does the organization support telecommuting and BYOD?

Developing, Implementing, and Maintaining the Policy

Information security policy development is an iterative process, because risks and business needs change.

- Designating and empowering a **policy owner** promotes accountability.
  - The policy owner typically should be the same individual (role) identified as the information security coordinator in any WISP.
- Policy development follows a **five-step process** to:
  - identify stakeholders, build collaboration, and gather information;
  - identify legal obligations;
  - develop policy content;
  - implement the policy and supporting processes; and
  - periodically review and update the policy.



Developing, Implementing, and Maintaining the Policy

Information security policies should be concise and change infrequently.

- A reasonable information security program requires more extensive **supporting documents** to ensure that the organization:
  - applies its policy consistently;
  - develops, implements, maintains, and improves individual program elements over time; and
  - can demonstrate the program's effectiveness in audits.

- Related documents provide technical details and may include:
  - supporting processes and procedures (organization-wide and local);
  - compliance programs;
  - technical security standards;
  - operations procedures;
  - best practices and guidelines; and
  - checklists.

Key Policy Topics and Provisions

No single information security policy is right for all organizations, but reasonable practices and standards call for addressing core topics.

- **Introductory statements**, including:
  - basic compliance and confidentiality expectations;
  - any guiding principles;
  - scope;
  - resources for getting help;
  - privacy and monitoring expectations; and
  - regulatory compliance, including a brief review of applicable laws.

- **Responsibilities, authorities, and obligations**, including:
  - naming and designating authority to the policy owner (information security coordinator);
  - exceptions and making exception requests;
  - workforce acknowledgment and compliance obligations;
  - sanctions;
  - training; and
  - customer/client policies (if applicable).

Key Policy Topics and Provisions

- **Data classification and risk-based safeguards and controls**, for example:
  - public information;
  - confidential information; and
  - sensitive (or highly) confidential information.

- **People-related policies**, such as:
  - roles for employees, contractors, and others;
  - identity and access management (access control); and
  - acceptable use.

Key Policy Topics and Provisions

- **Protecting information assets**, including:
  - end-user computers and access;
  - passwords and user credentials;
  - perimeter controls;
  - data and network segmentation;
  - encryption;
  - data and media disposal;
  - log management and retention;
  - physical security; and
  - disaster preparedness.
- Managing **customer/client information** (if applicable).
- **Managing information assets**, including limits regarding:
  - procurement;
  - asset inventory and management;
  - authorized computing environments and network connections;
  - change management; and
  - application and software development (if applicable).
- **Incident** reporting and response.
- **Service provider** governance.
- Risk and compliance management.

Communicating the Policy to the Workforce

Without clear communications and training, workforce members may be unaware of the organization's policy or confused about their personal obligations.

- The policy should make clear that:
  - in many cases, all workforce members are personally responsible for taking or avoiding specific actions as stated; but
  - in some situations, the information security team, IT, or another operational resource takes or avoids the stated actions.
- With counsel’s support, organizations should:
  - select one or more appropriate policy delivery methods;
  - provide workforce training; and
  - offer workforce members expert help when needed.

Practice Tips: Effective Policies

Effective policies share some common traits.

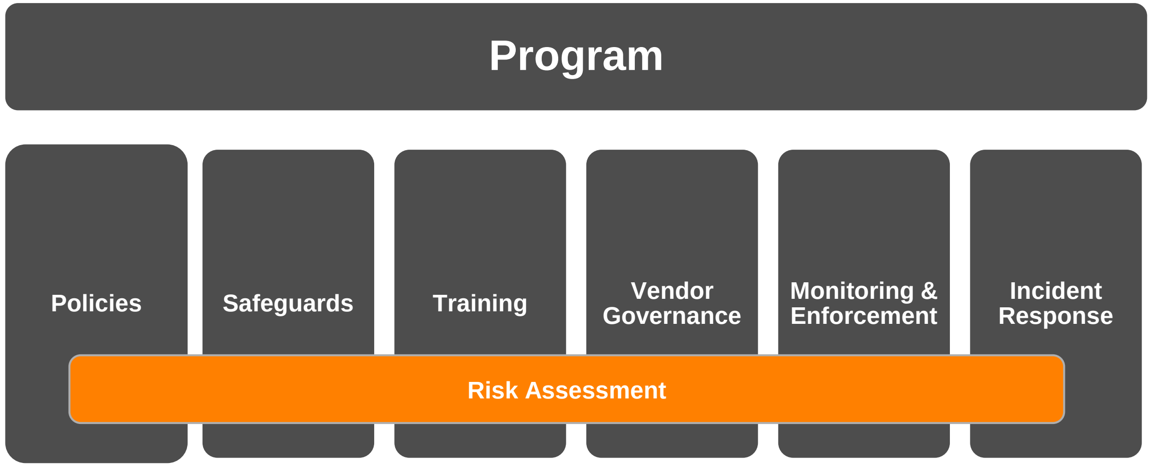
- Policies should:
  - have clear ownership coupled with collaborative development;
  - be based on detailed information gathering and informed decision making;
  - be written in plain language and made easily accessible;
  - apply to the current environment but evolve as the business changes;
  - set standards that are feasible to implement;
  - contemplate exceptions and their management;
  - be supported by responsive experts and processes;
  - be monitored for compliance and consistently enforced;
  - explain policy decisions where appropriate; and
  - help demonstrate information security's value to the organization.

Risk Assessment and Preventing Cyber Incidents

Counsel’s Role in Data Security Risk Assessments

Risk assessments are inherently operational, but counsel plays an important role in this crucial 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.
- To provide effective advice, counsel must understand common data security risk assessment:
  - terminology;
  - processes; and
  - standards.



Key Concepts for Defining Data Security Risks

Current laws and regulations that mandate risk assessments generally do not directly define risks or prescribe specific methods for identifying them.

- 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;
  - **vulnerabilities** or weaknesses that exist within the organization's environment;
  - the **likelihood** or probability that a particular threat or threat actor will exploit one or more vulnerabilities; and
  - the **impact** or harm likely to result from a particular event.

Key Concepts for Defining Data Security Risks

- Risk assessments typically focus on:
  - identifying **reasonably foreseeable internal and external risks** to data security; and
  - reviewing an organization's **current information security program** for:
    - compliance against a specified set of standards;
    - general effectiveness; or
    - both.

- Common forms of risk assessments include:
  - audits and certifications;
  - assessments;
  - penetration tests;
  - vulnerability scans;
  - asset scans; and
  - continuous monitoring programs.

Practice Tips: Protecting Risk Assessment Reports

Risk assessment reports and supporting documents typically contain highly confidential and sensitive information.

- Counsel should identify methods for protecting reports, such as:
  - applying attorney-client privilege, the work product doctrine, or both (where appropriate);
  - assigning the organization's most protective information classification level;
  - using extensive administrative, physical, and technical safeguards; and
  - educating risk assessment participants on the need to protect reports.

Practice Tips: Preventing Data Breaches, What Counsel Can Do

Most data breaches and cyber incidents are preventable. Counsel can help organizations minimize their risks and the potential impact of these unfortunate events.

- Help the organization understand that information security and privacy are not just IT issues.
- Develop a WISP and appropriate policies.
- Encourage appropriate training.
- Create and maintain data and IT asset inventories, because you cannot protect something that you don’t know is there.
- Support regular risk assessments.
- Maintain sound safeguards, including service provider oversight and governance.
- Stay vigilant because privacy and data security laws (and risks) are constantly evolving.
- Expect the best, but prepare for the worst with a solid (and tested!) incident response plan.

Practical Law Related Resources

- Practice Notes
  - US Privacy and Data Security Law: Overview
  - Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation
  - Developing Information Security Policies
  - Data Security Risk Assessments and Reporting
  - The NIST Cybersecurity Framework

- Standard Documents
  - Information Security Policy
  - Written Information Security Program (WISP)

- Common Gaps in Information Security Compliance Checklist

Q&A Session

CLE Credit

CLE credit is available for: Arizona, California, Colorado, Georgia, Hawaii, Illinois, Indiana, Mississippi, Missouri, New Hampshire, New Jersey, New York, North Carolina, Oklahoma, Pennsylvania, Vermont, Washington

CLE credit is being sought for: Louisiana, Minnesota, Oregon, Tennessee, Texas, Virginia

CLE credit can be self-applied for in: Florida

To obtain your certificate of attendance for your use in CLE credit compliance,

please fill out and submit the online form:

https://wlec.formstack.com/forms/pl_213278

- Once we receive your request, we will process it within an average of two (2) weeks. Your certificate will be archived on www.westlegaledcenter.com and instructions will be e-mailed to you on how to download your certificate from this location for your own records.

- If your requested state(s) allow the sponsor to report your CLE attendance, we will do so and pay the associated fees within 30 days of your course.

- If you have questions, please contact accreditation@westlegaledcenter.com.