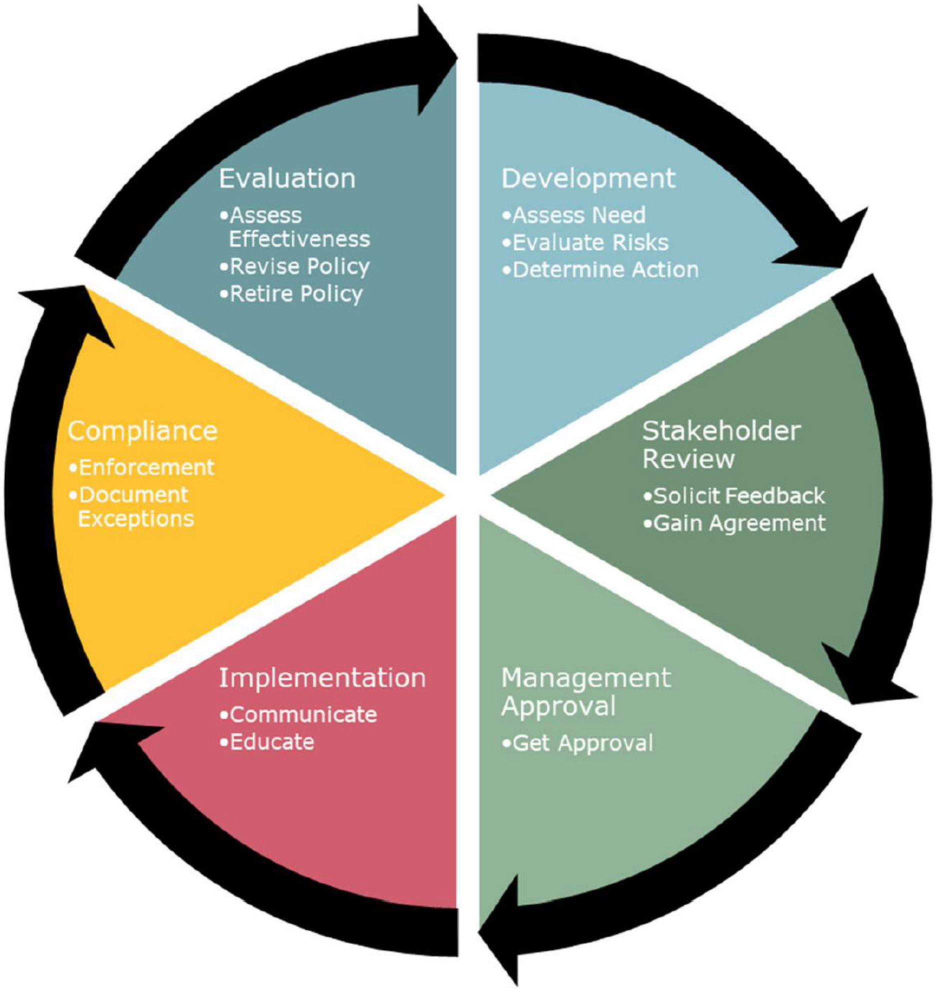
Information Security Policy Lifecycle

By Joanna Grama

The policy lifecycle describes the stages that a policy goes through, from conception to retirement. The graph below describes the policy lifecycle. The guidance below outlines the items that should be considered in each step of the policy lifecycle. All policies should follow the policy lifecycle, even though this resource specifically addresses information security policies.



Note: For the most part, the word “policy” is used in its most generic sense in the below guidance; meaning that it refers in whole to policies, standards, procedures, and similar information security governance documents. The use of the general term is to enable the reader to quickly review and understand the policy development lifecycle.

The **Development** stage contains the following general steps:

Suggestions for new policies or procedures, or revisions to existing policies or procedures, should be reviewed and assessed according to need. Questions to review include:

- Does the proposed document (or anticipated revision) address a situation that applies to the entire organization or a single department?
- Does any other policy or procedure already address the situation being discussed? (This is especially important for new documents, but may also apply to revisions as well.)
- What kind of risk is the proposed policy (or revision) intended to address? Is the risk related to compliance, a financial risk, an IT lifecycle risk, an operational risk, a reputation risk, or a strategic risk?
    - Compliance: Risks that relate to a potential violation of a law or regulation or organizational policy or requirement
    - Financial: Risks that impact the organization's financial resources or financial operations
    - IT Lifecycle: Risks that impact the provisioning of IT systems and services
    - Operational: Risks that impact the day-to-day operation of IT systems and services
    - Reputational: Risks that negatively affect organizational image, standing, or character
    - Strategic: Risks that may have a lasting impact on an organization's ability to pursue its overarching mission or strategic goals
- Can you clearly describe the following items for the proposed policy (or revision):
    - Description of the policy (or revision)
    - The business reason or justification for the policy (or revision), as well as the risks and potential impacts of (not) implementing the policy.
    - Impacted stakeholders
    - Any organizational dependencies that would impact the implementation of the policy (or revision) (e.g., technical, regulator, or organizational dependencies)
    - Policy (or revision) implementation milestones
    - Compliance and enforcement expectations
- Following a review of these items, the organization will decide on a course of action for the proposed policy (or revision). Possible courses of action include drafting a new document, making revisions to an existing policy document, choosing not to take action, or pursuing some other type of action. At this point, if necessary, policy (or revision) drafting should commence according to the information security policy development process.

The **Stakeholder Review** stage contains the following general steps:

Stakeholder review is one of the most important steps in the policy development (or revision) process. There is no one best process for stakeholder review. The most important thing is to make sure that the individuals charged with policy responsibilities have an opportunity to review any draft policies (or revisions). Stakeholders usually include impacted subject matter experts and business owners, including information security, legal counsel, human resources, operational staff, and any other applicable data or IT steering committees.

Stakeholder review often unearths issues that may negatively impact policy implementation, can help identify avenues to explore for compliance and enforcement, and ultimately builds consensus for the policy. Stakeholder review can help make policies more readable and understandable and ensures that organizational leaders are invested in the successful implementation of a policy. This engagement ultimately helps encourage community members to comply with the policy and results in changed organizational behavior. In addition to thinking about the same types of questions explored in the Development stage, Stakeholders can conduct their review of draft policies (or revisions) by thinking about the following questions:

- Is this policy (or revision) understandable?
- Is this the right type of policy (or revision) for this situation, or would some other course of action be more useful? (and why?)
- Does the policy (or revision) balance security/protection with productivity? For the organization? For my unit/department?
- What does the organization (or my unit/department) need to do to comply with this policy (or revision)? Can we comply with it or will we need an exception? (Keep in mind that one difficulty with information security policies is a balance must be struck between providing enough detail that community members understand their responsibilities, but not so much detail that the organization is exposed to unnecessary information security risk).
- Do people know what they will need to do to comply with the policy (or revision) by reading the document, or is more guidance needed? As a leader, do I know what I will need to do to support the policy?
- Are there any potential barriers or obstacles to policy implementation? How can those be overcome?

After stakeholder review, the unit responsible for drafting the proposed policy (or revisions) may choose to make changes to the document. Substantive changes should always be reviewed by stakeholders for additional feedback (and this helps build consensus). A substantive change is one that is a significant modification or alters the intent of the original document. They include modifications like changes to the scope of the policy, the list of permitted (or unpermitted actions), or a change to compliance or enforcement actions. Following the conclusion of this stage, stakeholders should largely agree on the terms contained in the draft policy (or revision).

The **Management Approval** stage contains the following general steps:

During this stage, the unit responsible for drafting the proposed policy (or revisions) presents the draft to the ultimate decision-makers (or signatories) for review and approval. Review and approval are usually shown by the highest applicable leadership level signing or ratifying the document. At the end of this stage, the document is considered an official organizational or departmental policy, or procedure (either as newly promulgated or revised).

The **Implement** stage contains the following general steps:

The policy development process doesn't stop once a document is approved by management. During the implementation stage, the unit responsible for the policy must make sure that the entire organization (or at the very least the audiences subject to the policy) is aware of the policy and knows what it needs to do to comply with the policy. If the organization and applicable audiences don't know about the policy or their responsibilities, then the effectiveness of the policy will be in jeopardy. During this stage, the unit responsible for the policy should consider the following:

- Has the policy been posted to the organizational policy repository or website (or internal intranet site)?
  - Policies with requirements for multiple audiences should be published without authentication (so that all end users can see the policies). This is particularly important if policies apply to entities with no organizational affiliation or authentication credentials (e.g., third party providers).
  - Policies that include detail about operational security activities should be protected with authentication.
  - IT staff should have access to all information security policies and procedures to do their jobs. Documentation should be protected by authentication where necessary to protect operational security.
- Does this policy (or revision) need to be communicated to the entire organization?
- What vehicles (e.g. newsletters, email, social media, listservs) are available for communication to various audiences about the policy (or revision)?
- Are marketing and communication staff members available to help tailor communications to individual audiences?
- How often should the policy (or revision) be communicated to the various audiences? (More complex policies might be communicated more frequently; or require yearly reminders.)
- Do organizational community members need general training on the policy?
  - Is the training required by a regulatory requirement?
  - Is the training mandatory or optional?
  - Must the training be in a particular format (e.g., live, online, written, verbal)?
  - Who will produce the training and give the training (if in person)?
  - Who will communicate the training when it is available?
  - How long do audience members have to complete the training?
  - Who will document that audience members have completed the training?
  - How often must the training be repeated?
- Do any organizational community members need specialized training on the policy (e.g., technical staff or staff charged with implementing policy or procedure elements)? (See the same sub-questions as above.)

The **Compliance** stage contains the following general steps:

The compliance stage includes actions taken by the unit responsible for policy to ensure that the policy is being followed and that any exceptions to policy compliance are documented, approved, and regularly reviewed. During this stage, the unit responsible for the policy may take the following general actions:

- Coordinating with other units/departments on their policy compliance activities
- Coordinating with organizational audit and other oversight groups regarding organizational policy compliance
- Responding to questions about the policy and/or compliance issues
- Following a documented policy exception process and ensuring that requested policy exceptions are reviewed according to that process
- Developing ongoing communications about organizational policy compliance (e.g., policy reminders and coordinating non-mandatory policy training).
- Coordinating and scheduling required policy compliance training

The **Evaluate** stage contains the following general steps:

Continuous review and improvement are a critical part of the information security policy lifecycle. All policy documents should be regularly reviewed to ensure that they are still appropriate and continue to meet the organization's information security goals. In most instances, the unit responsible for the policy will review the policy at required intervals or when external or internal triggers require the review and update of the policy. Some of the most common triggers that would indicate that policy review is needed include:

- Changes in Federal or State laws and regulations
- Audit findings
- Changes in technology or in how technology is provisioned
- Major information security project deployments
- New organizational business practices
- Conversations with organizational stakeholders that indicate a need for policy support

Following the policy review, the unit responsible for reviewing a policy may decide that:

- The document continues to be accurate and needs no updates or revisions
- The document needs updating or other revisions
- The document is no longer needed and should be rescinded

Revisions to existing policies should be addressed according to this lifecycle process (beginning with the development stage). Sometimes a policy will indicate the timeframe for review (i.e. every 3-5 years). If not, the responsible department should establish and follow a review cycle for policies.

Vantage Technology Consulting Group provides a broad spectrum of interrelated information technology consulting services ranging from visioning and strategic planning to design and commissioning. We work with IT departments to develop their technology and communications infrastructure and mitigate cybersecurity and physical security risks. Contact us for more information. www.vantagetcg.com