7 BUSINESS-CRITICAL IT POLICIES & HOW TO IMPLEMENT THEM

Organizations know that policies are critical to any mission. How do you handle data? How do you navigate surprise incidents or emergency changes? How do you secure critical information?

Governance is a key element of the service value system—that is, the way you create and deliver value to your customers. The ISO/IEC 38500:2015 standard for governance of IT departments and organizations defines IT governance as the system by which the current and future use of IT is directed and controlled.

According to ITIL® 4, this direction usually comes in two forms: strategies and policies.

- **Strategies** set priorities for business activities and investment.
- **Policies** establish the requirements for how everyone across the organization handles certain practices, including suppliers, partners, and other stakeholders where relevant.

Strategies are typically spelled out from the CEO and executive leadership. But what are the policies that an organization needs to have in place in order to succeed? Experts suggest a few IT areas that need policy.

Let's take a look.

What are policies?

Policies are the framework and constraints (guardrails) within which employees can strive for individual and collective success. ISO vocabulary defines a policy as:

> *"Intentions and direction of an organization, as formally expressed by its top management."*

Developing company IT policies

In IT, the scope for policies covers many areas, ranging from high-level, organization-wide policies to specific topical policies that likely affect only IT employees. When developing policies for your organization, consider:

- Aims and objectives of your organization
- Strategies adopted by your organization
- The target group for the policy
- Structure and processes of your organization

When it comes to policy content, the VeriSM™ service management approach provides three simple clear questions that your policies must answer:

1. **Why is this necessary?** Be very clear (within one sentence) as to what the policy objective is.
2. **What needs to be achieved?** Don't explain how you'll achieve this policy. The related process and/or procedures will do that (provide reference links, if available). Instead, explain the conditions of the policy—what must occur.
3. **How will I know if this is done and it works?** Define appropriate measurements to demonstrate compliance. SMART goals will help you get there.

List of critical IT policies

So, what are the most critical IT Policies? The ones your business must have? Well, each organization is different. What's critical to one may not be the same for others.

The golden rule in governance has long been that we cannot outsource oversight.

Most organizations embracing digital transformation have outsourced the need to maintain IT infrastructure and platforms—this used to take up significant policy effort. Depending on your organization's maturity, you may no longer need many I&O policies, for instance.

If you do have a cloud strategy, it's likely that your policy focus has shifted to service and data layers. This is where most interaction with technology is now happening, especially when it comes to app development. But that doesn't mean that you can neglect the underlying layers. Instead, you'll likely pivot to areas like security and billing.

(Interestingly, most modern app development approaches align to the agile manifesto, which de-emphasizes rigid processes and comprehensive documentation—two elements that are traditionally the bedrock of policies.)

When we look at standards, here's what we see. The ISO/IEC 20000:2018 standard for Service Management defines only three policies defined that any IT organization should maintain:

- Service management policy

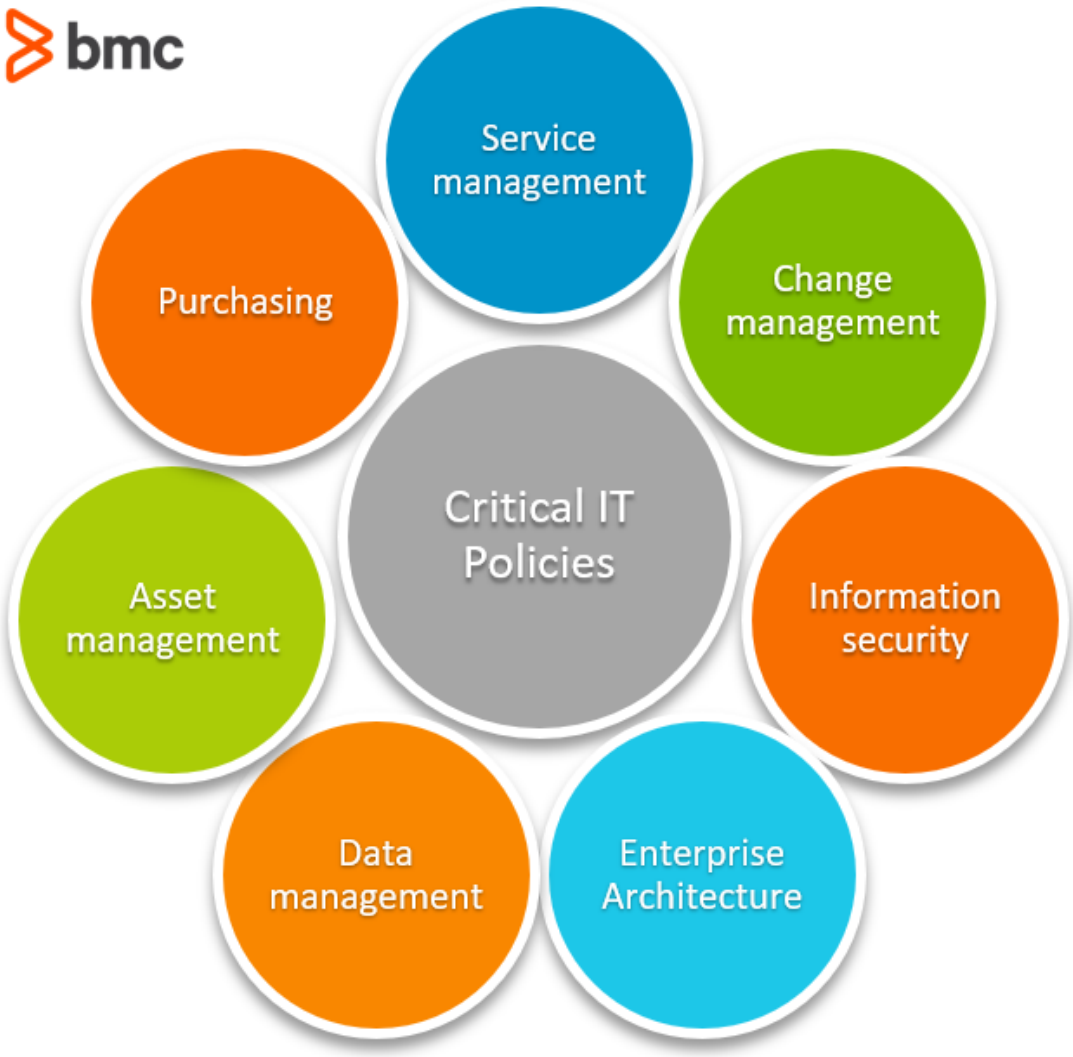
- Change management policy
- Information security policy

You might be wondering about *other* policies that seem critical.

The Info~Tech Research Group defines other policies that IT organizations need to put in place. These include:

- Enterprise Architecture policy
- Data Management policy
- Asset Management policy
- Purchasing policy

Your organization may need policy in all seven of these areas; or, maybe only four are appropriate. We'll briefly look at each one here, then point you to more resources about these practices.



Service management policy

This policy establishes the framework of setting service management objectives in line with the organization's purpose. This policy includes:

- Commitments to satisfy applicable requirements
- Commitments to continually improve the organization's service management system and

services

It is the definitive top management commitment to service management, aligning directly with ISO/IEC 20000 requirements.

Without it, there is no evidence of service management direction from the leadership, potentially leading to a disjointed approach to service management activities across the organization.

(Check out what's happening in service management today.)

Change management policy

The intention of a change management policy is to maximize the number of successful service and product changes by ensuring that you're properly assessing risk, authorizing changes to proceed, and managing the change schedule. (In ITIL 4, this policy is renamed to change enablement.)

The policy defines:

- Service components and other items that are under the control of change management
- Categories of change and how they are to be managed
- Criteria to determine changes that have potential to have a major impact on customers or services

Without this policy, risks of unplanned service disruption or bureaucratic hurdles to smooth change execution are likely to occur (exactly when you don't need them).

(Learn more about the roles involved in change management and navigating change in the cloud.)

Information security (InfoSec) policy

This policy spells out the required posture to secure the availability, integrity and confidentiality of business information on IT systems from potential risks, through appropriate controls that align with organizational and regulatory requirements.

For the most part, any Information Security policy comes with a lot of sub-policies covering different topics as per controls, including, among others:

- Risk assessment policy
- Access management policy
- Acceptable usage policy
- Password management policy
- Information classification policy
- Disaster recovery policy

With cyber security risk becoming the #1 focus for most digital organizations, absence of this policy is itself a risk. Without coordinated effort to secure data, your organization's existence is threatened if a significant attack occurs.

(Learn more about the InfoSec management and cybercrime prevention.)

Enterprise architecture policy

The Enterprise Architecture policy outlines how IT supports the business mission and operations, through alignment and prioritization of IT strategies and initiatives. It also includes guidelines for designing, planning, implementing, and governing enterprise IT architecture.

Without this policy, your organization risks increased costs and poor performance.

(Understand the role of a system architect and architecture in DevOps environments.)

Data management policy

This policy focuses on the management and governance of data assets—i.e., documents, databases, and application data files—with a strong focus on data protection and privacy.

A key data management component is the data classification policy, a formal framework for categorizing and managing data.

The heart of a data classification policy is to sort data according to its sensitivity, its value, and the impact that altering, destroying, or disclosing it to unauthorized parties would have.

Organizations can then apply the right protections based on these characteristics. Public data needs little protection, whereas more sensitive internal, confidential, and restricted data needs more protection.

Protecting data is important, but so is demonstrating compliance with regulations and security frameworks. You may need to show how you have used, managed, and protected data in adherence to legal requirements and standards. This also shows customers and partners that your systems are trustworthy.

Lastly, your data classification policy helps you efficiently use resources to reduce security risks to your data and systems. Instead of treating all data as equal, you can focus on protecting the most sensitive data.

Without this policy, you're risking the misuse, loss, regulatory penalties, or lost opportunity from data usage.

(See how data ethics and the data lifecycle can help you create data policy.)

Asset management policy

This policy provides guidelines on activities involved in the asset lifecycle, from acquisition, tagging, deployment, usage, maintenance, withdrawal, and disposal.

Absence of this policy would impact the organization financially because you're not maximizing the ROI of your assets—and you may even be taking a loss.

(Understand what assets are and explore software asset management tips.)

Purchasing policy

This policy provides guidance on acquisition of service components required for delivery of IT services, ensuring value for money and holding suppliers to their contractual commitments.

Without it, the organization can be impacted financially by poor decisions that could lead to:

- Material loss
- Litigation
- Poor third-party service delivery

(Explore cost management strategies and tips.)

Importance of an IT policy

Adopting and maintaining an IT policy ensures all employees understand the importance of cybersecurity and protecting data and systems. Moreover, it provides clear guidance on each person's responsibilities when using, managing, and securing technology.

- **Risk mitigation**: Your IT policy lowers risk to your IT infrastructure and data, engaging the entire organization in using technology properly to protect sensitive data and safeguard your digital assets against cyber threats.
- **Resource management**: Using a clear and consistent framework helps you apply resources in an efficient manner, both to protect assets and to stay compliant. The right policy supports you in focusing resources on high-value, high-risk issues.
- **Consistency and performance**: When IT resources are used properly, your organization maintains the integrity and availability of IT systems and data, protecting confidentiality and supporting your organization's goals and objectives.
- **Accountability and responsibility**: When employees know their roles in protecting IT systems, they can be held accountable for their actions and outcomes. They are motivated and empowered to act responsibly to reduce cybersecurity risks.

Choosing the right IT policies and procedures

Whether it is because of compliance with regulations, need for internal controls, operating requirements, or risk management, the need for IT policies cannot be understated.

With the ever-evolving technology landscape and the strategic drive for digital transformation, ensuring that sound policies that shepherd, not constrain, good practice are an essential ingredient of maturity and excellence for any IT outfit.

Related reading

- BMC Service Management Blog
- BMC IT Operations Blog
- Choosing IT Metrics That Matter
- What Is Digital Service Management? A Must for ITSM