**How to build a security program**

Information security programs need to:

* Establish a benchmark for security;
* Measure against that benchmark;
* Enable informed decision making; and,
* Support the execution of decisions.

### 9 Steps on Implementing an Information Security Program

BARR Advisory’s experienced team has outlined the following nine steps you can take to establish a working, future-ready information security program:

#### Step 1: Build an Information Security Team

Before you begin this journey, the first step in information security is to decide who needs a seat at the table. One side of the table holds the executive team, made up of senior-level associates responsible for crafting the mission and goals of the security program, setting security policies, risk limitations, and more. On the other side of the table sits the group of individuals responsible for daily security operations. As a whole, this group designs and builds the framework of the security program.

#### Step 2: Inventory and Manage Assets

The security team’s first job is to understand which assets exist, where those assets are located, ensure the assets are tracked, and secure them properly. In other words, it’s time to conduct an inventory of everything that could contain sensitive data, from hardware and devices to applications (both internally and third party developed) to databases, shared folders, and more. Once you have your list, assign each asset an owner, then categorize them by importance and value to your organization should a breach occur.

#### Step 3: Assess Risk

To assess risk, you need to think about threats and vulnerabilities. Start by making a list of any potential threats to your organization’s assets, then score these threats based on their likelihood and impact. From there, think about what vulnerabilities exist within your organization, categorize and rank them based on potential impact. These vulnerabilities can consist of people (employees, clients, third parties), processes or lack thereof, and technologies in place.

Look at the two lists you’ve created and find where threats and vulnerabilities may intersect, showing you where your greatest levels of risk exist. A high-impact threat with high vulnerability becomes a high risk, for example. [Contact us](https://www.barradvisory.com/contact/) if you need assistance putting together a risk analysis like this.

#### Step 4: Manage Risk

Now that you have your risks ranked, decide whether you want to reduce, transfer, accept, or ignore each risk.

* **Reduce the risk:**Identify and apply fixes to counter the risk (e.g., setting up a firewall, establishing local and backup locations, purchasing water leak detection systems for a data center).
* **Transfer the risk:** Purchase insurance for assets or bring on a third party to take on that risk.
* **Accept the risk:**If the cost to apply a countermeasure outweighs the value of the loss, you can choose to do nothing to mitigate that risk.
* **Avoid the risk:** This happens when you deny the existence or potential impact of a risk, which is not recommended as it can lead to irreversible consequences.

#### Step 5: Develop an Incident Management and Disaster Recovery Plan

Without an Incident Management and Disaster Recovery Plan, you put your organization at risk should any security incident or natural disaster occur. This includes things like power outages, IT system crashes, hacking, supply chain problems, and even pandemics like COVID-19. A good plan identifies common incidents and outlines what needs to be done—and by whom—in order to recover data and IT systems.

#### Step 6: Inventory and Manage Third Parties

Make a list of vendors, suppliers, and other third parties who have access to your organization’s data or systems, then prioritize your list based on the sensitivity of the data. Once identified, find out what security measures high-risk third parties have in place or mandate necessary controls. Be sure to consistently monitor and maintain an updated list of all third-party vendors.

#### Step 7: Apply Security Controls

You’ve been busy identifying risks and deciding on how you’ll handle each one. For the risks you want to act on, it’s time to implement controls. These controls will mitigate or eliminate risks. They can be technical (e.g., encryption, intrusion detection software, antivirus, firewalls), or non-technical (e.g., policies, procedures, physical security, and personnel). One non-technical control you’ll implement is a Security Policy, which serves as the umbrella over a number of other policies such as a Backup Policy, Password Policy, Access Control Policy, and more.

#### Step 8: Establish Security Awareness Training

Conduct frequent security awareness trainings to share your information security plan and how each employee plays a role in it. After all, new security measures and policies do nothing if employees working with the data are not educated on how to minimize risk. Any time an element of your security program changes, your employees need to be aware. And be sure to document and retain evidence of trainings for future auditing purposes.

#### Step 9: Audit, audit, audit

The best way to determine the effectiveness of your information security program is to hire a third-party auditor to offer an unbiased assessment on security gaps. In some cases, this is mandatory to confirm compliance. Third-party assessors can also perform vulnerability assessments, which include penetration tests to identify weaknesses in your organization’s networks, systems, and applications, along with audits against criteria such as [ISO 27001](http://www.iso.org/iso/iso27001), [PCI DSS](https://www.pcisecuritystandards.org/pci_security/), [FedRAMP](https://www.fedramp.gov/), and [HITRUST](https://hitrustalliance.net/); as well as SOC 2® reports using the AICPA Trust Service Principles. Your company can also conduct internal audits to assess controls, policies, procedures, risk management, and more.