IGXGlobal
An ePlus Technology, inc. Company

6 steps for creating a security program

Build a strong foundation.

COMPROMISE NOTHING

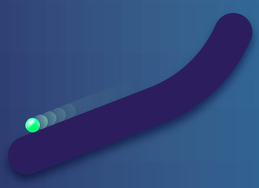
Information security is essential for protecting your organisation's data, reputation, and ability to operate. A well-designed program reduces risks, meets compliance requirements, and ensures effective response to incidents.

This guide provides six steps for creating a strong information security program.

STEP 1

Define environmental variables

A security program begins with a clear understanding of what makes your organisation unique. What factors influence your security? What legal or industry regulations — HIPAA, PCI DSS, etc. — are relevant to your organisation? What security technology do you currently use and what emerging threats do you need to guard against? What are your unique organisational attributes and attitudes regarding security and risk? Answer these questions (and more) to define the environmental variables you need to consider as you create your program.



People to involve:

- Executives (CIO, CISO, COO)
- Compliance leaders
- Legal counsel
- Human resources
- IT leadership

STEP 2

Document security requirements

Based on your organisational and environmental variables, create consolidated security requirements. Do this for all program domains: Governance, Assurance, and Operations. Establish a common language using program nomenclature so everyone in your organisation can understand and communicate on security topics.

People to involve:

- CISO
- Security specialists
- IT specialists
- IT leadership
- Compliance leaders

STEP 3

Establish a security target

With the information you now have, create a document that defines information security. This will describe your desired security state. Include sections on all elements of a security program: Leadership, Governance, Policies and Procedures, Risk Management, Security Controls, Incident Response and Recovery, Compliance and Legal Requirements, Training, Monitoring and Reporting, and Continuous Improvement. Make sure business context, organisational objectives, requirements, and business drivers are clear.

People to involve:

- Senior leadership
- Core security and IT teams
- Compliance leaders
- Human resources
- Legal
- Business unit leaders

STEP 4

Measure variance

Perform a gap analysis to determine how your current security posture compares to your desired state. Make sure the assessment addresses technology, processes, and people, and clearly communicates the results.

People to involve:

- CISO
- Core security and IT teams

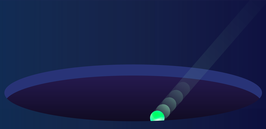
STEP 5

Build a roadmap to close gaps

Reaching your desired state may take time, depending on your current posture and specific requirements. Based on your variance assessment, create a strategic roadmap to close any gaps uncovered. Lay out a realistic timeline with estimates of resources required and other costs so your executive leadership team has a full picture of what it will take to reach your security goals.

People to involve:

- CISO
- Core security and IT teams



STEP 6

Communication and training

Once gaps are closed and your program is finalised, the last step before implementation is communication and training. Make sure all stakeholders are onboard and people are trained on your new policies and procedures.

People to involve:

- All employees

It's a team effort

An information security program is more than just policies or tools. It is a coordinated effort involving leadership, employees, and technical experts. By following these six steps, you can create an effective program aligned with your business strategy.

How strong is your security program?

Start assessment