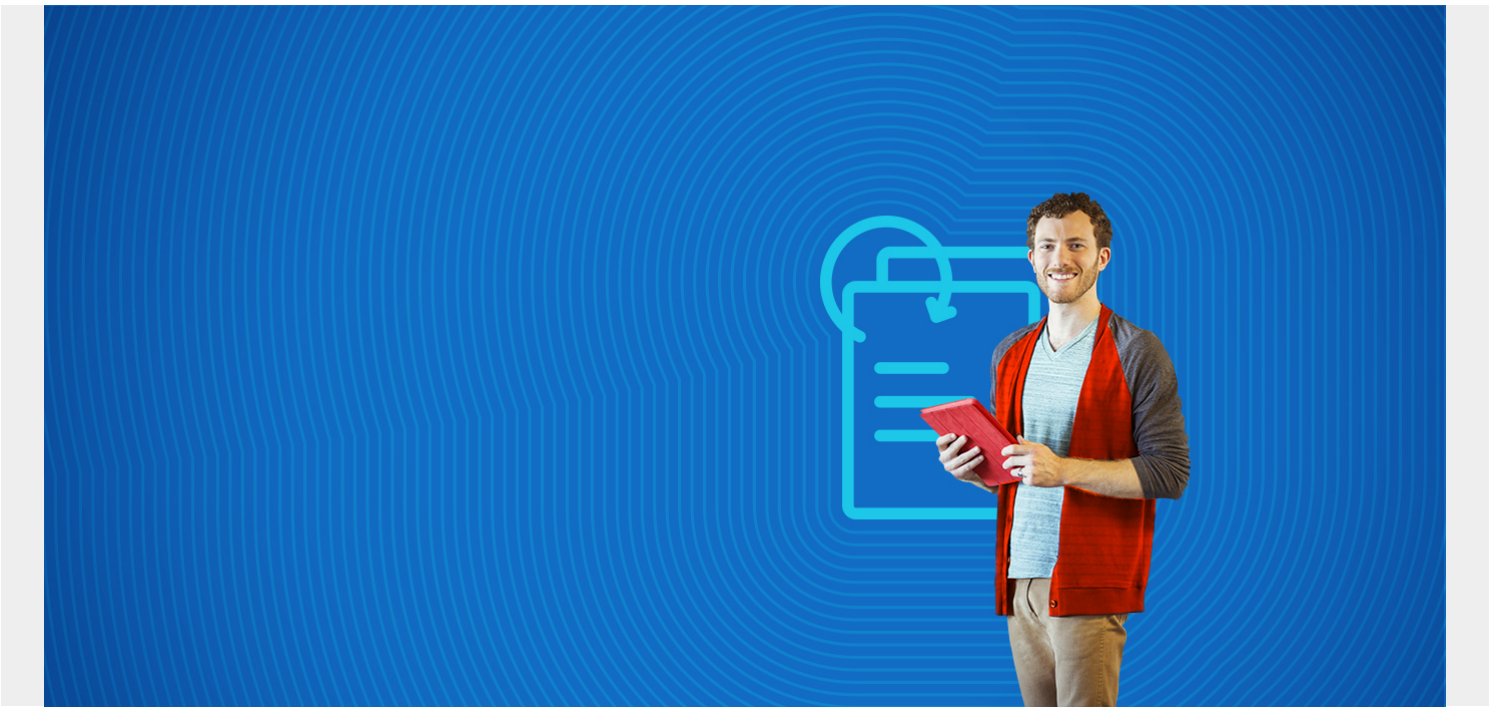
WHAT IS INFOSEC? INFORMATION SECURITY EXPLAINED



The need to secure your organization's information has gone from an operational job to a strategic imperative. After all, the digital age has anchored data as the most important asset for any entity, no matter your industry.

Because of this, many bad actors want to get their hands on your data, through hacking, social engineering, and other techniques. And with Cybersecurity Ventures expecting that the cost of cybercrime will reach $10.5 trillion annually by 2025, there is little wonder that the World Economic Forum reported cybersecurity threats and IT infrastructure breakdown as some of the highest impact global risks in this decade.

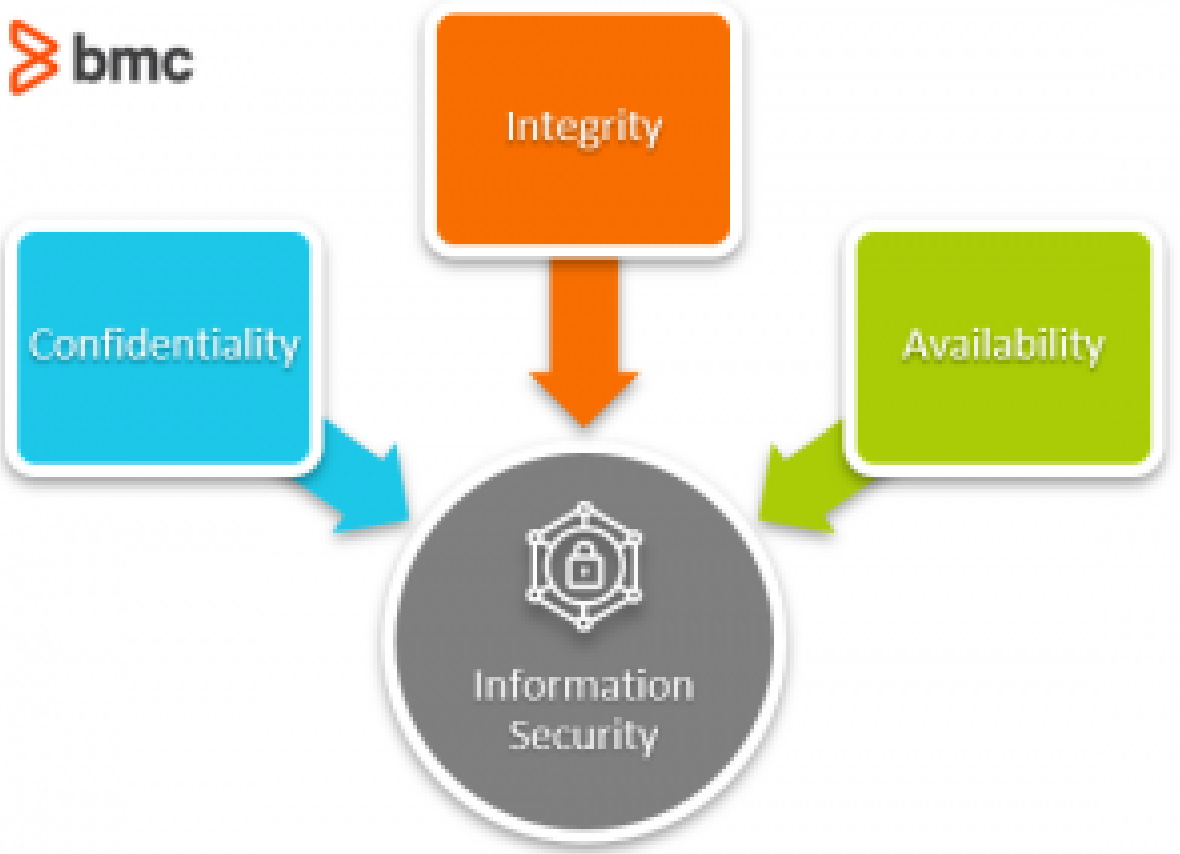
On top of that, there are the regulations on personal data protection coming with hefty fines for violations, leaving very limited options for organizations who don't see information security as a top priority.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

What is Information Security?

The ISO/IEC 27000:2018 standard defines information security as the preservation of confidentiality, integrity, and availability of information. Often known as the CIA triad, these are the foundational elements of any information security effort.

It also considers other properties, such as authenticity, non-repudiation, and reliability.



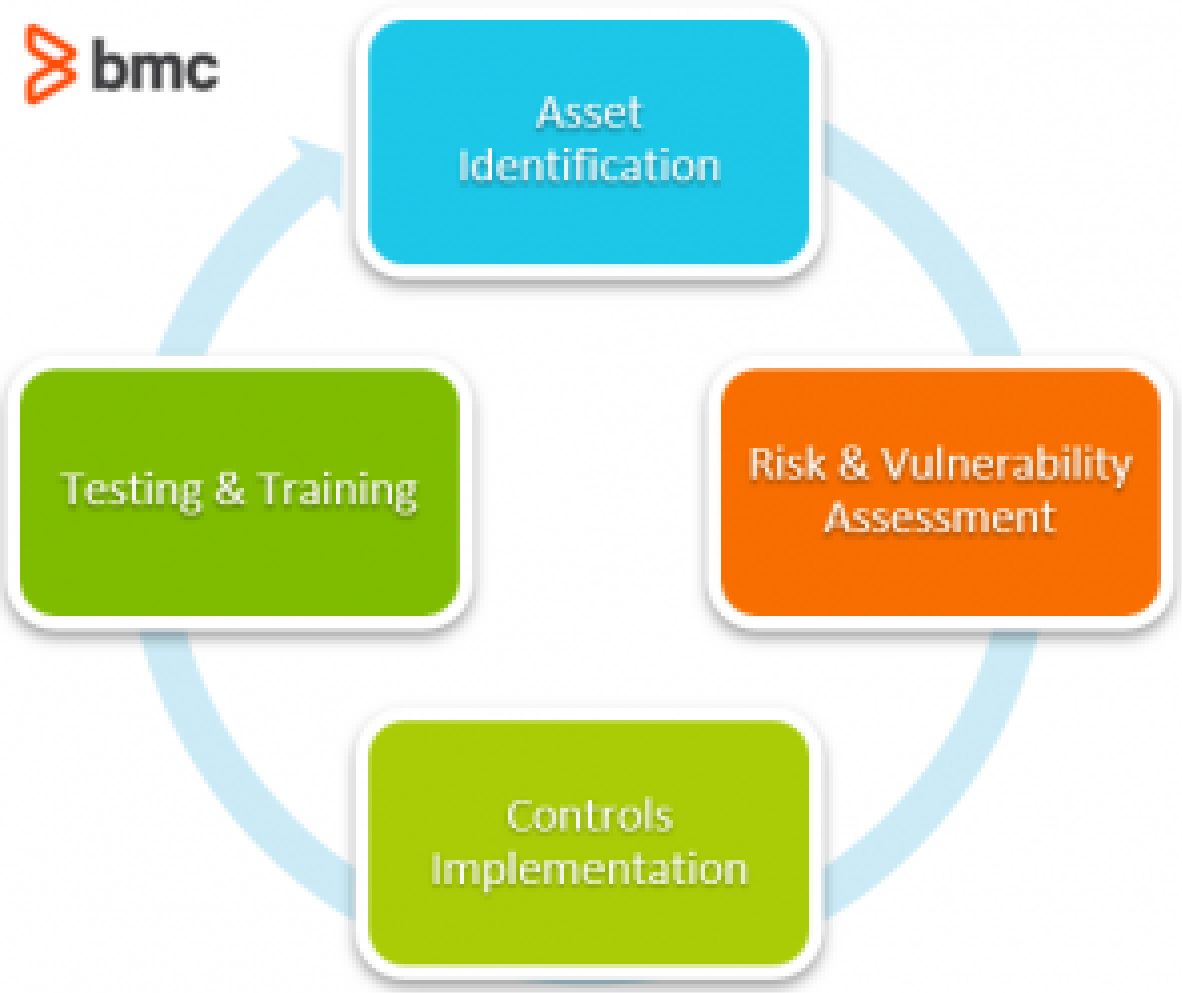
The InfoSec CIA Triad

Let's take a brief look at each property:

- **Confidentiality.** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Here, we consider that data that should only be seen by those who have the right authorization; those who don't are restricted. Think about your health records, HR payroll, or a company's strategies falling in the wrong hands.
- **Integrity.** The property of accuracy and completeness of information. Here, we do not want to find our data is different from what we expect. For example, someone adding several zeros to their bank account balance, or changing the delivery address in your e-commerce account.
- **Availability.** The property of being accessible and usable on demand by an authorized entity. If information isn't available, then the organization or its customers are hindered from achieving their objectives. For example, if you can't access your emails, or a hospital cannot access patient health records.
- **Authenticity.** The property that an entity is what it claims to be. Here, we expect a person, application, or process is exactly who or what it identifies itself to be. For example, the user Michael has logged in with his username and password or token—and it is actually Michael.
- **Non-repudiation.** The ability to prove the occurrence of a claimed event or action and its originating entities. This involves providing undeniable proof that someone did something, or something happened. This property is useful particularly for assigning responsibility for actions for instance who created or approved a transaction.
- **Reliability.** The property of consistent intended behavior and results. Here, we expect our information systems to work as they should and be able to process the data in the right way over an expected period of time. Nobody likes a system that crashes when you need it most or is too slow to suit our needs.

Implementing Information Security

The following steps can help you effectively implement information security in your organization.



1. Identifying your assets

An asset is anything that is of value to an organization, such as people, systems, processes, office buildings etc.

In information security, asset identification is all about figuring out which assets handle the data and information that is critical to the success of the organization. Of course, in the digital age, the prime assets will be computing devices, whether on-premise or cloud based.

A formal asset management process will ensure that assets are identified, documented, and ownership assigned for purposes of accountability. Identifying assets is the first point in information security management. A business impact analysis exercise can be used to identify criticality of assets and hence prioritize security efforts.

2. Assessing risk & vulnerability

Once you've identified the assets, you can then identify threats to the information contained in them. A risk and vulnerability assessment exercise will go a long way towards this effort:

- Risks are any effect of uncertainty on objectives and can be considered opportunities if positive or threats if negative.
- A vulnerability is defined as a weakness that can be exploited by one or more threats.

Risks would generally be documented in a risk register along with information such as:

- Likelihood and impact if the risk materializes
- Priority of the risk based on an agreed evaluation criteria
- Owner of the risk
- Proposed risk treatment plan
- Residual risk following the treatment

You would also document where risks are accepted by the organization in the risk register.

Vulnerabilities would be included as part of asset risk registers and would include information on how to address or contain any exploitative threats. To find public information on well-known vulnerabilities, refer to the Common Vulnerabilities and Exposures (CVE) references online.

(Learn more about risk and vulnerability assessments.)

3. Implementing controls

Once you've assessed your risks and vulnerabilities, treating the risks is the logical next step. You want to ensure the properties listed earlier are maintained.

There are three categories of InfoSec controls:

- **Physical controls.** These address risks that impact physical locations such as offices and data centers. They include gates, locks, guards, mantraps, CCTV, and biometric access passes, among others.
- **Technical controls.** These are technology centric controls that address vulnerabilities or contain risks. They include Intrusion Detection and/or Prevention Systems (IDS/IPS), firewalls, encryption, anti-malware software, and Security Information and Event Management (SIEM) solutions.
- **Administrative controls.** These are the people-centric controls which include information security policies, access rights reviews, segregation of duties, and business continuity plans, among others.

A different approach to looking at InfoSec controls is based on their position in dealing with threats that materialize. For instance:

- **Preventive controls** try to stop the threat from materializing. Examples are firewalls, access control and acceptable use policies, fences, etc.
- **Detective controls** spot a threat immediately it materializes such as CCTV, IDS/IPS and SIEM.
- **Corrective controls** reverse the impact of the materialized threats such as anti-malware software.

Organizations usually deploy multiple types of controls to cover all bases. This approach is called defense-in-depth, where layers upon layers of controls are used to limit the impact of a materialized threats or exploited vulnerabilities.

For instance, firewalls block access by malicious actors, but if penetrated, then you have a segregated network and encrypted information which is backed up in an alternate location.

4. Testing & training

Once the controls are in place, there must be a mechanism to regularly test the controls to ensure they remain effective in the face of evolving threats. This can include:

- Audit tests
- Penetration tests
- Disaster recovery tests

Results of these tests should be documented. Following review, you'll want to agree on remedial or improvement actions and then track these through to implementation.

The human firewall remains the best form of defense, and failure to keep one's staff and customers aware of information security can render the best security controls useless. A regular program to educate users on threats to information security is critical. A variety of means can be employed, such as:

- Workshops
- Online training
- Security bulletins
- Phishing tests
- And more

InfoSec is a critical policy

For any business or organization, there are a few IT policies that are absolutely critical—and InfoSec is one. Don't wait until it's too late to protect your data and information assets.

Related reading

- BMC Security & Compliance Blog
- IT Security Policy: Key Components & Best Practices for Every Business
- Introduction To Data Security
- What Is DevSecOps? Combining Development, Security & Operations
- IT Security Certifications: An Introduction
- Top IT Security, InfoSec & CyberSecurity Conferences