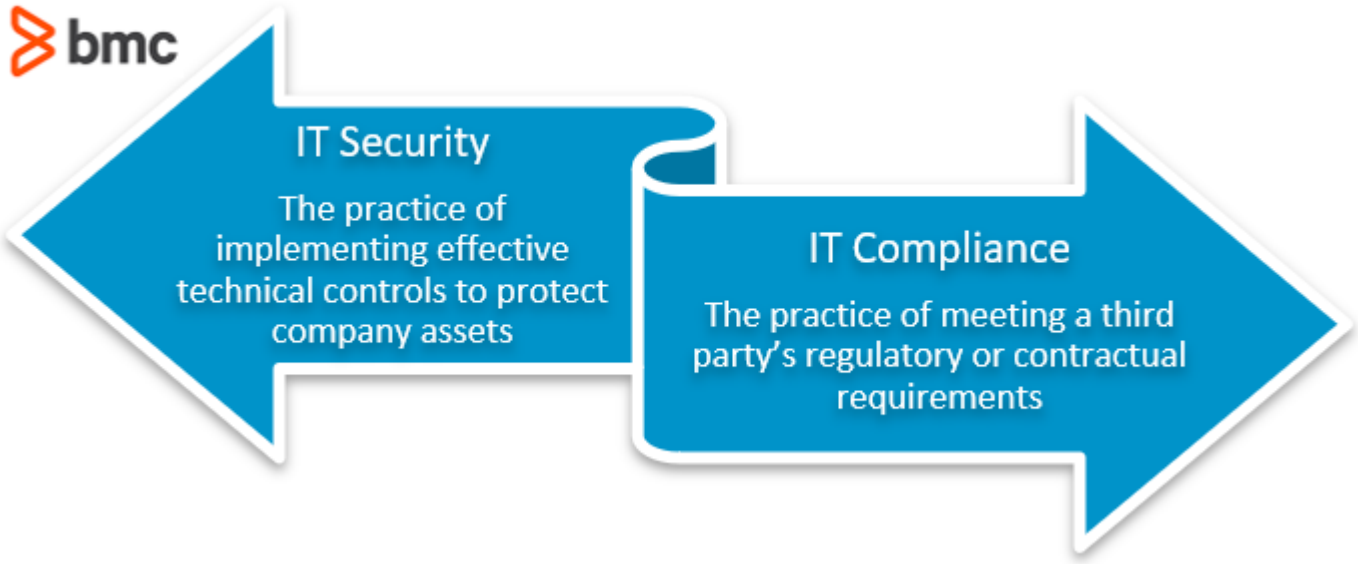
IT SECURITY VS IT COMPLIANCE: WHAT'S THE DIFFERENCE?

The line between security and compliance is easily blurred. Sometimes they feel like a moving target. Maybe you've asked yourself one of these burning questions:

- How do we create comprehensive security programs *while* meeting compliance obligations?
- Is checking the compliance box really enough?
- How does all this enable the business to function and move forward?

These questions shape the direction of an organization and ultimately cause it to succeed or fail.

So, in this article, let's clarify the differences between IT security and IT compliance.



What is IT security?

Security officers follow industry best practices to secure IT systems, especially at the organizational or enterprise level. Security pros are constantly looking at how to both:

- Prevent attackers from harming the company IT infrastructure and business data
- Mitigate the amount of damage that is done when an attack is successful

In the past, administrators would take a purely technical approach and rely heavily on systems and tools to protect their network. Today, though, things have changed.

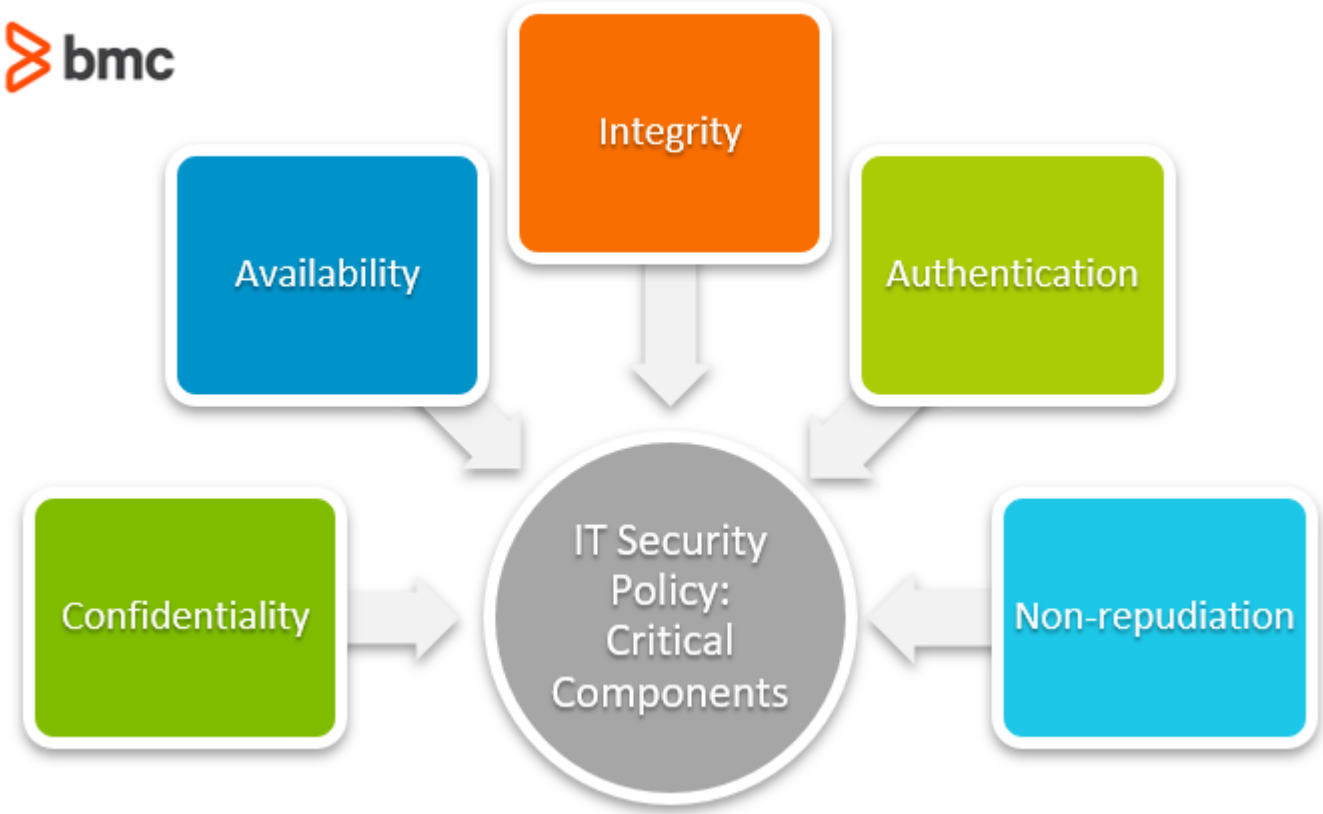
Due to increased specialization and technical know-how, IT security is not limited to a single field or discipline. Instead, there are multiple areas such as architecture and infrastructure management, cybersecurity, testing, and especially information security—arguably the most critical policy for any organization.

Information security (InfoSec) is exercising due diligence and due care to protect the confidentiality, integrity, and availability of critical business assets, something security pros know as the CIA Triad. Any IT security program must take a holistic view of an organization's security needs and implement the proper physical, technical, and administrative controls to meet those objectives.

Taking the three key functions of confidentiality, integrity, and availability, organizations can implement effective InfoSec protocols. But what does CIA actually mean?

Here are three key sections in understanding how InfoSec must be managed.

- **Confidentiality**. Company information can be sensitive information—customer data, proprietary information, innovations in the works. It is the duty of IT security to protect this information. Ensuring that only the correct and authorized user(s) and system(s) can read, change, and use data is key.
- **Integrity**. Information and the system it is contained in must be correct. Having integrity means knowing that what is stored is correct and the system has measures to ensure that.
- **Accessibility**. Systems and information need to be available when they are needed. If a system isn't available, it can't be relied on.



Two additional properties, authentication and non-repudiation, are also vital to IT security.

(Learn more in our IT security policy explainer.)

How IT security looks today

Traditionally, security professionals would rely on devices like firewalls and content filters along with network segmentation and restricted access. But as modern threat agents became more and more sophisticated, the tools that security analysts and officers have to use become more complex too.

Old-school technical controls cannot account for:

- 95% of cyber-security breaches coming from human error
- 45% coming from hacking, including technically adept threat agents exploiting vendor-created backdoors or executing remote code

Today, security professionals need to have a fuller kit of tools to battle against malicious outside threats.

The concept of IT Security comes down to employing certain measures to have the best possible protection for an organization's assets. At the heart of all good IT security protocols is the CIA triad.

(Explore the roles of Chief Information Security Officer and the security team.)

What is IT compliance?

IT compliance is the process of meeting a third party's requirements with the aim of enabling business operations in a particular market or aligning with laws or even with a particular customer.

Compliance sometimes overlaps with security—but the motive behind compliance is different. It is centered around the requirements of a third party, such as:

- Industry regulations
- Government policies
- Security frameworks
- Client/customer contractual terms

Let's say that IT security is a carrot. it motivates the company to protect itself because it is good for the company. IT Compliance, then, is the stick—failure to effectively follow compliance regulation can have serious effects on your business.

Often, these external rules ensure that a given organization can deal with complex needs. Sometimes, compliance requires an organization to go beyond what might be considered reasonably necessary. These objectives are critical to success because a lack of compliance will result in:

- At minimum, a loss of customer trust and damage to your reputation.
- At worst, legal and financial ramifications that could result in your organization paying hefty fees or being blocked from working in a certain geography or market.

Areas where compliance is a key business concern:

- Countries with data/privacy laws like GDPR, the California Consumer Privacy Act, and more
- Markets with heavy regulations, such as healthcare or finance
- Clients with high confidentiality standards

These areas almost always demand a high level of compliance. Importantly, IT compliance can apply in domains other than IT security. Complying with contract terms, for example, might be about how available or reliable your services are, not *only* if they're secure.

When is compliance necessary?

When you need to comply with certain regulations depends on many factors:

- Your industry
- Your company's size or location
- The customers you serve
- Many other factors

Many laws outline very specific criteria that a business must meet—but they don't apply to everyone. For example:

- HIPAA is a U.S. law that defines how the healthcare industry protects and shares personal health information.
- SOX is a financial regulation in the U.S. that applies to a broad spectrum of industries.
- Payment Card Industry Data Security Standards (PCI-DSS) are a group of security regulations that protect consumer privacy when personal credit card information is transmitted, stored, and processed by businesses.
- ISO 27001, on the other hand, is not a law but a standard that companies can opt into by aligning with these InfoSec standards.

Other standards you must comply might not be law or opt-in—some might originate directly with your customers. A high-profile client may require the business to implement very strict security

controls in order to award their contract.

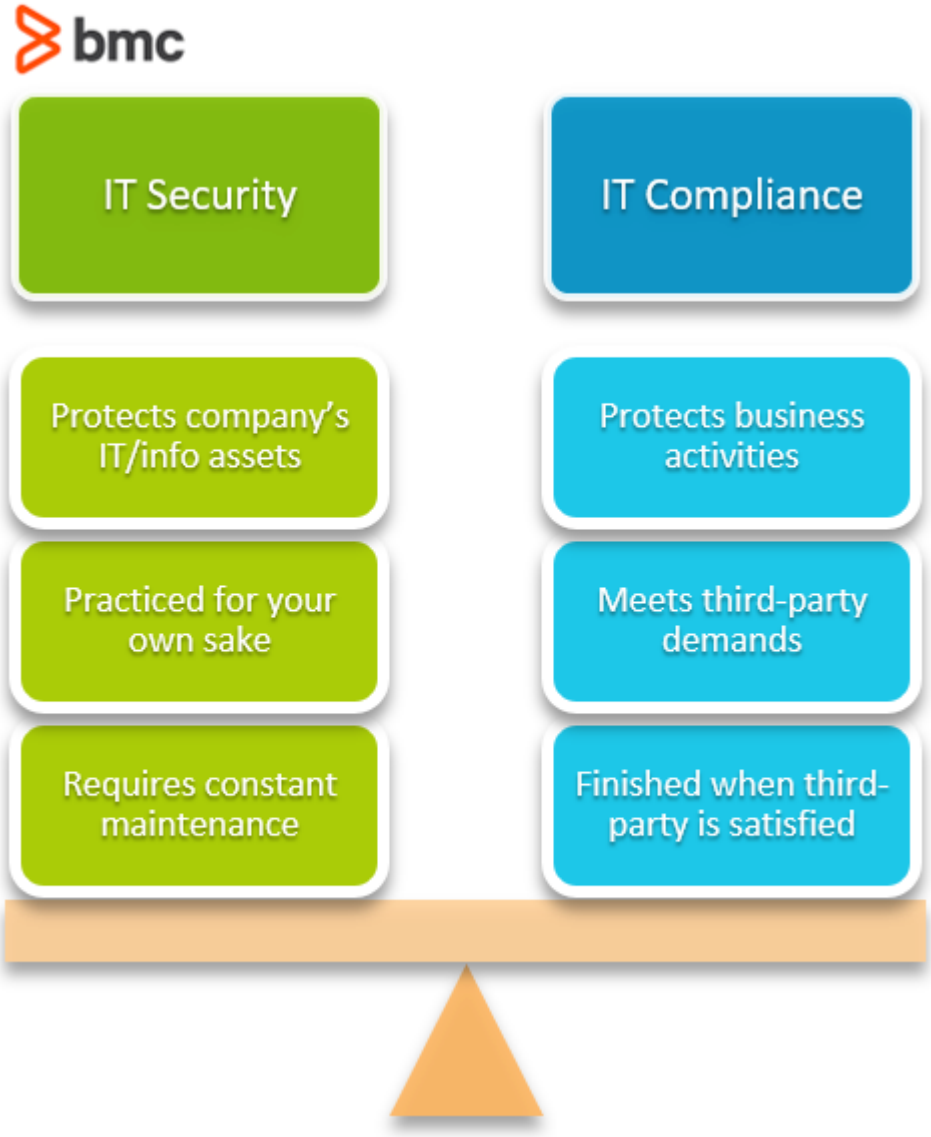
Compliance & GRC

Compliance is only one section of a greater scheme of ensuring an organization is compliant with industry, government, or other regulations. These are summed up in the acronym GRC:

- **Governance**. Before compliance is possible, organizations need to make plans that are directed and controlled. Setting direction, monitoring developments, and evaluating outcomes are all key to effective governance.
- **Risk**. Danger is everywhere and it needs to be recognized. Compliance needs for risks to be identified, analyzed, and controlled as much as is possible.
- **Compliance**. When appropriately governed and risk-managed, an organization can evaluate its compliance. Standards are not just set but evaluated and managed at every step.

Comparing IT security & IT compliance

Security is the practice of implementing effective technical controls to protect company assets. Compliance is the application of that practice to meet a third party's regulatory or contractual requirements.



Here is a brief rundown of the key

differences between these two concepts. Security is:

- Practiced for its own sake, not to satisfy a third party's needs
- Driven by the need to protect against constant threats to an organization's assets
- Never truly finished and should be continuously maintained and improved

Compliance is:

- Practiced to satisfy external requirements and facilitate business operations
- Driven by business needs (rarely technical needs)
- "Done" when the third party is satisfied

At first glance, it's easy to see that a strictly compliance-based approach to IT security falls short of the mark. This attitude focuses on doing only the minimum required in order to satisfy requirements, which would quickly lead to serious problems in an age of increasingly complex malware and cyberattacks.

How security & compliance work together

We can all agree that businesses need an effective IT Security program. Robust security protocols and procedures enable your business to go beyond checking boxes and start employing truly effective practices to protect its most critical assets.

This is where concepts like defense-in-depth, layered security systems, and user awareness training come in, along with regular tests by external parties to ensure that these controls are actually working. If a business were focused solely on meeting compliance standards that don't require these critical functions, they would be leaving the door wide open to attackers who prey on low-hanging fruit.

While compliance is often seen as doing only the bare minimum, it's useful in its own right. Compliance is an asset to the business—it isn't just hoops you must jump through. Becoming compliant with a respected industry standard like ISO:27001 can:

- Bolster your organization's reputation
- Garner new business with security-minded customers

Compliance can also help to identify any gaps in your existing IT security program which might not have otherwise been identified outside of a compliance audit. Additionally, compliance helps organizations to have a standardized security program, as opposed to one where controls may be chosen at the whim of the administrator.

Secure & comply: both business-critical

The astute security professional will see that security and compliance go hand in hand and complement each other in areas where one may fall short.

- Compliance establishes a comprehensive baseline for an organization's security posture.
- Diligent security practices build on that baseline to ensure that the business is covered from every angle.

With an equal focus on both of these concepts, a business will be empowered to not only meet the

standards for its market but also demonstrate that it goes above and beyond in its commitment to digital security.

Related reading

- BMC Security & Compliance Blog
- SecOps vs InfoSec: An IT Security Comparison
- Embracing SecOps with a BMC Helix & BMC AMI Security Integration
- The MITRE ATT&CK Framework Explained
- Top IT Security, InfoSec & CyberSecurity Conferences
- AI Cyberattacks & How They Work, Explained