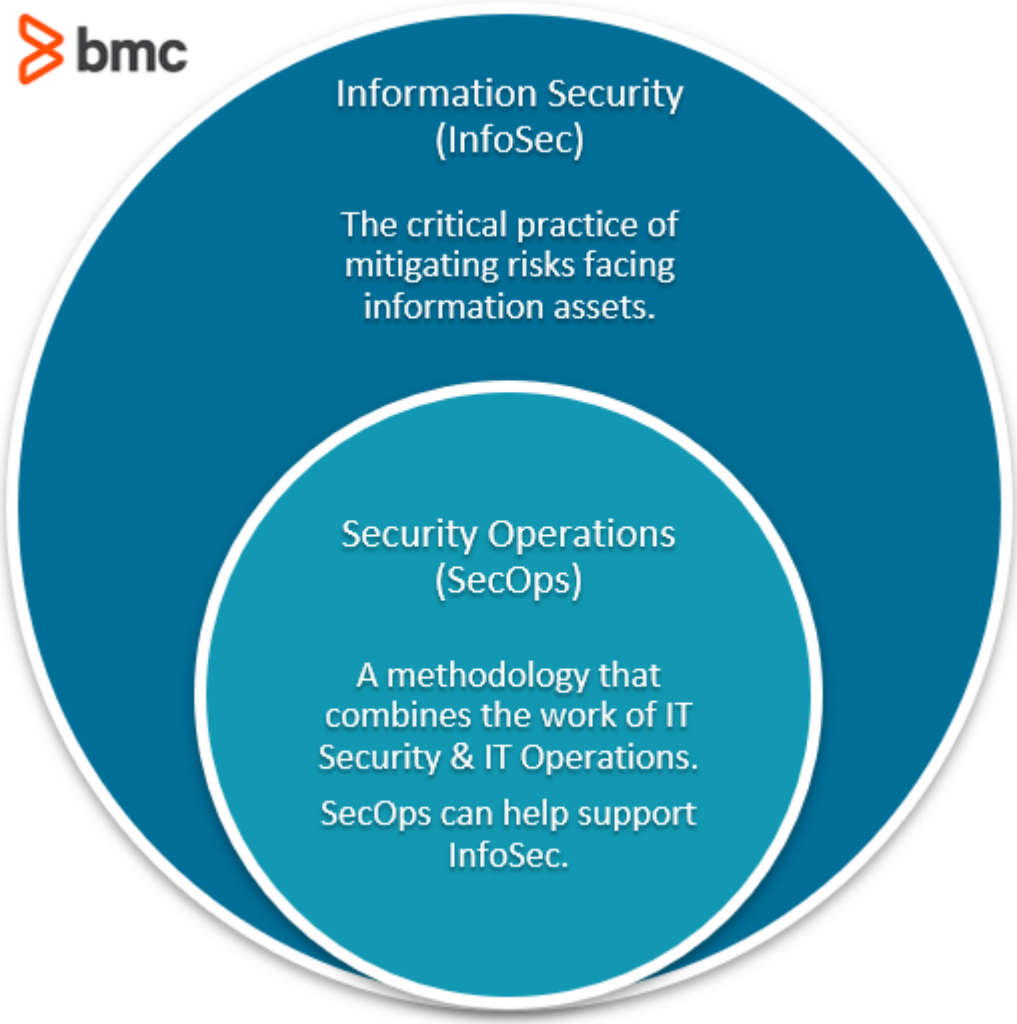
SECOPS VS INFOSEC: AN IT SECURITY COMPARISON

When it comes to IT security, SecOps and InfoSec are related but they're not the same thing. Where Information Security (InfoSec) is a critical practice for every single business, Security Operations (SecOps) is one modern approach that can help support InfoSec.

Let's take a look at today's enterprise security landscape, and we'll illustrate how InfoSec and SecOps work—and can work together.



IT security landscape today

Some of the most valuable assets of an enterprise are manifested in digital format. That's why organizations engage a variety of IT functions and roles to improve their security posture—enterprise security. They invest heavily in sophisticated tooling, security models, and operational frameworks.

Yet, cybersecurity incidents remain a common occurrence:

- 68% of organizations believe cybercrime incidents are on the rise (Accenture).
- An average data breach costs $3.86 million (IBM).
- It takes an average of 207 days since the cybersecurity incident to identify the data breach and up to 280 days to contain the damages (IBM).

And it seems that most organizations are inadequately equipped in IT Security and therefore remain vulnerable to a variety of security attacks:

- 48% of all malicious files are email attachments (Symantec).
- Only 5% of folders in corporate networks are adequately protected (Varonis).
- 40% of IT leaders believe that cybersecurity jobs are the most difficult to fill (CSO Online).

In order to address these challenges, organizations pursue operational frameworks and processes to fill gaps in their cybersecurity capabilities. These gaps can arise for several reasons:

- Lack of skills

- Insufficient security solutions
- Siloed functions of Information Security (InfoSec) and Operations teams

To fix the latter—siloed functions—the IT industry has introduced the concept of SecOps, which merges the usually separate domains of IT Security and IT Operations. SecOps takes guiding principles from the popular DevOps methodology: combining the responsibilities of development and operations teams.

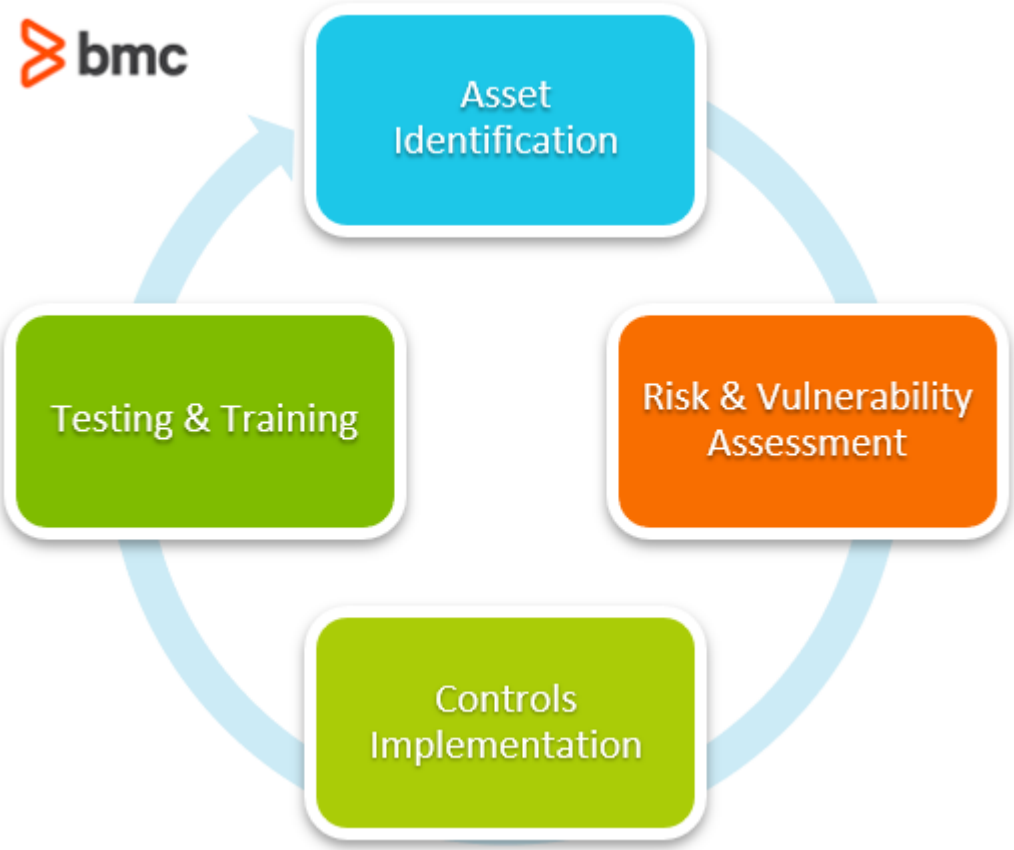
Importantly, SecOps is one approach that can support information security, but it's not the only one.

InfoSec overview

Information Security (InfoSec) refers to the discipline of mitigating risks facing information assets. It includes the technologies, practices, frameworks, and processes designed to protect sensitive business information from:

- Manipulation
- Destruction
- Unauthorized access
- Any other form of compromise

This is a typical view into the InfoSec lifecycle:



InfoSec deals exclusively with the processes designed to protect data and intellectual property that is usually in digital form. InfoSec is further classified into several categories protecting data with different processes in the security pipeline:

- **Application security** protects against vulnerabilities in software and Application Programming Interface (APIs) accessing data.

- **Cloud security** protects the data center network used to store and access data.
- **Cryptography** protects the confidentiality and integrity of information in event of unauthorized access and validates it during transmission between users.
- **Incident response** prepares an organization to defend against an active security attack or network infringement.
- **Vulnerability management** scans the IT environment for vulnerabilities and identifies risk priority for remediation efforts.

(Read more about the InfoSec practice.)

InfoSec in practice

In reality, there are several gaps in the operational workflows and functions that prevent effective InfoSec activities. Consider this example of vulnerability management in an organization managing large-scale data center or cloud network:

The security professionals run regular scans across the IT environment and generate a deluge of raw data that holds insights into vulnerabilities and risks facing every node and layer of the network. The information is then thrown over the fence to operations teams who are required to make sense of data, convert information into useful knowledge, and, finally, act upon it. Before any actions take place however, a new scan would identify more vulnerabilities, more risks, and ultimately, more requirements on deploying and managing the IT infrastructure.

IT Security and IT Operations fail to coordinate their efforts and collaborate on developing and maintaining an IT environment with security embedded from the ground up. This is where SecOps comes into play.

SecOps overview

SecOps is a methodology that combines the responsibilities and functions of IT Security and IT Operations. It integrates the technologies and processes with the aim of achieving collective goals of InfoSec and IT Ops.

Similar to DevOps, SecOps is also an approach, a mindset, and collective guiding principles that help the (otherwise siloed) teams of InfoSec and Operations to work together. A strong focus on automation, collaboration, and shared responsibility is adopted to ensure fully functional security and agile infrastructure operations.

Some key SecOps guiding principles include:

- **Common objectives.** Ensuring that the IT environment, apps, and services operate efficiently while complying with security regulations, organizational policies, and security best practices.
- **Collaboration & communication.** IT Security and Ops professionals work together using broad visibility and control into the technology, operations, and decisions.
- **Integrated tooling & automation.** a combined portfolio of tools that integrate the security and operations process to optimize both the protection of information and facilitate operational efficiency.
- **Proactive security.** Shift Left on security and develop policies that encourage IT to introduce security measures from the ground up.
- **Streamlined operations.** Improve the ability to deploy, manage, and patch infrastructure

systems. Maintain high availability and fewer compliance failures in the infrastructure environment.

With organizations readily moving their data assets and apps to the cloud, SecOps will play a key role in information security.

Related reading

- BMC Security and Compliance Blog
- IT Security Policy: Key Components & Best Practices for Every Business
- The SecOps Engineer: Role & Responsibilities
- What Is DevSecOps? Combining Development, Security & Operations
- Top IT Security, InfoSec & CyberSecurity Conferences To Attend