Cloud security functions

• 4 minutes to read •

This article provides a summary of the organizational functions required to manage information security risk in an enterprise. These roles and responsibilities form the human portion of an overall cybersecurity system.

Security is a team sport

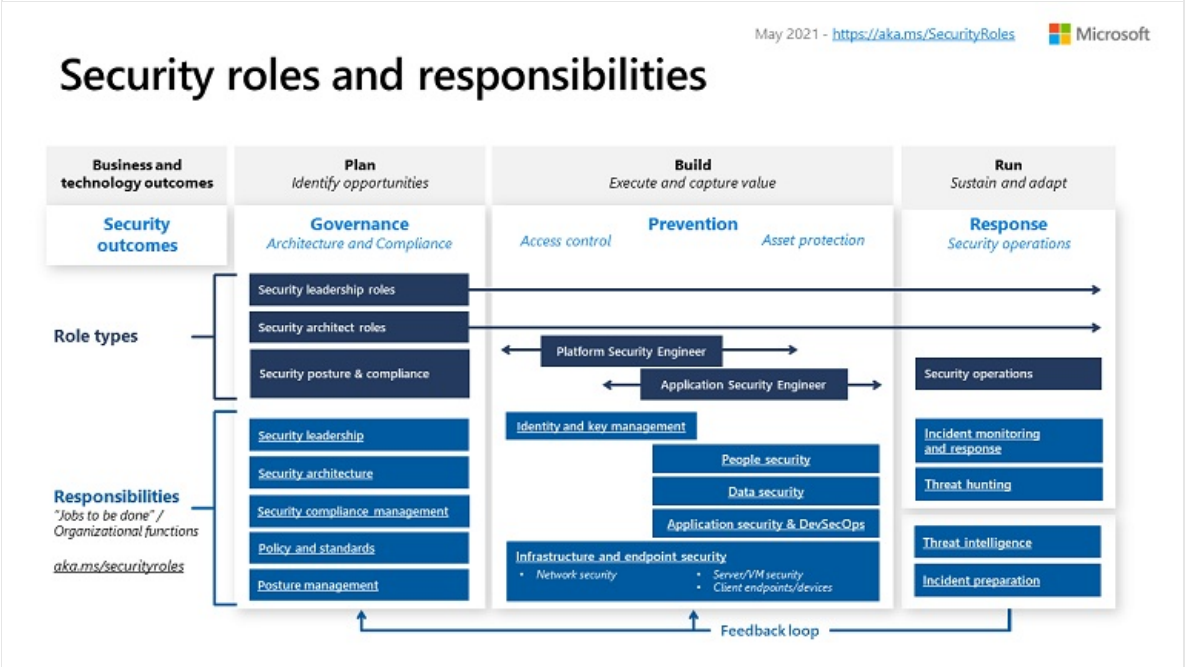
It's critical that individuals on the security team see each other as part of a whole security team, part of the whole organization, and part of a larger security community defending against the same adversaries.

This holistic worldview enables the team to work well in general. It's especially important as the teams work through any unplanned gaps and overlaps discovered during the evolution of roles and responsibilities.

Security responsibilities (functions)

This diagram depicts the specific organizational functions within security, often called responsibilities or "jobs to be done".

These diagrams and documentation represent an ideal view of a complete enterprise security team. This may be an aspirational view for security teams with limited resources that may not have formal responsibilities defined around all of these functions. Each function may be performed by one or more people, and each person may perform one or more functions depending on various factors such as culture, budget, and available resources.



Each of the following articles provides information about each function including a summary of objectives, how the function can evolve because of the threat environment or cloud technology changes, and the relationships and dependencies that are critical to its success.

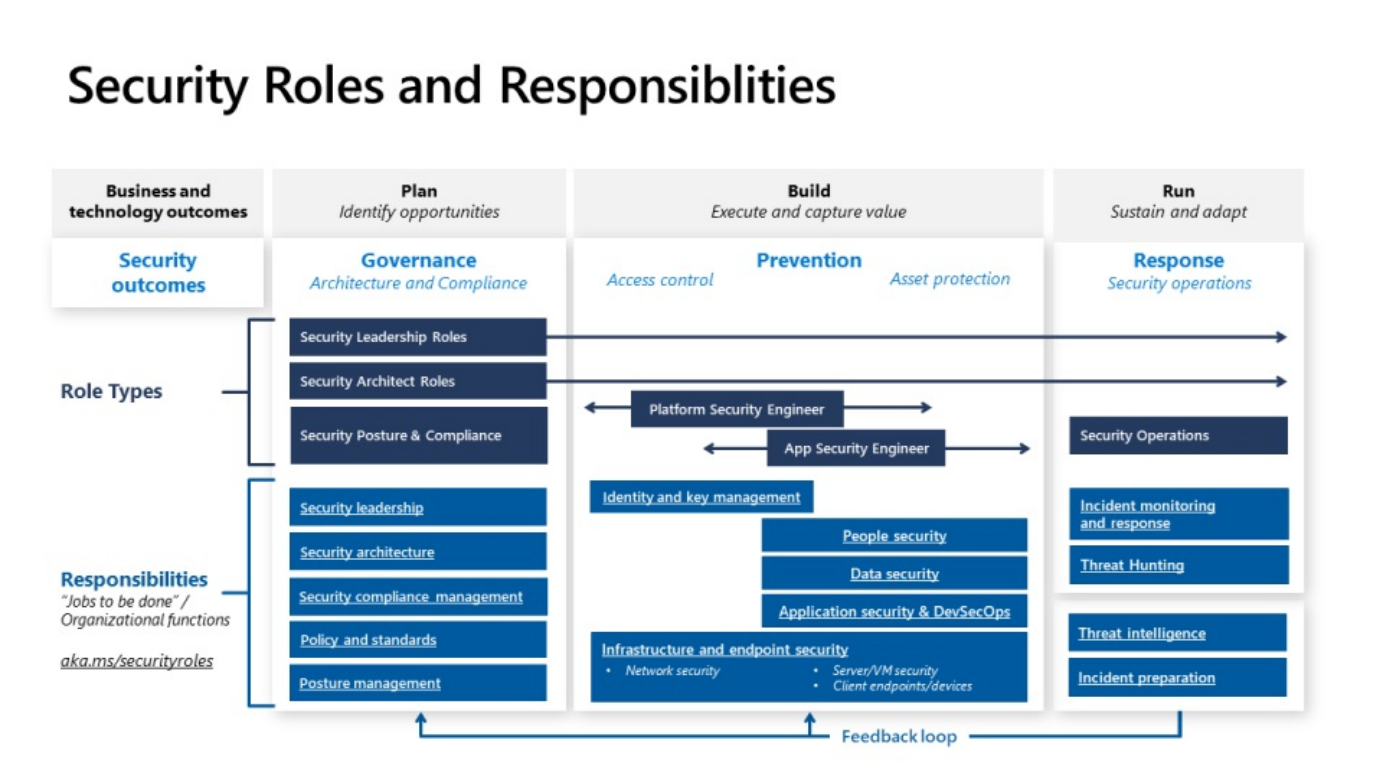
- Policy and standards
- Security operations
- Security architecture
- Security compliance management
- People security
- Application security and DevSecOps
- Data security
- Infrastructure and endpoint security
- Identity and key management
- Threat intelligence
- Posture management

- Incident preparation

These responsibilities are referenced throughout Microsoft documentation including the Azure Security Benchmark, securing privileged access: rapid modernization plan, and the Azure security top 10,

Roles and responsibilities

The following diagram depicts how these functions map to role types within an organization:



Mapping security to business outcomes

At the organizational level, the security disciplines map to standard plan-build-run phases seen widely across industries and organizations. While this cycle is accelerating into a continuous change cycle with the digital age and the advent of DevOps, this illustrates how security maps to normal business processes.

Security is both discipline with its own unique functions *and* a critical element to integrate into normal business operations.

Role types

The middle (dark blue) section groups these responsibilities into typical roles that have common skill sets and career profiles. These groupings also help provide clarity on how industry trends are affecting security professionals:

- Security leadership: These roles frequently span across functions, ensuring that teams coordinate with each other, providing prioritization and setting cultural norms, policies, and standards for security.
- Security architect: These roles span across functions and provide a key governance capability to ensure all of the technical functions work harmoniously within a consistent architecture
- Security posture and compliance: This is a newer role type that represents the increasing convergence of compliance reporting with traditional security disciplines like vulnerability management and configuration baselines. While the scope and audience are different for security and compliance reporting, they are answering different versions of the question of "how secure is the organization?". The way that question is answered is growing more similar via tools like Microsoft Secure Score and Azure Security Center:
  - The use of on-demand data feeds from cloud services is reducing the time required to report compliance.
  - The increased scope of data available is enabling security governance to look beyond traditional software updates/patches and discover/track "vulnerabilities" from security configurations and operational practices
- Platform security engineer: These are technology roles focused on platforms that host multiple workloads, focused on

both access control and asset protection. These roles are often grouped into teams with specialized technical skill sets including network security, infrastructure and endpoints, identity and key management, and others. These teams work on both preventive controls and detective controls, with detective controls being a partnership with SecOps and preventive controls being primarily a partnership with IT operations. For more information, see Security integration.

- Application security engineer: These technology roles focused on security controls for specific workloads, supporting both classic development models and modern DevOps/DevSecOps model. This is a blend of application/development security skills for unique code and infrastructure skills for common technical components like VMs, databases, and containers. These roles may be located in central IT or security organizations or within business and development teams, depending on organizational factors.

Note

As both DevOps and infrastructure as code trends progress, we expect to see some security talent migrate from platform security engineering teams to application security teams and posture management roles. This is because the DevOps model requires infrastructure security skills (such as securing the *ops* in DevOps) and governance teams will also require these skills and experience to effectively monitor technical security posture in real time. Additionally, infrastructure as code will automate repetitive manual technical tasks, reducing the volume of time required for these skills in the platform security engineer roles (though increasing the need for broad technical skill sets and automation or scripting skills).

Next steps

Review the Secure methodology