# Cloud security stakeholders

So far, you've learned about a cloud security analyst's role and responsibilities, and how they function within cloud teams. You've also learned that the security ecosystem includes a variety of different roles, like cloud security architects, engineers, analysts, and compliance specialists. The security ecosystem also includes stakeholders, or people or organizations who can affect or be affected by a system. Stakeholders include leadership and upper management who need to be involved in security decisions for organizations.

In this reading, you'll explore different types of stakeholders, and how you might engage with them on the job.

## Stakeholder types

In cloud security, stakeholders involve a variety of different roles. A cloud security analyst's ability to effectively communicate with diverse stakeholders is an important aspect of the job.

### Leadership figures

It's important that cloud security analysts can communicate effectively with leadership figures. Leadership figures might include Chief Executive Officers (CEOs), Chief Financial Officers (CFOs), Chief Technology Officers (CTOs), and upper management. The leader in charge of security governance is called the Chief Information Security Officer (CISO). When security incidents happen, analysts can share important information with their managers by writing status reports, or speaking at team meetings.

### Other employees at your organization

Analysts also need to know how to communicate technical security information to colleagues who might not have a technical background. This skill is especially important in the event of security breaches or threats.

For example, imagine a security team is dealing with a phishing attack that's targeting employee emails. Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software. The team is already tracking the source of the phishing attack, but they urgently need to communicate this threat to other employees in the organization. The security team decides to send a company-wide email that explains what the phishing email looks like, and the steps to take if an employee has become a target. The email also describes how to detect phishing attempts in the future as a way to help educate colleagues.

Analysts should be able to convey technical information in a simplified way to colleagues when necessary, and answer questions as they arise.

### Compliance

It's likely that analysts will collaborate with compliance teams in the workplace. Compliance teams are specifically interested in how software complies with industry standards and legal requirements. So, it's important for cloud security analysts to have an awareness of how industry standards and legal requirements impact security architecture. Analysts need to know the security controls in place that enforce compliance, and how to communicate this information with compliance teams. For example, one communication tool analysts can use to communicate is an internal audit report. In an audit report, analysts identify controls that impact legal requirements, and discuss the strengths or improvements needed to enhance security posture.

### End users

Cloud security analysts must be able to communicate about technical incidents that could impact end users, like security breaches or threats. While analysts usually don't communicate directly with end users, they do provide context for the teams that do, like public relations (PR). For example, if a vulnerability is detected in an application, the security team might patch the issue or deploy a new version of the application. Then, analysts can provide the PR team with a high-level overview of the incident, how it was fixed, and what actions end users should take. The PR team uses this information to notify end users, keeping the community safe.

Organizations should have transparent security policies that end users can access to stay well informed about potential threats and risks, including their own devices.

## Key takeaways

It's important that cloud security analysts can communicate with stakeholders and meet their needs regularly. The style of communication and level of detail will vary based on the type of stakeholder. Communicating with stakeholders is an integral part of a cloud security analyst's job, so it's important to understand the different ways analysts interact with different audiences.