**What does an IT security manager do?**

This strategically important role compromises nine key responsibilities:

1. **Monitor all operations and infrastructure.** This could be something you do by yourself, or you could be leading a team — either way, your daily bread and butter involves going through alerts and logs (the computer security equivalent of video surveillance) in order to keep an eye on your organization’s digital security footprint.
2. **Maintain all security tools and technology.** This could be a shared responsibility or the sole responsibility of the IT security manager and their team.
3. **Monitor internal and external policy compliance.** You want to ensure that both your vendors and employees understand your cybersecurity risk management policies and that they operate within that framework. The IT security manager is the living embodiment of policy, and while you may not always be in charge of enforcement, you are responsible for making sure things are in line internally.
4. **Monitor regulation compliance.** This is particularly important if you’re in a heavily regulated industry and are dealing with things like credit card information, health care data, or other personally identifiable information.
5. **Work with different departments in the organization to reduce risk.** From technical controls to policies (and everything in between), you’ll likely be tasked with working across the aisle of departments in your organization to get everyone on the same page.
6. **Implement new technology.** If your organization is looking at a new technology, you must evaluate it and help implement any controls that might mitigate the risk of its operation.
7. **Audit policies and controls continuously.** Cybersecurity is a circular process, and as a manager, you must drive that process forward. This means regularly auditing the policies and controls you put into place. These audits will tell you if there’s anything you need to improve, remediate, or quickly fix.
8. **Ensure cybersecurity stays on the organizational radar.** Does it seem as though the organization you’re with isn’t being proactive about cybersecurity? As the IT security manager, your job is to make the benefits clearly visible and champion all efforts going forward.
9. **Detail out the security incident response program.** Every organization should have a well-defined and documented plan of action to put into place if a security incident does occur.

As the IT security manager, it is your responsibility to ensure that this program is tested throughout the organization and that every high-level manager knows his or her duties during such an incident. This may be a responsibility that is the IT security manager’s alone, or it could be a shared responsibility.