MARCH, 2023

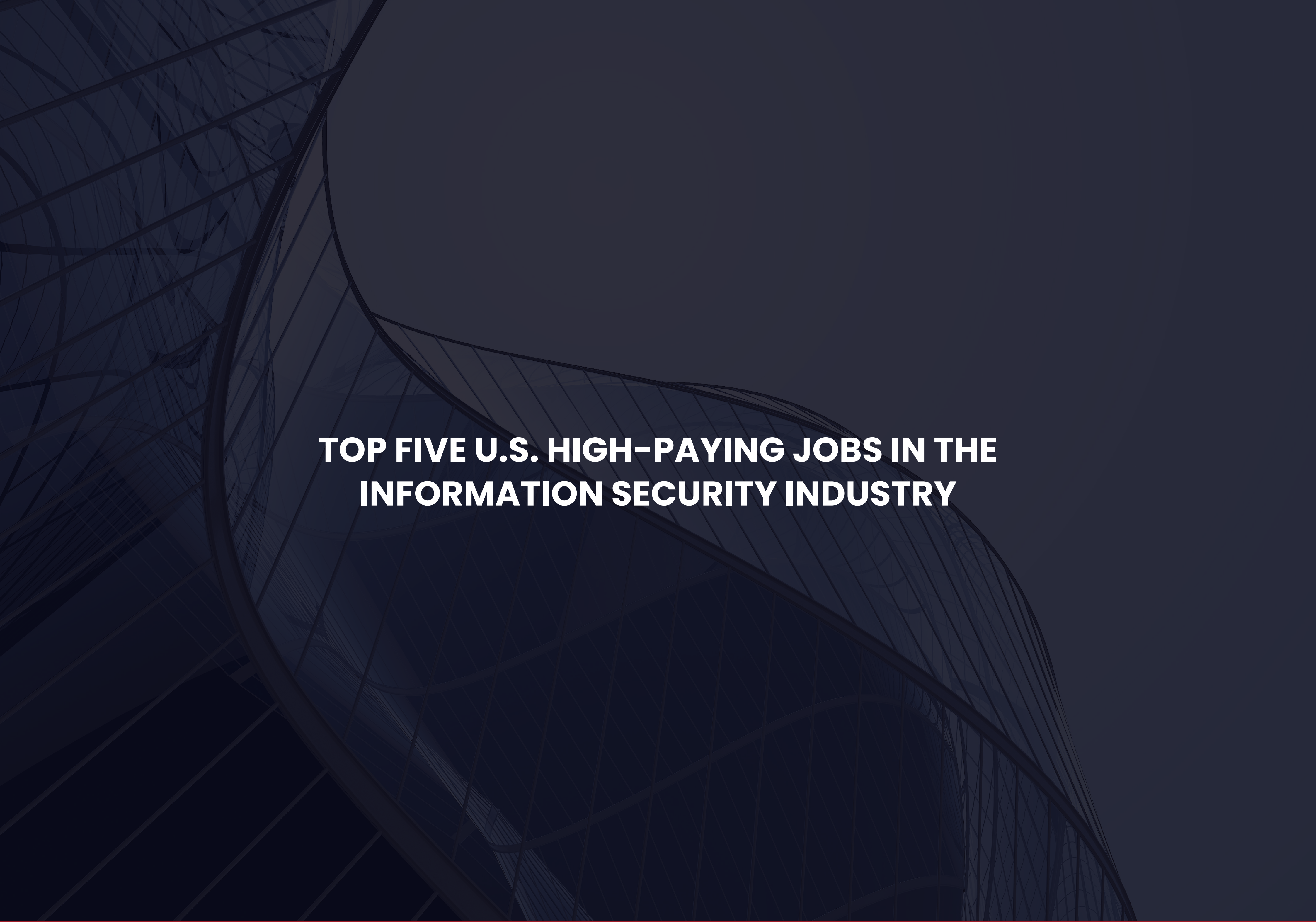
Top Five High-Paying Job Positions You Can Pursue with an ISO/IEC 27005 Certification

PECB

Advanced technology has had a profound impact on information security. On one hand, it has provided new opportunities for improving security, such as the use of encryption, firewalls, and intrusion detection systems. On the other hand, it has also created new threats, such as cyber-attacks, malware, and social engineering that take advantage of vulnerabilities in technology systems. The increasing interconnectedness of devices, networks, and systems has made it easier for attackers to gain access to sensitive information, and for malicious software to spread quickly from one device to another.

To mitigate these risks, organizations are investing to stay up-to-date with the latest security technologies and best practices, as well as regularly assess and update their security posture. According to Statista, by the year 2024, the global market size for information security is expected to reach approximately US $175 billion. Information security is critical in protecting assets and maintaining confidentiality, integrity, and availability of data.
Such protection can be achieved by following
and implementing frameworks or standards such as
ISO/IEC 27005.

ISO/IEC 27005 is an international standard for information security, cybersecurity, and privacy protection. It provides guidance on implementing and fulfilling ISO/IEC 27001 requirements and performing information security risk management activities. The standard covers areas such as risk assessment, risk treatment, and risk management processes.



TOP FIVE U.S. HIGH-PAYING JOBS IN THE INFORMATION SECURITY INDUSTRY

1. Information Security Manager

According to Salarycom, the average U.S. annual salary of an Information Security Manager is **US $145,366**.

An Information Security Manager is responsible for ensuring the confidentiality, integrity, and availability of an organization's information and systems. Their specific responsibilities may vary depending on the size and nature of the organization, but common tasks include:

- ✓ Developing and implementing information security policies, procedures, and standards.
- ✓ Conducting risk assessments and implementing controls to mitigate information security risks.
- ✓ Identifying, monitoring, and managing emerging security threats or incidents.
- ✓ Ensuring compliance with relevant laws and regulations, such as data protection and privacy laws.
- ✓ Managing the information security budget and resources.
- ✓ Educating employees and stakeholders about information security best practices and policies.
- ✓ Keeping up-to-date with the latest security technologies, trends, and threats.
- ✓ Developing and maintaining relationships with stakeholders, including business partners and suppliers, to ensure the effective management of information security risks.

An Information Security Manager needs a combination of technical, managerial, and communication skills. In addition to having an understanding of information security technologies, protocols, and best practices, they need to have the ability to assess and manage information security risks, have knowledge of relevant laws and regulations, ability to lead a team, and have strong communication and interpersonal skills.

2. Data Privacy Manager

Based on information gathered from Salarycom, the average U.S. annual salary of a Data Privacy Manager is **US $126,000**.

A Data Privacy Manager is responsible for overseeing and ensuring compliance with data protection and privacy regulations and policies within an organization. Their specific responsibilities may vary depending on the size and nature of the organization, but common tasks include:

- ✓ Developing and implementing data privacy policies and procedures, including data protection and privacy by design.
- ✓ Conducting privacy impact assessments (PIAs) and ensuring that privacy considerations are integrated into the development of new products and services.
- ✓ Monitoring and responding to data privacy incidents, including investigations and reporting.
- ✓ Ensuring compliance with relevant laws and regulations.
- ✓ Providing training and awareness to employees and stakeholders on data privacy best practices and policies.
- ✓ Keeping up with the latest data privacy developments and trends, including updates to privacy laws and regulations.
- ✓ Developing and maintaining relationships with stakeholders.

Data privacy managers need a variety of skills, mostly categorized into three main categories: technical, legal, and communication skills. They need to understand data privacy laws and regulations such as GDPR and CCPA or other relevant regulations, have the ability to assess and manage data privacy risks, have strong verbal and written communication skills, ability to build and maintain relationships with stakeholders, etc.

3. Information Risk Manager

According to Salarycom, the average U.S. annual salary for Information Risk Managers is **US $121,729**.

An Information Risk Manager is responsible for assessing, mitigating, and managing information security risks within an organization. Some of the main responsibilities of an Information Risk Manager include:

- ✓ Regularly conducting risk assessments, developing mitigation strategies to address risks, and communicating them to senior management, stakeholders, and employees.
- ✓ Developing, implementing, and maintaining risk management policies and procedures that align with the organization’s information security objectives.
- ✓ Monitoring compliance with information security policies, standards, and regulations, and taking appropriate action to resolve matters of non-compliance.
- ✓ Working with other departments and stakeholders to ensure that information security risks are effectively managed across the organization.
- ✓ Staying informed about the latest information security risks, threats, and mitigation strategies.
- ✓ Managing security incidents, leading the response to information security incidents, and ensuring that appropriate actions are taken to contain and resolve the incident.

It is necessary for information risk managers to understand information security technologies, risks, and mitigation strategies. Furthermore, they should be familiar with risk management methodologies, and be able to adapt to changing security environments by staying up-to-date on the latest security technologies, trends, and threats.

4. Information Security Consultant

As reported by Salarycom, the average U.S. annual salary of an Information Security Consultant is **US $105,031**.

An Information Security Consultant is responsible for providing expert advice and guidance to organizations on information security best practices and strategies. Their specific responsibilities may vary depending on the size and nature of the organization, but common tasks include:

- ✓ Assessing the organization's current information security posture and identifying areas for improvement.
- ✓ Developing and recommending information security policies, procedures, and standards.
- ✓ Conducting security audits and risk assessments, and developing plans to mitigate identified risks.
- ✓ Advising on the selection and implementation of information security technologies and solutions.
- ✓ Providing training and awareness to employees and stakeholders on information security best practices and policies.
- ✓ Keeping up with the latest security technologies, trends, and threats.
- ✓ Providing support during security incidents and investigations.
- ✓ Collaborating with other departments and stakeholders to ensure the effective management of information security risks.

In addition to extensive knowledge of information security technologies, information security consultants must be able to assess and manage information security risks, be able to manage multiple projects, communicate effectively, and have analytical and problem-solving skills.

5. Information Security Officer

According to Salarycom, the annual average U.S. salary of Information Security Officers is **US $92,505**.

An Information Security Officer is responsible for overseeing and managing the information security program within an organization. Some of the main responsibilities include:

- ✓ Developing and implementing information security policies, procedures, and standards that align with the organization's information security objectives.
- ✓ Regularly conducting risk assessments to identify potential information security risks, and developing mitigation strategies to address these risks.
- ✓ Monitoring compliance with information security policies, standards, and regulations, and taking appropriate action to address any non-compliance issues.
- ✓ Leading the response to information security incidents and ensuring that appropriate actions are taken to contain and resolve the incident.
- ✓ Keeping up with the latest information security risks, threats, and mitigation strategies.
- ✓ Communicating information security risks and mitigation strategies to senior management, stakeholders, and employees.
- ✓ Overseeing the security of information technology systems, including hardware, software, and data.
- ✓ Providing guidance and direction to the organization on information security matters, and ensuring that information security is integrated into all business processes.

Information security officers require a strong knowledge of information security technologies and experience with risk management methodologies. They should have the ability to provide guidance and direction to the organization on information security-related matters. Furthermore, they need to have interpersonal skills, be adaptable, and possess strategic thinking.

The PECB ISO/IEC 27005 training courses are designed to provide individuals with the knowledge and skills for the implementation of an information security system that is based on a risk management approach.

Note: The salaries of the above-mentioned positions are not definitive and they may change with time and industry development.

CLICK HERE TO SEE HOW PECB CAN HELP

→

☎ +1-844-426-7322

✉ support@pecb.com

🌐 www.pecb.com

PECB