Summary As you have seen, the nature of international laws, standards, and regulations make cloud computing complex and at times difficult to comprehend. The International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Organization for Economic Cooperation and Development (OECD) have promulgated what have become the de facto standards for information security and privacy for the vast majority of the international community outside the United States. Inside the United States, auditors still work primarily with standards and regulations such as GLBA, PCI DSS, SSAE 18, and HIPAA. Agencies and governmental bodies continually generate these standards and regulations, making a consistent standard difficult to obtain. However, it is the CCSP's responsibility to understand all the challenges these present in order to provide sound advice when working with customers' and vendors' architectural, policy, and management efforts. **Exam Essentials Explain the different sources of law in the United States.** Federal statutes are created by the legislative branch, after passing both houses of Congress and obtaining the signature of the president. The executive branch may create administrative law to assist in the interpretation and enforcement of statutes. The judicial branch reviews, applies, and interprets both legislative and administrative law, creating a body of case law. **Explain the difference between criminal and civil liability.** Liability is what allows one party to take action against another party in court. Criminal liability occurs when a person violates a criminal law. If a person is found guilty of a criminal law violation, they may be deprived of their liberty through imprisonment. Civil liability occurs when one person claims that another person has failed to carry out a legal duty that they were responsible for fulfilling. **Describe the four elements of the tort of negligence.** Negligence is a commonly occurring tort that occurs when one party causes harm to another party by their action or lack of action. The theory of liability for negligence involves four elements. First, there must be a duty of care. Second, there must be a breach of that duty of care. Third, there must be damages involved, and fourth, there must be causation. **Explain the chain of custody.** When gathering forensic evidence for possible use in court, investigators must document how and when they collected the evidence and every time someone handles the evidence between collection and presentation in the courtroom. This is known as documenting the chain of custody to demonstrate that evidence was properly managed at all times. **Understand the purpose of e-discovery.** When an organization is subject to a lawsuit, it must preserve any records related to the matter at hand. Electronic discovery e-discovery programs provide a process and mechanism for collecting and retaining that information. In cloud environments, eDiscovery may be guided by ISO 27050 and guidance from the Cloud Security Alliance (CSA). **Describe the types of sensitive information.** Organizations may handle many types of sensitive information in the cloud. This includes information about individuals, known as personally identifiable information (PII). It also includes information about healthcare, known as protected health information (PHI), and payment card information. **Explain the major laws that govern security and privacy in the cloud.** Security and privacy efforts in the cloud are subject to many different laws and regulations. Healthcare organizations are subject to the Health Insurance Portability and Accountability Act (HIPAA). Financial institutions are subject to the Gramm–Leach–Bliley Act (GLBA). Publicly traded companies are subject to the Sarbanes–Oxley Act (SOX). Organizations doing business in the European Union are subject to the General Data Protection Regulation (GDPR).