CCSP

CCSP EXAM CRAM

EXAM PREPARATION SERIES

2023 EDITION

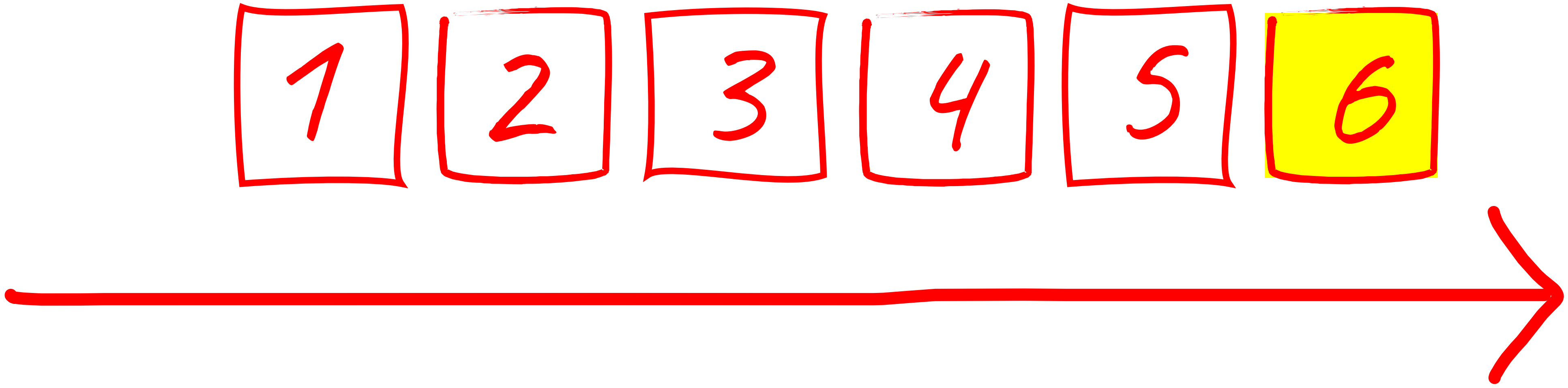
DOMAIN 6

Coverage of every topic in the official exam syllabus!

with **Pete Zerger** vCISO, CISSP, MVP

INTRODUCTION: SERIES OVERVIEW

LESSONS IN THIS SERIES



One lesson for each exam domain

...and a consolidated full course video when the series is complete

EXAM OBJECTIVES (DOMAINS)

DOMAIN	WEIGHT
1. Cloud Concepts, Architecture, and Design	17%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	16%
6. Legal, Risk, and Compliance	**13%**

Domain 6 is the focus of this video

(ISC)²
CCSP
Certified Cloud Security Professional
Official Study Guide
Third Edition
OFFICIAL
SYBEX

EXAM ESSENTIALS - 6

Explain different sources of law in the United States

Administrative law, common law, case law, regulations, jurisdiction.

Explain difference between criminal and civil liability

Criminal liability is a breach of law, civil liability a failure in fulfilling responsibilities (due care).

Know the four elements of the tort of negligence

1) Duty of care, 2) Breach of duty, 3) Damages, 4) Causation.

Explain chain-of-custody

End-to-end documentation of evidence, means of collection, and proper handling at all times.

Know purpose of e-discovery

Preservations of records related to subject of a lawsuit. Role of ISO 27050, CSA guidance.

Describe sensitive info types

Personally identifiable info (PII), Protected health info (PHI), payment card information.

Major laws that govern security and privacy in the cloud

Laws and regulations including HIPAA, GLBA, SOX, and GDPR.

EXAM ESSENTIALS - 6

Know the elements of policy frameworks

They consist of policies, standards, procedures and guidelines.

Common policies used in an org’s security program

Acceptable use, data roles & ownership, data retention, and account management.

How vendors are a source of external security risk

Importance of internal assessment of systems, due diligence in vendor review to reduce risk.

Risk management strategies an organization may adopt

Risk mitigation, risk avoidance, risk transference, risk acceptance.

5. CLOUD SECURITY 6. LEGAL, RISK AND COMPLIANCE

6.1 Articulate Legal Requirements and Unique Risks within the Cloud Environment

Conflicting international legislation

Evaluation of legal risks specific to cloud computing

Legal framework and guidelines

eDiscovery
(e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27050, Cloud Security Alliance (CSA) Guidance)

Forensics requirements

CONFLICTING INTERNATIONAL LEGISLATION

It is important to be aware of the various laws and regulations that govern cloud computing.

Laws can introduce risks to a business, such as fines, penalties, or even a loss of the ability to do business in a certain place.

It is important to identify such risks and make recommendations to mitigate them just like any other risk.

EXAMPLE

Conflict with GDPR and CLOUD Act

GDPR forbids the transfer of data to countries that lack adequate privacy protections

The **Clarifying Lawful Overseas Use of Data (CLOUD) Act** requires CSPs to hand over data to aid in investigation of serious crimes, even if stored in another country.

Which law prevails when the two are in conflict?

CONFLICTING INTERNATIONAL LEGISLATION

It is important to be aware of the various laws and regulations that govern cloud computing.

Laws can introduce risks to a business, such as fines, penalties, or even a loss of the ability to do business in a certain place.

It is important to identify such risks and make recommendations to mitigate them just like any other risk.

EXAMPLE

Conflict with GDPR and CLOUD Act

As with many aspects of security, legal compliance requires collaboration.

Legal counsel should be part of the evaluation of any cloud-specific risks, legal requests, and the company's response to these.

The consumer is responsible for navigating these challenges

Encryption and Privacy

Computer Export Controls. US companies can't export to Cuba, Iran, North Korea, Sudan, and Syria.

Encryption Export Controls. Dept of Commerce details limitations on export of encryption products outside the US.

Privacy (US). The basis for privacy rights is in the Fourth Amendment to the U.S. Constitution.

Privacy (EU). General Data Protection Regulation (GDPR) is not a US law, but very likely to be mentioned!

Applies to any company with customers in the EU!

CONFLICTING INTERNATIONAL LEGISLATION

Cloud practitioners must be aware of multiple sets of laws and regulations and the risks introduced by conflicting legislation across jurisdictions.

Copyright and intellectual property law
particularly the jurisdictions that companies need to deal with (local versus international) to protect and enforce their IP protections.

Safeguards and security controls required for privacy compliance
particularly details of data residency or the ability to move data between countries, as well as varying requirements of due care in different jurisdictions

Data breaches and their aftermath, particularly breach notification

International import/export laws
particularly technologies that may be sensitive or illegal under various international agreements

LAWS, REGULATIONS, STANDARDS, FRAMEWORKS

For the exam, you'll want to be familiar with the difference between laws, regulations, standards, and frameworks

Laws are the legal rules. That are created by government entities, such as legislatures/congress.

Regulations are the rules that are created by governmental agencies.

Laws and regulations must be followed or can result in civil or criminal penalties for the organization.

Standards dictate a reasonable level of performance.

They can be created by an organization for its own purposes (internal) or come from industry bodies or trade groups (external).

Frameworks are a set of guidelines helping organizations improve their security posture.

TYPES OF LAW

Familiarity with different **sources of law** may be helpful on exam day

Criminal law contains prohibitions against acts such as murder, assault, robbery, and arson.

Civil law Examples include contract disputes, real estate transactions, employment matters, and estate/probate procedures.

Vendor contracts fall into this category.

Administrative law policies, procedures, and regulations that govern the daily operations of government and government agencies.

Regulations like HIPAA fall into this category.

TYPES OF LAW

Constitutional Law

The **U.S. Constitution** is the highest possible source of law in the United States, and no laws from other sources may conflict with the provisions in the Constitution

SEVEN ARTICLES OF THE

US CONSTITUTION

Remember this for the exam →

- **Article I** establishes the legislative branch.
- **Article II** establishes the executive branch.
- **Article III** establishes the judicial branch.
- **Article IV** defines the relationship between the federal government and state governments
- **Article V** creates a process for amending the Constitution itself.
- **Article VI** contains the supremacy clause, establishing that the Constitution is the supreme law of the land.
- **Article VII** sets forth the process for the initial establishment of the federal government.

TYPES OF LAW

Case law. Interpretations made by courts over time establish a body of law that other courts may refer to when making their own decisions.

In many cases, the case law decisions made by courts are binding on both that court and any subordinate courts.

Common law is a set of judicial precedents passed down as case law through many generations.

And stand as examples cited in future court cases.

Contract law Violations of a contract generally do not involve law enforcement agencies, so they are treated as private disputes between parties and handled in civil court.

A violation is known as a "breach of contract" and courts may take action to enforce the terms of a contract.

LEGAL LIABILITY

And related to types of law are types of **legal liability**.

Liable means “responsible or answerable in law; legally obligated”.

Comes in two forms:

Criminal liability occurs when a person violates a criminal law.

Civil liability occurs when one person claims that another person has failed to carry out a legal duty that they were responsible for.

Civil cases are brought to court by one party, called the **claimant**, who is accusing another party of a violation, called the **respondent**.

Claimant may be an individual, a corporation, or the government.

TORTS AND NEGLIGENCE

Torts are another form of civil violation that do not involve a contract but instead, involve harm to one party caused by the actions of another party.

Negligence is a commonly occurring tort that occurs when one party causes harm to another party by their action or lack of action.

There must be a **duty of care**. The person accused of negligence must have an established responsibility to the accuser.

There must be a breach of that duty of care. The accused person must have either taken action or failed to take an action that violated the duty of care.

There must be **damages** involved. The accuser must have suffered some type of harm, be it financial, physical, emotional, or reputational.

There must be **causation**. A reasonable person must be able to conclude that the injury caused to the accuser must be a result of the breach of duty by the accused.

LEGAL RISKS SPECIFIC TO CLOUD COMPUTING

Legal, regulatory, and compliance risks in the cloud can be significant for certain types of data or industries.

Differing legal requirements

For example, State and provincial laws in the United States, Canada have different requirements for data breach notifications, such as timeframes.

Different legal systems and frameworks in different countries

In some countries, clear written legislation exists. In others, others legal precedent is more important

Precedent refers to the judgments in past cases and is subject to change over time with less advance notice than updates to legislation.

Conflicting laws

The EU's **GDPR** and the U.S. **Clarifying Lawful Overseas Use of Data (CLOUD) Act** directly conflict on the topic of data transfer.

LEGAL RISKS SPECIFIC TO CLOUD COMPUTING

The bottom line on legal risks specific to cloud computing

Responsibility for compliance with laws and regulations

Researching and planning response in case of conflicting laws

Ensuring necessary audit and incident response data is logged and retained

Any additional due diligence and due care

...rests with the cloud consumer (customer)!

LEGAL FRAMEWORKS AND GUIDELINES

Cloud security practitioners should be aware of the legal frameworks and guidelines that affect the cloud computing environments

Organisation for Economic Co-operation and Development (OECD)

An international organization comprised of 38 member states from around the world, publishes guidelines on data privacy.

Its principles are aligned with European privacy law including consent, transparency, accuracy, security, and accountability

Asia-Pacific Economic Cooperation Privacy Framework (APEC)

Comprised of 21 member economies in the Pacific Rim.

Incorporates many standard privacy practices into their guidance, such as preventing harm, notice, consent, security, and accountability.

Promotes the smooth cross-border flow of information between APEC member nations.

LEGAL FRAMEWORKS AND GUIDELINES

Cloud security practitioners should be aware of the legal frameworks and guidelines that affect the cloud computing environments

General Data Protection Regulation (GDPR)

European Union's GDPR is perhaps the most far-reaching and comprehensive set of laws ever written to protect data privacy.

Mandates privacy for individuals, defines companies' duties to protect personal data, and prescribes punishments for companies violating these laws.

Includes mandatory notification timelines in the event of data breach.

GDPR formally defines many data roles related to privacy and security (subject, controller, processor).

LEGAL FRAMEWORK AND GUIDELINES

Additional legal frameworks & standards

Health Insurance Portability and Accountability Act (HIPAA)
1996 U.S. law regulates the privacy and control of health information data.

Payment Card Industry Data Security Standard (PCI DSS)
An industry standard for companies that accept, process, or receive payment card transactions.

Privacy Shield
Exists to solve the lack of an US-equivalent to GDPR, which impacts rights and obligations around data transfer.

Sarbanes-Oxley Act (SOX)
Law was enacted in 2002 and sets requirements for U.S. public companies to protect financial data when stored and used.

LAWS AND REGULATIONS

As a cloud security practitioner, you should know the difference between **statutory**, **regulatory**, and **contractual requirements**

Statutory requirements

are required by law. HIPAA, GDPR, FERPA

Regulatory requirements FISMA, FedRAMP

may also be required by law but refer to rules issued by a regulatory body that is appointed by a government entity.

Contractual requirements PCI DSS

are required by a legal contract between private parties.

These agreements often specify a set security controls or a compliance framework that must be implemented by a vendor

e.g. SOC, GAPP, CSA CCM

E-DISCOVERY CHALLENGES/COMPLEXITIES IN THE CLOUD

Cloud computing's essential characteristics add significant complexity to eDiscovery

An organization investigating an incident may lack the ability to compel the CSP to turn over vital information needed to investigate.

The information may be housed in a country where jurisdictional issues make the data more difficult to access.

Maintaining a chain of custody is more difficult since there are more entities involved in the process.

Three important considerations include 1) vendor selection, 2) architecture, 3) due care obligations

E-DISCOVERY CHALLENGES/COMPLEXITIES IN THE CLOUD

Cloud computing's essential characteristics add significant complexity to eDiscovery

Vendor selection considerations

When considering a cloud vendor, eDiscovery should be considered as a security requirement during the selection and contract negotiation phases.

Architecture considerations

Data residency and system architecture are other important considerations for eDiscovery in the cloud and can be handled proactively.

such as when designing or deploying a system or business process

Due care considerations Ensuring the org is prepared for DFIR

Cloud security practitioners must inform their organizations of any risks and required due care and due diligence related to cloud computing

E-DISCOVERY FRAMEWORKS

eDiscovery Frameworks

CSPs may not preserve essential data for the required period of time to support historical investigations.

They may not even log all the data relevant to support an investigation.

This shifts the burden of recording and preserving potential evidence onto the consumer

Consumers must identify and implement their own data collection.
eDiscovery frameworks include cloud-specific guidance that may help

FORENSICS REQUIREMENTS

Digital forensics and eDiscovery requirements for many legal controls are greatly complicated by the cloud environment

In the cloud, it's difficult or impossible to perform physical search and seizure of cloud resources such as storage or hard drives.

ISO/IEC and **CSA** provide guidance on best practices for collecting digital evidence and conducting forensics investigations in the cloud.

All security practitioners should be familiar with the following standards, even if they do not specialize in forensics

We touched on all the relevant standards
in Domain 5, but we'll revisit here

ELECTRONIC DISCOVERY FRAMEWORKS

NIST

NISTIR 8006

NISTIR 8006, “Cloud Computing Forensic Science Challenges

NISTIR = **NIST I**nteragency or **I**nternal **R**eports

Addresses common issues and solutions needed to address DFIR in cloud environments.

DFIR = **D**igital **F**orensics and **I**ncident **R**esponse

FROM THE NISTIR 8006 ABSTRACT

Guidance on DFIR for cloud

Summarizes research performed by the members of the **NIST Cloud Computing Forensic Science Working Group**

Aggregates, categorizes, and discusses the forensics challenges faced by experts when responding to incidents that have occurred in a cloud-computing ecosystem

GUIDANCE ON FORENSIC DATA COLLECTION

DOMAIN 5 REFRESHER

ISO/IEC 27050

A four-part standard within the ISO/IEC 27000 family of information security standards

Offers a framework, governance, and best practices for forensics, eDiscovery, and evidence management

Hiring an outside forensic expert is the best path for most organizations

CSA Security Guidance

Free guidance in **Domain 3: Legal Issues: Contracts and Electronic Discovery**

Offers guidance on legal concerns related to security, privacy, and contractual obligations

Covers topics like data residency, liability of data processor role

FORENSIC INVESTIGATION STANDARDS

Forensic Investigation Standards

-ISO/IEC 27037:2012
-ISO/IEC 27041:2015
-ISO/IEC 27042:2015

-ISO/IEC 27043:2015
-ISO/IEC 27050-1:2016
-CSA Domain 3: Contracts & eDiscovery

ISO/IEC 27037:2012

Guide for collecting, identifying, and preserving electronic evidence

ISO/IEC 27041:2015

Guide for incident investigation

ISO/IEC 27042:2015

Guide for digital evidence analysis.

ISO/IEC 27043:2015

Guide for incident investigation principles and processes

6. LEGAL, RISK AND COMPLIANCE

6.2 Understand Privacy Issues

Difference between contractual and regulated private data
(e.g., protected health information (PHI), personally identifiable information (PII))

Country-specific legislation related to private data
(e.g., protected health information (PHI), personally identifiable information (PII))

Jurisdictional differences in data privacy

6. LEGAL, RISK AND COMPLIANCE

6.2 Understand Privacy Issues

Standard privacy requirements
(e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27018, Generally Accepted Privacy Principles (GAPP), General Data Protection Regulation (GDPR))

Privacy Impact Assessments (PIA)

CONTRACTUAL AND REGULATED PRIVATE DATA

Personally Identifiable Information (PII)
Any information that can identify an individual (name, SSN, birthdate/place, biometric records, etc)

Defined by NIST SP 800-122

Protected Health Information (PHI).
Health-related information that can be related to a specific person

Must be protected by strong controls and access audited

Regulated by HIPAA / HITRUST

Payment Data. Applies to those processing the transactions
Allowable storage of information related to credit and debit cards and transactions.

Defined and regulated by PCI DSS and is CONTRACTUAL

CONTRACTUAL AND REGULATED PRIVATE DATA

A Security team must understand:

-what types of data an organization is processing

-where it is being processed

-any associated requirements, such as contractual obligations

In any cloud computing environment, the legal responsibility for data privacy and protection rests with the cloud consumer.

The **data controller** is always responsible for ensuring that the requirements for protection and compliance are met.

...even if that data is processed in a CSP's cloud service.

Responsibility cannot be transferred but risk can be mitigated

Components of a contract may include how data is processed, security controls, deletion of data, physical location, audit, and use of subcontractors.

COUNTRY-SPECIFIC LEGISLATION – AUS

Australian Privacy Act

organizations may process data belonging to Australian citizens offshore.

transferring entity (the data owner) must ensure that the receiver of the data holds and processes it in accordance with the principles of Australian privacy law.

Data owner (controller) is responsible for data privacy

commonly achieved through contracts that require recipients to maintain or exceed the data owner's privacy standards

The entity transferring the data out of Australia remains responsible for any data breaches by or on behalf of the recipient entities

Canada Privacy Law

Personal Information Protection and Electronic Documents Act (PIPEDA)

a national-level law that restricts how commercial businesses may collect, use, and disclose personal information.

PIPEDA covers information about an individual that is identifiable to that specific individual.

DNA, age, medical, education, employment, identifying numbers, religion, race/ethnic origin, financial information

includes a data breach notification requirement.

PIPEDA may also be superseded by province-specific laws that are deemed substantially similar to PIPEDA.

COUNTRY-SPECIFIC LEGISLATION – EU

GDPR

GENERAL **D**ATA
PROTECTION **R**EGULATION

Includes the following on data subject privacy rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (the right to be forgotten)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Other private data types in GDPR: race or ethnic origin, political affiliations or opinions, religious or philosophical beliefs, and sexual orientation.

STANDARD PRIVACY REQUIREMENTS

GDPR

General Data Protection Regulation

Deals with the handling of data while maintaining privacy and rights of an individual.

It is international as it was created by the EU, which has 27 different countries as members.

GDPR applies to ANY company with customers in the EU

Includes a 72-hour notification deadline in the case of data breach

National, Territory, and State Laws

Gramm-Leach-Bliley Act (GLBA) of 1999

focuses on services of banks, lenders, and insurance

severely limits services they can provide and the information they can share with each other

This act consists of three main sections:

The Financial Privacy Rule, which regulates the collection and disclosure of private financial information

The Safeguards Rule, which stipulates that financial institutions must implement security programs to protect such information

The Pretexting provisions, which prohibit the practice of pretexting (accessing private information using false pretenses)

COUNTRY-SPECIFIC LEGISLATION – U.S.

National, Territory, and State Laws

Privacy Shield
an international agreement between the United States (U.S.) and the European Union.

allows the transfer of personal data from the European Economic Area (EEA) to the U.S. by U.S.-based companies.

...but is not an indicator of GDPR compliance

Orgs commit to seven principles of the agreement:

- Notice
- Choice
- Security
- Access
- Accountability for onward transfer
- Data integrity and purpose limitation
- Recourse, enforcement, and liability

COUNTRY-SPECIFIC LEGISLATION – U.S.

National, Territory, and State Laws

The Stored Communication Act (SCA) of 1986

created privacy protection for electronic communications like email or other digital communications stored on the Internet.

extends the Fourth Amendment of the U.S. Constitution to the electronic realm

The Fourth Amendment:
Details the people's "right to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"

It outlines that private data is protected from unauthorized access or interception (by private parties or the government).

National, Territory, and State Laws

Health Insurance Portability and Accountability Act (HIPAA) of 1996

privacy and security regulations requiring strict security measures for hospitals, physicians, insurance companies

HIPAA-covered entities are those organizations that collect or generate protected health information (PHI)

under HIPAA there are separate rules for privacy, security, and breach notification, and flow of these rules down to third parties

Under HIPAA, PHI may be stored by cloud service providers provided that the data is adequately protected

COUNTRY-SPECIFIC LEGISLATION – U.S.

National, Territory, and State Laws

Clarifying Lawful Overseas Use of Data (CLOUD) Act

aids in evidence collection in investigation of serious crimes

created in 2018 due to the problems that FBI faced in forcing Microsoft to hand over data stored in Ireland

requires U.S.-based companies to respond to legal requests for data no matter where the data is physically located.

JURISDICTIONAL DIFFERENCES IN DATA PRIVACY

Different laws and regulations may apply depending on the **location** of

- data subject
- data collector
- cloud service provider
- subcontractors processing data
- company headquarters of the entities involved

Legal concerns can:

- prevent the utilization of a cloud services provider
- add to costs and time to market
- drive changes to technical architectures required to deliver services

Never replace compliance with convenience when evaluating services, as this increases risks

Many privacy laws impose fines or other action for noncompliance.

STANDARD PRIVACY REQUIREMENTS

ISO/IEC
27018

ISO 27018 was published in July 2014 as a component of the ISO 27001 standard.

Adherence to these privacy requirements enables customer trust in the CSP.

Major CSPs such as Microsoft, Google, and Amazon all maintain ISO 27000 compliance

Can provide a HIGH level of assurance.

STANDARD PRIVACY REQUIREMENTS

ISO/IEC

27018

Consent: Personal data obtained by a CSP may not be used for marketing purposes unless expressly permitted by the subject.

A customer should be permitted to use a service without requiring this consent.

Control: Customers shall have explicit control of their own data and how that data is used by the CSP.

Transparency: CSPs must inform customers of where their data resides AND any subcontractors that may process personal data.

Communication: Auditing should be in place, and any incidents should be communicated to customers.

Audit: Companies (CSP, in this case) must subject themselves to an independent audit on an annual basis.

GENERALLY ACCEPTED PRIVACY PRINCIPLES (GAPP)

Generally Accepted Privacy Principles (GAPP) is a framework of privacy principles

Created by AICPA

GAPP are widely incorporated into the SOC 2 framework as an optional criterion

Organizations that pursue a SOC 2 audit can include these privacy controls if appropriate

(depends on the type of services they provide)

Similar to ISO 27018, which is an optional extension of the controls defined in ISO 27002

can increase assurance

An audit of these controls results in a report that can be shared with customers or potential customers, who can use it to assess a service provider's ability to protect sensitive data.

GENERALLY ACCEPTED PRIVACY PRINCIPLES (GAPP)

1

Management

The organization defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

2

Notice

The organization provides notice of its privacy policies and procedures. The organization identifies the purposes for which personal information is collected, used, and retained.

3

Choice and consent

The organization describes the choices available to the individual, and secures implicit or explicit consent regarding the collection, use, and disclosure of the personal data.

4

Collection

Personal information is collected only for the purposes identified in the notice provided to the individual.

5

Use, retention, and disposal

WHY org can retain WHEN to dispose

The personal information is limited to the purposes identified in the notice the individual consented to.

Categories of the 10 main privacy principles

GENERALLY ACCEPTED PRIVACY PRINCIPLES (GAPP)

6 **Access**

The organization provides individuals with access to their personal information for review or update.

7 **Disclosure to third parties**

Personal information is disclosed to third parties only for the identified purposes and with implicit or explicit consent of the individual.

8 **Security for privacy**

Personal information is protected against both physical and logical unauthorized access.

9 **Quality**

The organization maintains accurate, complete, and relevant personal information that is necessary for the purposes identified.

10 **Monitoring and enforcement**

The organization monitors compliance with its privacy policies and procedures. It also has procedures in place to address privacy-related complaints and disputes

Categories of the 10 main privacy principles

PRIVACY IMPACT ASSESSMENT

What is a PIA?

A privacy impact assessment (PIA) is designed to identify the privacy data being collected, processed, or stored by a system, and assess the effects of a data breach

When is a PIA necessary?

Several privacy laws explicitly require PIAs as a planning tool for identifying and implementing required privacy controls, including GDPR and HIPAA.

Conducting a PIA typically begins when a system or process is being evaluated

However, evolving privacy regulation often necessitates assessment of existing systems.

To conduct a PIA, you must define assessment scope, data collection methods, and plan for data retention

The **International Association of Privacy Professionals (IAPP)** has published guides and resources related to privacy efforts, including PIA.

6. LEGAL, RISK AND COMPLIANCE

6.3 Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment

Internal and external audit controls

Impact of audit requirements

Identify assurance challenges of virtualization and cloud

Types of audit reports
(e.g., Statement on Standards for Attestation Engagements (SSAE), Service Organization Control (SOC), International Standard on Assurance Engagements (ISAE))

6. LEGAL, RISK AND COMPLIANCE

6.3 Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment

Restrictions of audit scope statements
(e.g., Statement on Standards for Attestation Engagements (SSAE), International Standard on Assurance Engagements (ISAE))

Gap analysis
(e.g., control analysis, baselines)

Audit planning

Internal information security management system

6.3 Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment

Internal information security controls system

Policies
(e.g., organizational, functional, cloud computing)

Identification and involvement of relevant stakeholders

6. LEGAL, RISK AND COMPLIANCE

6.3 Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment

Specialized compliance requirements for highly-regulated industries
(e.g., NERC / CIP, HIPAA/HITECH, PCI DSS)

Impact of distributed information technology (IT) model
(e.g., diverse geographical locations and crossing over legal jurisdictions)

AUDIT PROCESS AND METHODOLOGIES

What is Auditing?

a methodical examination of an environment to ensure compliance with regulations and to detect abnormalities, unauthorized occurrences, or outright crimes.

serves as a primary type of detective control.

frequency is based on risk.

degree of risk also affects how often an audit is performed.

Secure IT environments rely heavily on auditing and many regulations require it.

AUDITING & DUE CARE

Security audits and effectiveness reviews are key elements in displaying due care. without them, senior management will likely be held accountable and liable for any asset losses that occur.

Act with common sense, prudent management, responsible action

SECURITY AUDITS AND REVIEWS

Security audits and reviews

help ensure that management programs are effective and being followed.

commonly associated with account management practices to prevent violations with least privilege or need-to-know principles.

can also be performed to oversee many programs and processes

- patch management
- vulnerability management
- change management
- configuration management

CONTROLLING ACCESS TO AUDIT REPORTS

REAL WORLD

Audit reports often contain **sensitive information**

Often include purpose and scope of the audit, and results discovered or revealed

Can include sensitive information such as problems, standards, causes, and recommendations.

Only people with sufficient privilege should have access

FOR EXAMPLE:
senior security administrators = full detail
senior management = high-level summary

INTERNAL AUDITORS & AUDITS

Internal Auditor

Acts as a "trusted advisor" to the organization on risk, educating stakeholders, assessing compliance

Compliance may mean company policies or regulatory

Internal Audit

Can provide more continuous monitoring of control effectiveness and policy compliance

Enables the org to catch and fix any issues before they show up on a formal audit report

An **internal audit can also mitigate risk** by examining cloud architectures to provide insights into an organization's

- Cloud governance
- Data classifications
- IAM effectiveness
- Regulatory compliance
- Privacy compliance
- Cyber threats

INTERNAL AUDITORS & AUDITS

Internal Auditor

Acts as a "trusted advisor" to the organization on risk, educating stakeholders, assessing compliance

Compliance may mean company policies or regulatory

Internal Audit

Can provide more continuous monitoring of control effectiveness and policy compliance

Enables the org to catch and fix any issues before they show up on a formal audit report

Some legal and regulatory frameworks require the use of an independent auditor, others demand a third-party auditor

💡 An internal auditor is an independent entity who can provide facts without fear of reprisal

IMPACT OF AUDIT REQUIREMENTS

The requirement to conduct audits can have a large procedural and financial impact on a company.

Regulated industries

Some entities operate in heavily regulated industries subject to numerous auditing requirements, such as banks or critical infrastructure providers.

With multi-national companies, audit complexity may be higher due to conflicting requirements

Sample size and relevance

In large environments, representative samples of some infrastructure (e.g. 20 of 100 servers) may be checked but must be representative of the multi-region estate.

Multi-region data dispersion in the cloud and dynamic VM failure in hypervisors can complicate the audit process

ASSURANCE CHALLENGES WITH VIRTUALIZATION & CLOUD

The cloud is made possible by **virtualization** technologies, that enable dynamic environments needed for a global provider platform.

Depending on the cloud architecture employed, a cloud security professional must perform multiple layers of auditing.

To be effective, the auditor must understand the virtualization architecture of the cloud provider

PROVIDER CSP

Audits of controls over the hypervisor will usually be the purview of the CSP

Microsoft, Amazon, Google

CUSTOMER

VMs deployed on top of that hardware are usually under owned by the customer

Cloud consumers

TYPES OF AUDIT REPORTS

SSAE
Statements on Standards
for Attestation Engagements

ISAE
International Standard
on Assurance Engagements

CSA
Cloud Security Alliance

SSAE 18 is a set of standards defined by the AICPA (American Institute of CPAs)

Designed to enhance the quality and usefulness of System and Organization Control (SOC) reports.

Includes audit standards and suggested report formats to guide and assist auditors

TYPES OF AUDIT REPORTS

SSAE
Statements on Standards
for Attestation Engagements

ISAE
International Standard
on Assurance Engagements

CSA
Cloud Security Alliance

SOC 1

deals mainly with financial controls and are used primarily by CPAs auditing financial statements

SOC 2 Type 1

report that assesses the design of security processes at a specific point in time

✓

SOC 2 Type 2

(often written as "Type II") assesses how effective those controls are over time by observing operations for at least six months

Often require an NDA due to sensitive contents

SOC 3

contain only the auditor's general opinions and non-sensitive data, is publicly shareable

SSAE is US-based, but SOC2 has become a de facto global standard

TYPES OF AUDIT REPORTS

SSAE
Statements on Standards
for Attestation Engagements

ISAE
International Standard
on Assurance Engagements

CSA
Cloud Security Alliance

The **International Auditing and Assurance Standards Board** issues the ISAE

This board and it's ISAE standards are similar to the AICPA and it's SSAE standards

The ISAE 3402 standard is roughly equivalent to the SOC 2 reports in the SSAE

TYPES OF AUDIT REPORTS

SSAE
Statements on Standards
for Attestation Engagements

ISAE
International Standard
on Assurance Engagements

CSA
Cloud Security Alliance

The **Security Trust Assurance and Risk (STAR)** certification program comes from CSA

Can be used by cloud service providers, cloud customers, or auditors and consultants

Designed to demonstrate compliance to a desired level of assurance

STAR consists of two levels of certification, which provide increasing levels of assurance

TYPES OF AUDIT REPORTS

SSAE
Statements on Standards
for Attestation Engagements

ISAE
International Standard
on Assurance Engagements

CSA
Cloud Security Alliance

STAR consists of two levels of certification, which provide increasing levels of assurance

Level 1: Self-assessment
is a complimentary offering that documents the security controls provided by the CSP

Level 2: Third-party audit
requires the CSP to engage an independent auditor to evaluate the CSP's controls against the CSA standard

Stronger, as it's a third-party audit conducted by a trained, qualified auditor

More on CSA Star registry and assurance at **cloudsecurityalliance.org/star**

RESTRICTIONS OF AUDIT SCOPE STATEMENTS

Audit scope statements provide the reader with details on what was included in the audit and what was not

An audit scope statement generally includes:

- Statement of purpose and objectives
- Scope of audit and explicit exclusions
- Type of audit
- Security assessment requirements
- Assessment criteria and rating scales
- Criteria for acceptance
- Expected deliverables
- Classification (*secret, top secret, public, etc.*)

Setting parameters for an audit is known as **audit scope restrictions**

RESTRICTIONS OF AUDIT SCOPE STATEMENTS

Determining the scope of an audit is usually a joint activity performed by the organization being audited and their auditor.

Who determines audit scope?

RESTRICTIONS OF AUDIT SCOPE STATEMENTS

Why limit the scope of an audit?

Audits are expensive endeavors that can engage highly trained (and highly paid) content experts.

Auditing of systems can affect system performance and, in some cases, require the downtime of production systems.

A new system not yet in production, without all the planned controls in place is not ready to audit.

Cost of implementing controls and auditing some systems is too high relative to the revenue the service generates.

GAP ANALYSIS

A **gap analysis** identifies where an organization does not meet requirements and provides important information to help remediate gaps

The main purpose is to compare the organization’s current practices against a specified framework and identify the gaps between the two.

May be performed by either internal or external parties

Choice of which usually driven by the cost and need for objectivity.

When is a gap analysis useful?

As a precursor to a formal audit process, so the organization can close gaps before a third-party (external) audit.

When assessing the impact of changes to regulatory or compliance frameworks, which introduce new or modified requirements.

'ISO 27002' and 'NIST CSF' are frameworks commonly used for gap analysis

Audit Planning Phases

The audit process can generally be broken down into four phases, starting with **audit planning**.

Audit planning activities include:

Document and define audit program objectives. collaborative internal planning of audit scope and objectives.

Gap analysis or readiness assessment. assessing the organization's ability to successfully undergo a full audit.

Define audit objectives and deliverables. it is important to identify the expected outputs from the audit.

Identifying auditors and qualifications. compliance and audit frameworks usually specify the type of auditor required.

AUDIT PLANNING

Audit Phases

There are three major phases of an audit, which include the following activities:

Audit fieldwork: involves the actual work the auditors perform to gather, test, and evaluate the organization.

Audit reporting: report writing begins as auditors conduct their fieldwork, capturing notes and any findings.

Audit follow-up: various activities may be conducted after the audit, including addressing any identified weaknesses

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

An **information security management system (ISMS)** is a systematic approach to information security

An ISMS focuses processes, technology, and people designed to help protect and manage an organization’s information.

ISO 27001 addresses need and approaches to implementing an ISMS

ISMS Functions

Quantify risk

Develop and execute risk mitigation strategies

Provide formal reporting on status of mitigation efforts

ISMS Benefits

Improve data security

Increased organizational resilience to cyberattacks

Central info security mgmt.

Formal risk management

INTERNAL INFORMATION SECURITY CONTROLS SYSTEM

a system of **information security controls** provides guidance for mitigating the risks identified as part of ISMS risk management processes.

There are several control frameworks to choose from.

Scoping controls refers to reviewing controls in the framework to identify which controls apply to the organization and which do not.

Tailoring is a process of matching applicable controls with the organization's specific circumstances to which they apply.

Organizations implementing an ISO 27001 ISMS will find the ISO 27002 controls very easy to use, since they are designed to fit together.

Other control frameworks include:

-NIST SP 800-53
-NIST Cybersecurity Framework (CSF)
-Secure Controls Framework
-CSA Cloud Controls Matrix (CCM)

POLICIES

Organizational, Functional, and Cloud Computing

Policies are a key part of any data security strategy and facilitate a number of capabilities for an organization:

Provide users and organizations with a way to understand and enforce requirements in a systematic way.

Make employees and management aware of their roles and responsibilities.

Standardize secure practices throughout the organization.

Know the difference between **organizational** and **functional** policies, and how they should be applied to the cloud

ORGANIZATIONAL POLICIES

Companies use policies to outline rules and guidelines, usually complemented by documentation such as procedures, job aids

Organizations typically define policies related to proper use of company resources, like expense reimbursements and travel

Policies are a proactive risk mitigation tool designed to reduce the likelihood of risks, such as:

- Financial losses
- Data loss or leakage
- Reputational damage
- Statutory and regulatory compliance issues
- Abuse or misuse of computing systems and resources

Employees should generally sign policies to acknowledge acceptance

What is a functional policy?

A set of standardized definitions for employees that describe how they are to make use of systems or data.

Typically guide specific activities crucial to the organization, such as appropriate handling of data, vulnerability management, and so on.

Functional policies generally codify requirements identified in the ISMS and align to your chosen control framework

Examples of functional policies

The following, while not an exhaustive list, identifies several common policies that organizations might find useful:

Acceptable use: What is and is not acceptable to do on company hardware and networks.

Email use: What is and is not acceptable to do on company email accounts.

Passwords and access management: Password complexity, expiration, reuse, requirements for MFA, and requirements for use of access management tools such as a password manager.

Incident response: How incidents are handled, and requirements for defining an incident response plan.

FUNCTIONAL POLICIES

Examples of functional policies

The following, while not an exhaustive list, identifies several common policies that organizations might find useful:

Data classification: Identifies types of data and how each should be handled.

Network services: How issues such as remote access and network security are handled.

Vulnerability scanning: Routines and limitations on internal scanning and penetration testing.

Patch management: How equipment is patched and on what schedule.

APPLYING POLICIES TO THE CLOUD

Ease of deploying cloud resources without governance results in "**shadow IT**" – resources deployed without IT approval!

This can create security risks, like data loss or leakage through unauthorized use of cloud storage services.

Also creates financial risks, as spending is more difficult to measure and control.

Cloud services should be included in organization policies, and requirements for use clearly documented.

A CASB can help identify and stop shadow IT!

Policies should define requirements users must adhere to and specify which cloud services are approved for various uses.

Identification and Involvement of Relevant Stakeholders

One key challenge in the audit process is the inclusion of any **relevant stakeholders**

Who are an org’s relevant stakeholders?

Organization’s **management** who will likely be paying for the audit

Security practitioners responsible for facilitating the audit

Employees who will be called upon to provide evidence to auditors in the form of documentation, artifacts, or sitting for interviews.

Cloud computing environments can include more stakeholders than on-premises and even multiple CSPs

REQS FOR HIGHLY REGULATED INDUSTRIES

Many CSPs have compliance-focused cloud service offerings, which meet the requirements of specific regulatory or legal frameworks

NERC/CIP

North American Electric Reliability Corporation Critical Infrastructure Protection regulates organizations involved in power generation and distribution.

HIPAA/HITECH

Does not specifically address cloud computing

Both deal with PHI and implement specific requirements for security and privacy protections, as well as breach notification requirements.

PCI DSS

Also no specific mention of cloud

Specifies protections for payment card transaction data.

CSPs make the controls available, but responsibility for compliance to any relevant regulations ultimately rests with the cloud consumer

IMPACT OF DISTRIBUTED IT MODEL

Cloud computing enables distributed IT service delivery, with systems that can automatically **replicate data globally**

One impact of this distributed model is the additional geographic locations auditors must consider when performing an audit.

A common technique in cloud audits is **sampling**, which is the act of picking a subset of the system's physical infrastructure to inspect.

Sampling 20 servers of 100 servers across many regional datacenters can save time & expense and maintain accuracy

CSPs have found ways to collect evidence that provides auditors with sufficient assurance that they have collected a representative sample.

6. LEGAL, RISK AND COMPLIANCE

6.4 Understand Implications of Cloud to Enterprise Risk Management

Assess providers risk management programs
(e.g., controls, methodologies, policies, risk profile, risk appetite)

Difference between data owner/controller vs. data custodian/processor

Regulatory transparency requirements
(e.g., breach notification, Sarbanes-Oxley (SOX), General Data Protection Regulation (GDPR))

6. LEGAL, RISK AND COMPLIANCE

6.4 Understand Implications of Cloud to Enterprise Risk Management

Risk treatment
(i.e., avoid, mitigate, transfer, share, acceptance)

Different risk frameworks

Metrics for risk management

Assessment of risk environment
(e.g., service, vendor, infrastructure, business)

ASSESS PROVIDERS RISK MANAGEMENT PROGRAMS

Reviewing provider controls

Prior to establishing a relationship with a cloud provider, a cloud customer needs to analyze the risks associated with adopting that provider's services

Rather than performing a direct audit, the customer must rely on their **supply chain risk management (SCRM)** processes.

Primary areas of focus in SCRM include evaluating:

- whether a supplier has a risk management program in place, and if so
- whether the risks identified by that program are being adequately mitigated.

Unlike traditional risk management activities, SCRM in a CSP scenario often requires customers to take an indirect approach –reviewing audit reports.

Major CSPs all make available SOC 2, ISO 27001, FedRAMP, or CSA STAR audit reports in lieu of direct audit.

ASSESS PROVIDERS RISK MANAGEMENT PROGRAMS

Reviewing provider controls

When reviewing an audit report, there are several key elements of the report to focus on, such as scoping information or description of the audit target.

Some compliance frameworks allow audits to be very narrowly scoped, such as SOC 2.

IMPORTANT: If the CSP's SOC 2 audit did not cover a specific service a customer wants to use, then the audit finding does not provide any value!

This may drive changes, such as enhanced customer-side controls, tracking the CSP's mitigation and resolution efforts, or migrating to another CSP altogether.

ASSESS PROVIDERS RISK MANAGEMENT PROGRAMS

Methodologies

There are resources that can help organizations build out or enhance their SCRM program:

- **NIST** has a resource library that includes working groups, publications, and other resources, available at: csrc.nist.gov/Projects/cyber-supply-chain-risk-management .
- **ISO 27000:2022** specifies a security management system for security and resilience, with a particular focus on supply chain management.

Risk Profile

Risk profile describes the risk present in the organization based on all the identified risks and any associated mitigations in place.

ASSESS PROVIDERS RISK MANAGEMENT PROGRAMS

Risk Appetite

Risk appetite describes the amount of risk an organization is willing to accept without mitigating.

Regulated industries will be more apt to **mitigation**, **transference**, and **avoidance.**

Smaller orgs and startups will be more apt to simply **accept** risks to avoid cost of treatment.

GDPR Data Roles & Responsibilities

Data Processor. Anyone who processes personal data on behalf of the data controller. The CUSTODIAN

Is responsible for the safe and private custody, transport, and storage

Data Controller. The person or entity that controls processing of the data. The OWNER

Owns the data and risks associated with any data breaches

When data controllers use processors, they must ensure that security requirements follow the data.

GDPR Data Roles & Responsibilities

Data Protection Officer (DPO). ensures the organization complies with data regulations.

Under GDPR, the DPO is a mandatory appointment

Data Subject is the individual or entity that is the subject of the personal data.

Know the data roles

How do you identify each of these roles?

Data Owner Data CONTROLLER in GDPR

Usually a member of **senior management**.

CAN delegate some day-to-day duties.

CANNOT delegate total responsibility.

Data Custodian Data PROCESSOR in GDPR

Usually someone in the **IT department**.

DOES implement controls for data owner

DOES NOT decide what controls are needed

TIP: If question mentions “day-to-day” it’s custodian!

REGULATORY TRANSPARENCY REQUIREMENTS

A cloud security professional should be aware of the **transparency requirements imposed on data controllers** by various regulations and laws around the world.

Breach Notification

Most recent privacy laws include mandatory breach notification.

There are some variations among the laws, mainly around issues of timing of the notification and who must be notified

Regulations that require breach notification include, but are not limited to, GDPR, HIPAA (as amended by the HITECH Act), GLBA, and PIPEDA.

WHO should be notified and HOW QUICKLY

Incident response plans and procedures should include relevant information about the time period for reporting, as well as the required contacts in the event of a data breach.

REGULATORY TRANSPARENCY REQUIREMENTS

Sarbanes-Oxley Act

If a company is publicly traded in the United States, they are subject to transparency requirements

Under the Sarbanes-Oxley Act (SOX) of 2002. Specifically, as data owners, these companies should consider the following:

- **Section 802**: It is a crime to destroy, change, or hide documents to prevent their use in official legal processes.
- **Section 804**: Companies must keep audit-related records for a minimum of five years.

SOX compliance is often an issue with both data breaches and ransomware incidents at publicly traded companies.

The loss of data related to compliance due to external actors does not protect a company from legal obligations.

REGULATORY TRANSPARENCY REQUIREMENTS

General Data Protection Regulation (GDPR)

For companies doing business in the European Union or with citizens of the EU, transparency requirements under the GDPR are laid out in Article 12.

Available at https://gdpr-info.eu/art-12-gdpr

States that a data controller "must be able to demonstrate that personal data are processed in a manner transparent to the data subject."

The obligations for transparency begin at the data collection stage and apply "throughout the lifecycle of processing."

Stipulates that communication to data subjects must be "concise, transparent, intelligible and easily accessible, and use clear and plain language."

Meeting the requirement for transparency also requires processes for providing data subjects with access to their data.

Risk Treatment

The practice of modifying risk, usually to lower it.

Typically begins with identifying and assessing risks by measuring the likelihood and impact.

Risks most likely to occur and impactful would be prioritized for treatment.

RISK TREATMENT

Risk treatment is the organization's response to risk

Risk Avoidance Can negatively impact business opportunities

Where the organization changes business practices to completely eliminate the potential that a risk will materialize.

Risk Mitigation

The process of applying security controls to reduce the probability and/or magnitude of a risk.

Risk Transference e.g. cyber insurance

Shifts some of the impact of a risk from the organization experiencing the risk to another entity.

Risk Acceptance Use when cost of mitigation > cost of impact

Deliberately choosing to take no other risk management strategy and to simply continue operations as normal in the face of the risk.

Know these concepts and be ready to recognize examples on the exam!

RISK MANAGEMENT STRATEGIES

Risk Appetite. Sometimes called *"risk tolerance"*, is the amount of risk that a company is willing to accept.

These terms are often used interchangeably, though many experts can articulate a difference.

Regulations that affect risk posture

regulations addressing data privacy and security that influence an organizations risk posture include:

-General Data Protection Regulation (**GDPR**)

-Sarbanes-Oxley Act (**SOX**),

-Health Insurance Portability Accountability Act (**HIPAA**)

-Payment Card Industry & Data Security Standard regulations (**PCI-DSS**)

Security Controls

Risk treatments for countering and minimizing loss or unavailability of services or apps due to vulnerabilities

Security Controls

The terms **safeguards** and **countermeasure** may seem to be used interchangeably

Security Controls

safeguards are **proactive** (reduce likelihood of occurrence)

countermeasures are **reactive** (reduce impact after occurrence)

DIFFERENT RISK FRAMEWORKS

There are several risk management frameworks available for security practitioners to use as guides when designing a risk management program.

In the cloud computing arena, a cloud security professional should be familiar with these risk frameworks:

- ISO 31000:2018 guidance standard
- ENISA’s cloud computing risk assessment
- NIST 800-37, “Risk Management Framework”

Also, worth mention is:

NIST 800-146, “Cloud Computing Synopsis and Recommendation,” Although not a dedicated risk management standard, the various risks and benefits associated with different deployment and service models are discussed.

DIFFERENT RISK FRAMEWORKS

There are several risk management frameworks available for security practitioners to use as guides when designing a risk management program.

ISO 31000

ISO 31000 contains several standards related to building and running a risk management program.

ISO 31000:2018, “Risk management —Guidelines,”
provides the foundation of an organization’s risk management function.

IEC 31010:2019, “Risk management —Risk assessment techniques”
provides guidance on conducting a risk assessment.

ISO GUIDE 73:2009, “Risk management —Vocabulary”
provides a standard set of terminology used through the other documents and is useful for defining elements of the risk management program.

DIFFERENT RISK FRAMEWORKS

There are several risk management frameworks available for security practitioners to use as guides when designing a risk management program.

NIST

NIST Special Publication 800-37 is the NIST Risk Management Framework

NIST Special Publication 800-146 "Cloud Computing Synopsis and Recommendations" provides definitions of various cloud computing terms

ENISA

A rough equivalent to the U.S. NIST

ENISA produces useful resources related to cloud-specific risks that organizations should be aware of and plan for when designing cloud computing systems.

This guide identifies various categories of risks and recommendations for organizations to consider when evaluating cloud computing.

These include research recommendations to advance the field of cloud computing, legal risks, and security risks.

METRICS FOR RISK MANAGEMENT

There are some key cybersecurity metrics that companies can track to present measurable data to company stakeholders

Patching levels: How many devices are fully patched and up-to-date?

Unpatched devices often contain exploitable vulnerabilities.

Time to deploy patches: How may devices receive required patches in the defined timeframes?

A useful measure of how effective a patch management program is at reducing the risk of known vulnerabilities.

Intrusion attempts: How many times have unknown actors tried to breach cloud systems?

Increased intrusion attempts can be an indicator of increased risk likelihood.

METRICS FOR RISK MANAGEMENT

There are some key cybersecurity metrics that companies can track to present measurable data to company stakeholders

Mean time to detect (MTTD), mean time to contain (MTTC), and mean time to resolve (MTTR):

How long does it take for security teams to become aware of a potential security incident, contain the damage, and resolve the incident?

Inadequate tools or resources for reactive risk mitigation can increase the impact of risks occurring.

Cybersecurity metrics provide vital information for decision makers in the organization.

METRICS FOR RISK MANAGEMENT

There are some key cybersecurity metrics that companies can track to present measurable data to company stakeholders

Mean time to detect (MTTD), mean time to contain (MTTC), and mean time to resolve (MTTR):

How long does it take for security teams to become aware of a potential security incident, contain the damage, and resolve the incident?

Inadequate tools or resources for reactive risk mitigation can increase the impact of risks occurring.

Cybersecurity metrics within expected parameters indicate the risk mitigations are effective.

METRICS FOR RISK MANAGEMENT

There are some key cybersecurity metrics that companies can track to present measurable data to company stakeholders

Mean time to detect (MTTD), mean time to contain (MTTC), and mean time to resolve (MTTR):

How long does it take for security teams to become aware of a potential security incident, contain the damage, and resolve the incident?

Inadequate tools or resources for reactive risk mitigation can increase the impact of risks occurring.

Metrics that deviate from expected parameters are no longer effective and should be reviewed

ASSESSMENT OF RISK ENVIRONMENT

The cloud is a critical operating component for many organizations, so it is crucial to identify and understand the risks posed by a CSP.

The greater the dependency on the CSP, the greater the risk.

It is important to ask a number of questions when considering a cloud service, vendor, or infrastructure provider.

- Is the provider subject to takeover or acquisition?
- How financially stable is the provider?
- In what legal jurisdiction(s) are the provider's offices located?
- Are there outstanding lawsuits against the provider?
- What pricing protections are in place for services contracted?
- How will a provider satisfy any regulatory or legal compliance requirements?
- What does failover, backup, and recovery look like for the provider?

ASSESSMENT OF RISK ENVIRONMENT

The cloud is a critical operating component for many organizations, so it is crucial to identify and understand the risks posed by a CSP.

The greater the dependency on the CSP, the greater the risk.

Designing a supply chain risk management (SCRM) program to assess CSP or vendor risks is a due diligence practice.

Actually performing the assessment is an example of due care.

Remember, the customer organization is responsible.

Any organization that uses cloud services without adequately mitigating the risks is likely to be found negligent in a breach

This results in problems for data controller

ASSESSMENT OF RISK ENVIRONMENT

Common Criteria (ISO/IEC 15408-1)

Enables an objective evaluation to validate that a particular product or system satisfies a defined set of security requirements.

Assures customers that security products they purchase have been thoroughly tested by independent third-party testers

...and meets customer requirements.

The certification of the product only certifies product capabilities.

Designed to provide assurances for security claims by vendors

If misconfigured or mismanaged, software is no more secure than anything else the customer might use.

ASSESSMENT OF RISK ENVIRONMENT

Common Criteria (ISO/IEC 15408-1)

Evaluation is done through testing laboratories where the product or platform is evaluated against a standard set of criteria.

The result is an **Evaluation Assurance Level (EAL)**, which defines how robust the security capabilities are in the evaluated product

Most CSPs do not have common criteria evaluations over their entire environments, but many cloud-based products do

It's up to the customer to review details CC assurances

If misconfigured or mismanaged, software is no more secure than anything else the customer might use.

ASSESSMENT OF RISK ENVIRONMENT

CSA STAR **S**ecurity, **T**rust, **A**ssurance, and **R**isk

When evaluating the risks in a specific CSP or other cloud service, the CSA STAR can be a useful, lightweight method for ascertaining risks.

Contains evaluations of cloud services against the CSA's cloud controls matrix (CCM)

Organizations can opt for self-assessed or third-party- assessed cloud services. This will affect the level of assurance (low or high)

Overall, CSA Star is considered lightweight, lower assurance certification for the CSPs that use it.

EU Cybersecurity Certification Scheme on Cloud Services

EUCS

ENISA has published a standard for certifying the cybersecurity practices present in cloud environments

The framework, known as EUCS, defines a set of evaluation criteria for various cloud service and deployment models.

The goal is producing security evaluation results that allow comparison of the security posture across different cloud providers.

The standard was still under development as of 2022, so adoption is not yet widespread

5. CLOUD SECURITY OPERATIONS

6.5 Understand Outsourcing and Cloud Contract Design

Business requirements
(e.g., service-level agreement (SLA), master service agreement (MSA), statement of work (SOW))

Vendor management
(e.g., vendor assessments, vendor lock-in risks, vendor viability, escrow)

Contract management
(e.g., right to audit, metrics, definitions, termination, litigation, assurance, compliance, access to cloud/data, cyber risk insurance)

Supply-chain management
(e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27036)

THIRD-PARTY RISKS

Supply chain

Supply chain security has become a significant concern for organizations.

Includes, suppliers, manufacturers, distributors, and customers.

A breach at any link in the supply chain can result in business impact.

Vendor management

Risk of "island hopping attack"

Many orgs are reducing the number of vendors they work with and requiring stricter onboarding procedures.

Vendors may be required to submit to an external audit and agree to strict communication and reporting requirements in event of potential breach.

System integration

Potential for Increased risk of insider attack

System integration partners working on systems often have privileged remote or physical access, necessitating security measures and process controls.

BUSINESS REQUIREMENTS – SLA, MSA, SOW

MSA

Master Service Agreement

In legal terms, a cloud customer and a CSP enter into a master service agreement (MSA)

This is defined as any contract that two or more parties enter into as a service agreement

MSA should address compliance and process requirements the customer is passing along to CSP

Legal counsel is most often responsible for contracts, but security should be involved to share requirements

MSA should include breach notification – CSP duty to inform the customer of a breach within a specific time period after detection.

SERVICE-LEVEL AGREEMENTS

Stipulate performance expectations such as maximum downtimes and often include penalties if the vendor doesn't meet expectations.

Generally used with external vendors (like CSP) and is legally binding

SERVICE-LEVEL AGREEMENTS

Stipulate performance expectations such as maximum downtimes and often include penalties if the vendor doesn't meet expectations.

Often includes financial penalties for non-performance, and may allow customer to terminate a contract

BUSINESS REQUIREMENTS – SLA, MSA, SOW

SLAs should be written to ensure that the organization's service level requirements (SLRs) are met.

SLAs are best suited for defining recurring, discrete, measurable items the parties agree upon.

Common elements documented in SLAs include:

- Uptime guarantees
- SLA violation penalties
- SLA violation penalty exclusions and limitations
- Suspension of service clauses
- Provider liability
- Data protection and management
- Disaster recovery and recovery point objectives
- Security and privacy notifications and timeframes

STATEMENT OF WORK

Legal document usually created after an MSA has been executed and governs a specific unit of work.

MSA may document services and prices, a SOW covers requirements, expectations, and deliverables for a project.

MSA focus is "overall, ongoing", SOW is "limited & specific"

THIRD-PARTY RISK MANAGEMENT

NDA

NON-DISCLOSURE AGREEMENT

A contract with vendors and suppliers not to disclose the company’s confidential information.

A "mutual NDA" binds both parties in the agreement

VENDOR MANAGEMENT

Managing risk is complicated when parts of the organization's IT infrastructure exist outside the organization's direct control.

The practices of SCRM and vendor management overlap significantly.

However, in many cases vendor management will include more activities related to operational risks.

Cloud computing involves outsourcing ongoing organizational processes and infrastructure to a service provider

Therefore, the cloud requires more continuous management activities to monitor and manage the vendor relationship

VENDOR MANAGEMENT

Cloud professionals need strong project *and* people management to effectively perform vendor management activities, including:

Assess vendors:

Security practitioners should participate in the initial selection process for a CSP, which involves assessing security risks present in CSP and related services.

For many customers, this process will entail reviewing security reports like a SOC 2 on an annual basis after the CSP has undergone their yearly audit.

Assess vendor lock-in risks:

This assessment will require knowledge of not only the CSP's offerings but the architecture and strategy the customer organization intends to use.

Using any unique CSP offerings, such as artificial intelligence/machine learning (AI/ML) platforms, can result in a service that is dependent on that specific CSP.

VENDOR MANAGEMENT

Cloud professionals need strong project *and* people management to effectively perform vendor management activities, including:

Assess vendor viability:

This is often a process that is not conducted by the security team, as it deals with operational risk.

Assessing the viability of vendors may involve reviews of public information like:

- financial statements
- the CSP's performance history and reputation
- or even formal reports like a SOC 1

All of these identify potential weaknesses that could impact the CSP's ability to continue operations.

VENDOR MANAGEMENT

Cloud professionals need strong project *and* people management to effectively perform vendor management activities, including:

Explore escrow options:

Escrow is a legal term used when a trusted third party holds something on behalf of two or more other parties, such as source code or encryption keys.

ESCROW SCENARIO:

A software development company may wish to protect the intellectual property of their source code.

However, if they go out of business, their customers are left with an unmaintainable system.

In this scenario, an escrow provider could hold a copy of the source code and release it to customers in the event the provider is no longer in business.

CONTRACT MANAGEMENT

Organizations must employ adequate governance structures to **monitor contract terms and performance** and **be aware of outages** and **any violations of stated agreements**.

Contract Clauses

A contract clause is a specific article of related information that specifies the agreement between the contracting parties.

Some common contract clauses that should be considered for any CSP or other data service provider include the following:

-Right to audit

-Metrics

-Definitions

-Termination

-Litigation

-Assurance

-Compliance

-Access to cloud/data

CONTRACT MANAGEMENT

Contract Clauses

Right to audit

The customer can request the right to audit the service provider to ensure compliance with the security requirements agreed in the contract.

Contracts often written to allow the CSP's standard audits (e.g., SOC 2, ISO 27001 certification) to be used in place of a customer-performed audit.

Metrics

If there are specific indicators that the service provider must provide to the customer, they can be documented in a contract.

Tell you "how compliance with the agreement will be measured"

Contract Clauses

Definitions

A contract is a legal agreement between multiple parties.

It is essential that all parties share a common understanding of the terms and expectations.

Defining key terms like security, privacy, and key practices like breach notifications can avoid misunderstandings.

Termination

Termination refers to ending the contractual agreement.

This clause will typically define conditions under which either party may terminate the contract

May also specify consequences if the contract is terminated early.

CONTRACT MANAGEMENT

Contract Clauses

Litigation

This is an area where legal counsel must be consulted.

Agreeing to terms for litigation can severely restrict the organization's ability to pursue damages if something goes wrong.

Assurance

Defining assurance requirements sets expectations for both the provider and customer.

Many contracts specify that a provider must furnish a SOC 2 or equivalent to the customer on an annual basis

CONTRACT MANAGEMENT

Contract Clauses

Compliance:

Any customer compliance requirements that flow to the provider must be documented and agreed upon in the contract.

Data controllers that use cloud providers as data processors must ensure that adequate security safeguards are available for that data

Access to cloud/data:

Clauses dealing with customer access can be used to avoid risks associated with vendor lock-in.

CONTRACT MANAGEMENT

Cyber risk insurance is designed to help an organization reduce the financial impact of risk by transferring it to an insurance carrier.

In the event of a security incident, the insurance carrier can help offset associated costs, such as digital forensics and investigation, data recovery, system restoration.

It may even cover legal or regulatory fines associated with the incident.

Cyber insurance carriers are in the business of risk management and are unlikely to offer coverage to an organization lacking controls to mitigate risk.

Cyber insurance requires organizations to pay a premium for the insurance plan.

Most plans have a **limit of coverage** that caps how much the insurance carrier pays.

CONTRACT MANAGEMENT

Cyber risk insurance is designed to help an organization reduce the financial impact of risk by transferring it to an insurance carrier.

There may also be **sub-limits**, which cap the amount that will be paid for specific types of incidents such as ransomware or phishing.

An insurance broker can be a useful resource when investigating insurance options for your organization's circumstances, including

- the amount of coverage needed
- different types of coverage such as business interruption or cyber extortion
- security controls that the insurance carrier requires, such as MFA

Cyber risk insurance usually covers costs associated with the following:

-Investigation
-Direct business losses
-Recovery costs
-Legal notifications
-Lawsuits
-Extortion
-Food and related expenses

CONTRACT MANAGEMENT

Cyber risk insurance

Investigation

Costs associated with the forensic investigation to determine the extent of an incident.

This often includes costs for third-party investigators.

Direct business losses

Direct monetary losses associated with downtime or data recovery, overtime for employees, and, oftentimes, reputational damages to the organization.

Recovery costs

These may include costs associated with replacing hardware or provisioning temporary cloud environments during contingency operations.

They may also include services like forensic data recovery or negotiations with attackers to assist in recovery.

CONTRACT MANAGEMENT

Cyber risk insurance

Legal notifications

Costs are associated with required privacy and breach notifications required by relevant laws.

Lawsuits

Policies can be written to cover losses and payouts due to class action or other lawsuits against a company after a cyber incident.

Extortion

The insurance to pay out ransomware demands is growing in popularity.

This may include direct payments to ensure data privacy or accessibility by the company.

CONTRACT MANAGEMENT

Cyber risk insurance

Food and related expenses

Incidents often require employees to work extended hours or travel to contingency sites.

Costs associated with the incident response, including catering and lodging, may be covered, even though they are not usually thought of as IT costs!

SUPPLY CHAIN MANAGEMENT

Managing risk in the supply chain focuses on both **operational risks**, to ensure that suppliers are capable of providing the needed services, and **security risks**

The supply chain should always be considered in any business continuity or disaster recovery planning.

Proactive measures including contract language and assurance processes can be used to quantify the risks associated with using suppliers like CSPs…

as well as the effectiveness of these suppliers' risk management programs.

ISO/IEC 27036-1:2021 Cybersecurity — Supplier relationships.
The ISO 27000 family of standards includes a specific ISO standard dedicated to supply chain cybersecurity risk management.

SUPPLY CHAIN MANAGEMENT

ISO/IEC 27036-1:2021 Cybersecurity — Supplier relationships.

ISO 27036:2021 provides a set of practices and guidance for managing cybersecurity risks in supplier relationships.

This standard is particularly useful for organizations that use ISO 27001 for building an ISMS or ISO 31000 for risk management

ISO/IEC 27036 builds on concepts found in those standards.

ISO/IEC 27036 comprises four parts, including:

- Part 1: Overview and concepts
- Part 2: Requirements
- Part 3: Guidelines for information and communication technology supply chain security
- Part 4: Guidelines for security of cloud services

ISO 27036, like other ISO standards, is not a free resource.

SUPPLY CHAIN MANAGEMENT

ISO/IEC 27036-1:2021 Cybersecurity — Supplier relationships.

Part 1: Overview and concepts,” which provides an overview and foundation for a supply chain management capability.

Part 2: Requirements,” which provides a set of best practices and techniques for designing and implementing the supply chain management function.

Part 3: Guidelines for information and communication technology supply chain security,” which is of particular concern for security practitioners, as it lays out practices and techniques specific to managing security risks in the supply chain.

Part 4: Guidelines for security of cloud services,” which is the most relevant to cloud security practitioners. This standard deals with practices and requirements for managing supply chain security risk specific to cloud computing and CSP.

SUPPLY CHAIN MANAGEMENT

ISO/IEC 27036-1:2021 Cybersecurity — Supplier relationships.

Additional resources focusing on supply chain worth review include:

NISTIR 8276, “Key Practices in Cyber Supply Chain Risk Management: Observations from Industry”;

NIST SP 800-161,” Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations”;

ENISA publication “Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward.”, published in 2015

INSIDE CLOUD

AND SECURITY

THANKS

FOR WATCHING!