CISSP EXAM CRAM

THE COMPLETE COURSE

DOMAIN 2

Asset Security

INSIDE CLOUD AND SECURITY

WHAT'S NEW IN DOMAIN 2?

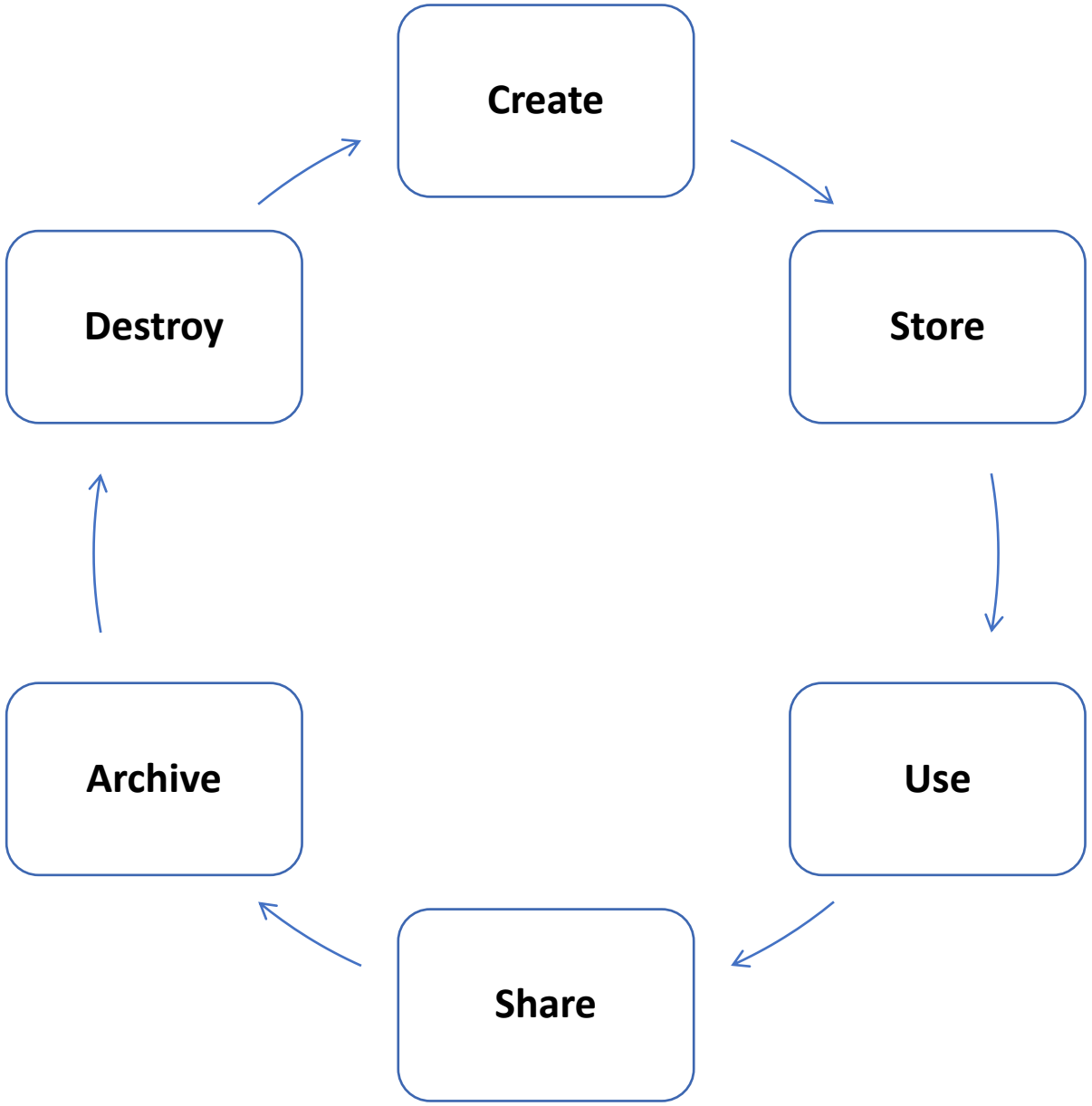
2.3 Provision resources securely

2.4 Manage data lifecycle

2.6 Determine data security controls and compliance requirements(DRM, CASB, DLP)

covered in 2018. elevated in 2021

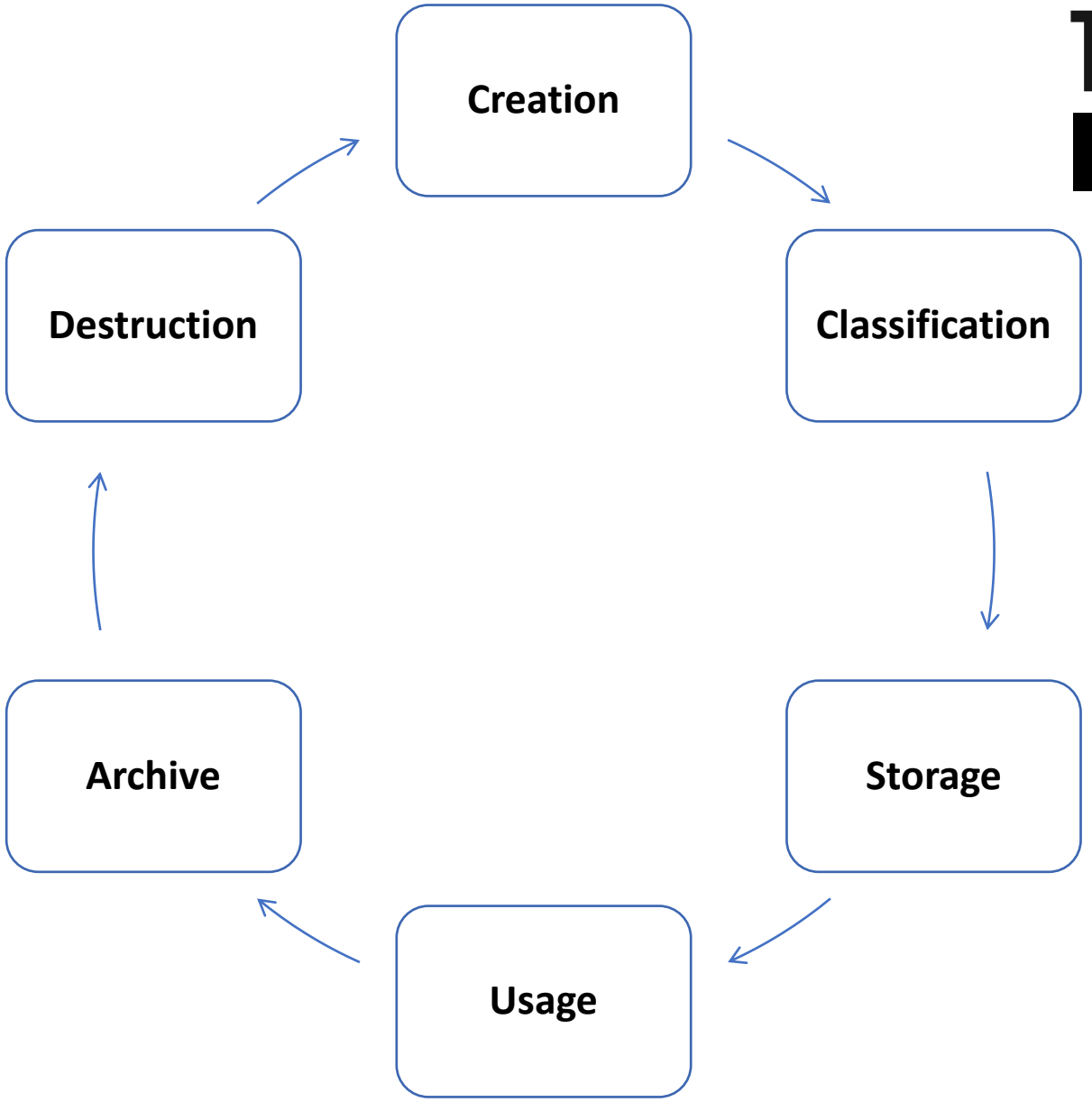
THE DATA LIFECYCLE



2.4 Manage data lifecycle

THE INFORMATION LIFECYCLE

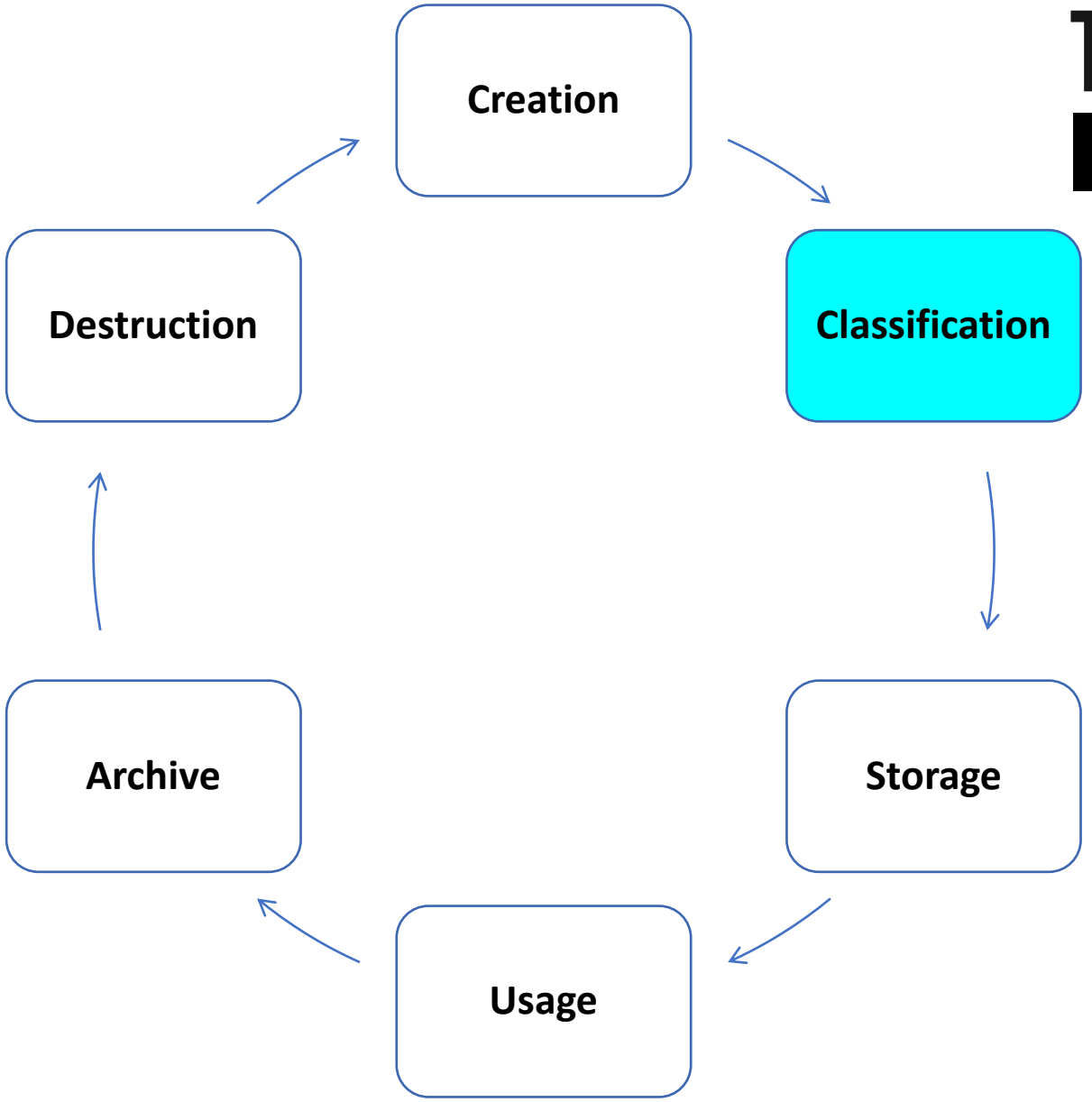
DOMAIN 7: SECURITY OPERATIONS



Focuses a bit more on "information protection"

THE INFORMATION LIFECYCLE

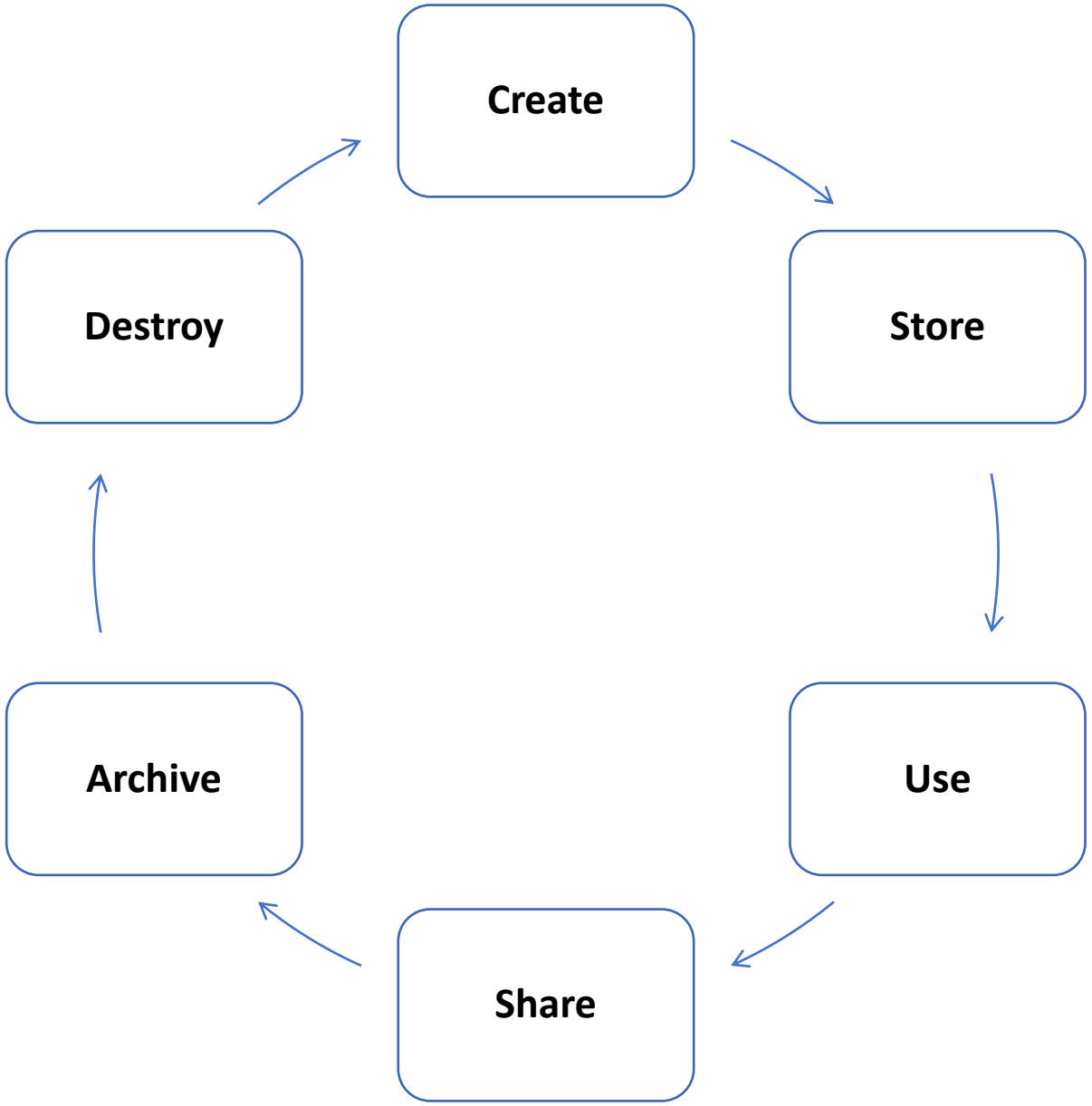
DOMAIN 7: SECURITY OPERATIONS



Focuses a bit more on "information protection"

there isn't a consistent standard used to identify each stage or phase of a data lifecycle.

THE DATA LIFECYCLE

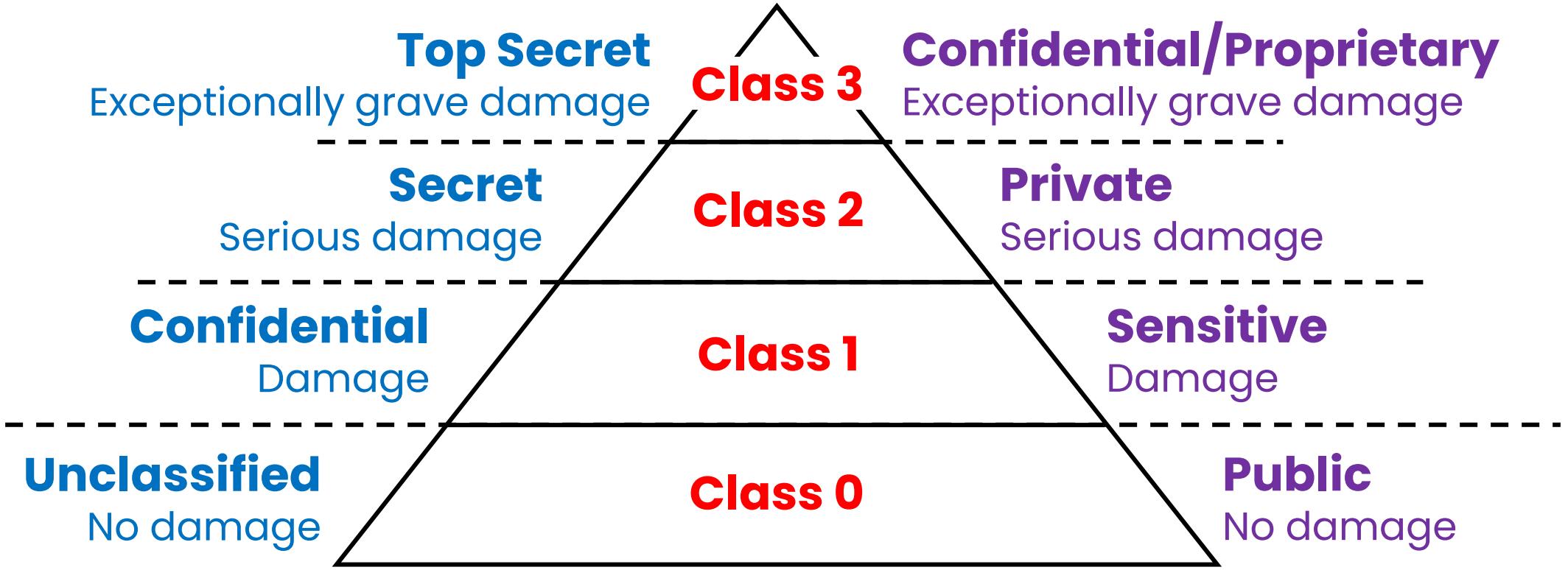


2.4 Manage data lifecycle

DOMAIN 2: DATA CLASSIFICATION

Government

Non-gov't (public)



Exam Outline

2.1 Identify and **classify** information and assets

2.2 Determine and maintain information and asset **ownership** 2 roles key for exam!

2.3 Protect **privacy**

2.4 Ensure appropriate **asset retention** (and data destruction)

2.5 Determine data **security controls**

2.6 Establish information and **asset handling requirements**

labeling, markings, chain of custody

WHAT'S NEW IN DOMAIN 2?

2.3 Provision resources securely

2.4 Manage data lifecycle

2.6 Determine data security controls and compliance requirements(DRM, CASB, DLP)

covered in 2018. elevated in 2021

Data Security Controls

Marking, Labeling, Handling, Classification.
Classification is the most important!

Data handling. Shipping, Chain of Custody.
Don't open boxes!

Data destruction. Erasing, Clearing (overwriting w/ unclassified data).

Record retention. If the retention policy is 1 year, it should be destroyed when it ages out (>1 year).

Tape Backup Security. Secure facility, tapes labeled ensures all understand the classification of the data.

Data Destruction Methods

Erasing. performing a delete operation against a file, files, or media. data is typically recoverable

Clearing (overwriting). preparing media for reuse and ensuring data cannot be recovered using traditional recovery tools

Purging. a more intense form of clearing that prepares media for reuse in less secure environments.

Degaussing. creates a strong magnetic field that erases data on some media.

Destruction. the final stage in the lifecycle of media and is the most secure method of sanitizing media.

Security Control Baseline

Provides a listing of controls that an organization can apply as a baseline.

FOR THE EXAM

Be familiar with **record retention** (and **data destruction**)

FOR THE EXAM

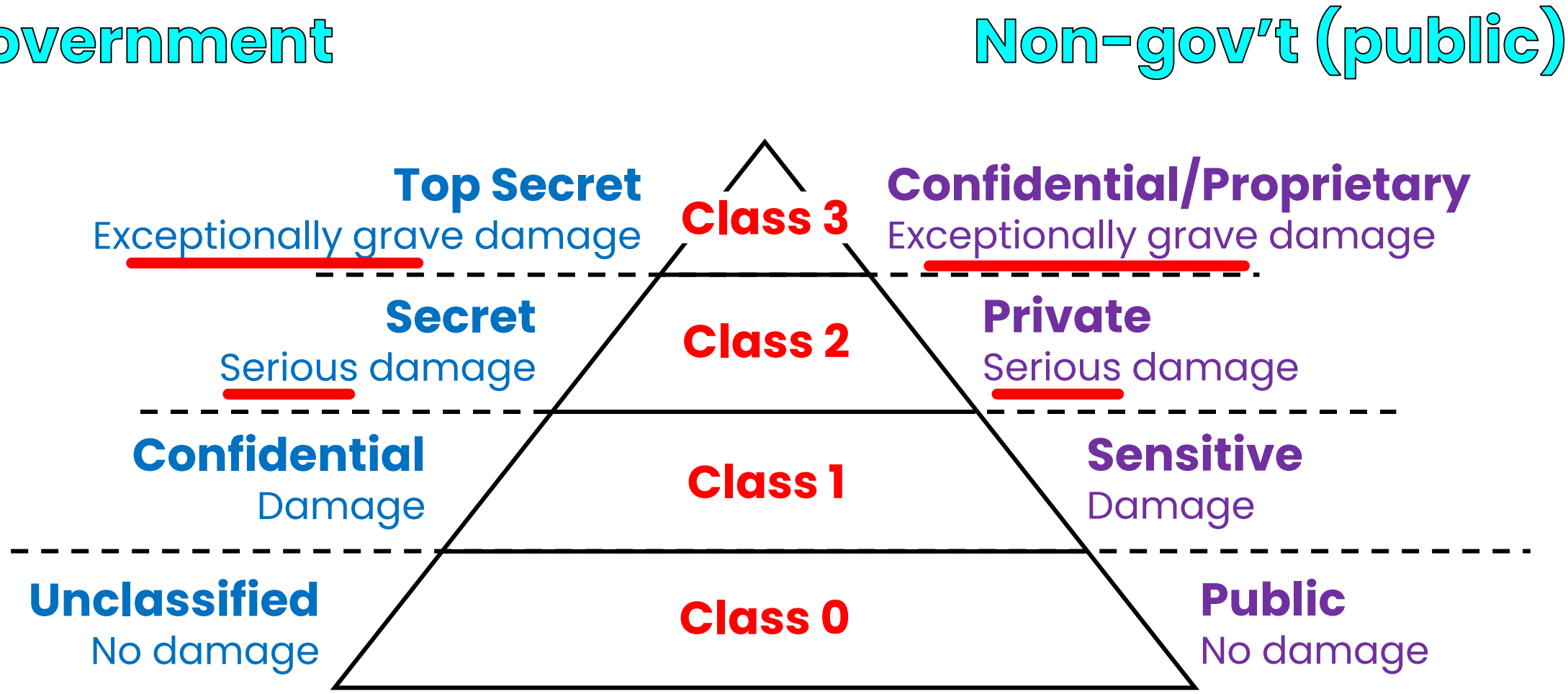
Keeping data longer than necessary presents unnecessary **legal issues**

Data protection

Confidentiality is often protected through encryption (at rest and in transport)

We'll cover encryption in Lesson 3 (DOMAIN 3)

DOMAIN 2: DATA CLASSIFICATION



We'll talk "**sensitive but unclassified**" in cryptography (DOMAIN 3)

Asset Classifications

Asset classifications should match the data classifications.

Defining Sensitive Data

Sensitive data is any information that isn't public or unclassified.

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

Protected Health Information (PHI). and health-related information that can be related to a specific person. covered by HIPAA (from DOMAIN 1)

KNOW THESE TWO ROLES!

The most likely to show up on the exam?

Data Owner. Usually a member of senior management. Can delegate some day-to-day duties. Cannot delegate total responsibility.

Data Custodian. Usually someone in the IT department. Does not decide what controls are needed, but does implement controls for data owner

TIP: if question mentions "day-to-day" it's custodian!

KNOW THESE TWO ROLES!

The most likely to show up on the exam?

Data Owner. Usually a member of senior management. Can delegate some day-to-day duties. Cannot delegate total responsibility.

Data Custodian. Usually someone in the IT department. Does not decide what controls are needed, but does implement controls for data owner

TIP: if question mentions "day-to-day" it's custodian!

OTHER ROLES

Be prepared to answer questions on other roles

Data Administrators. Responsible for granting appropriate access to personnel (often via RBAC).

User. any person who accesses data via a computing system to accomplish work tasks.

Business/Mission Owners. Can overlap with the responsibilities of the system owner or be same role

Asset Owners. Owns asset or system that processes sensitive data and associated security plans

GDPR Terms and Requirements

Be prepared to answer questions on other roles

Data Processor. A natural or legal person, public authority, agency, or other body, which processes personal data solely on behalf of the data controller.

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

Data Transfer. GDPR restricts data transfers to countries outside the EU.

Reducing GDPR Exposure

Steps to reduce or eliminate GDPR requirements

Anonymization. The process of removing all relevant data so that it is impossible to identify original subject or person.

If done effectively, the GDPR is no longer relevant for the anonymized data.

Pseudonymization. The process of using pseudonyms (aliases) to represent other data.

Good only if you don't need the data!

Can result in less stringent requirements than would otherwise apply under the GDPR.

Use if you need data and want to reduce exposure

FOR THE EXAM

Be familiar with the **GDPR** terms, data roles, security controls.

Notification of data breach must be made within 72 hours