CISSP

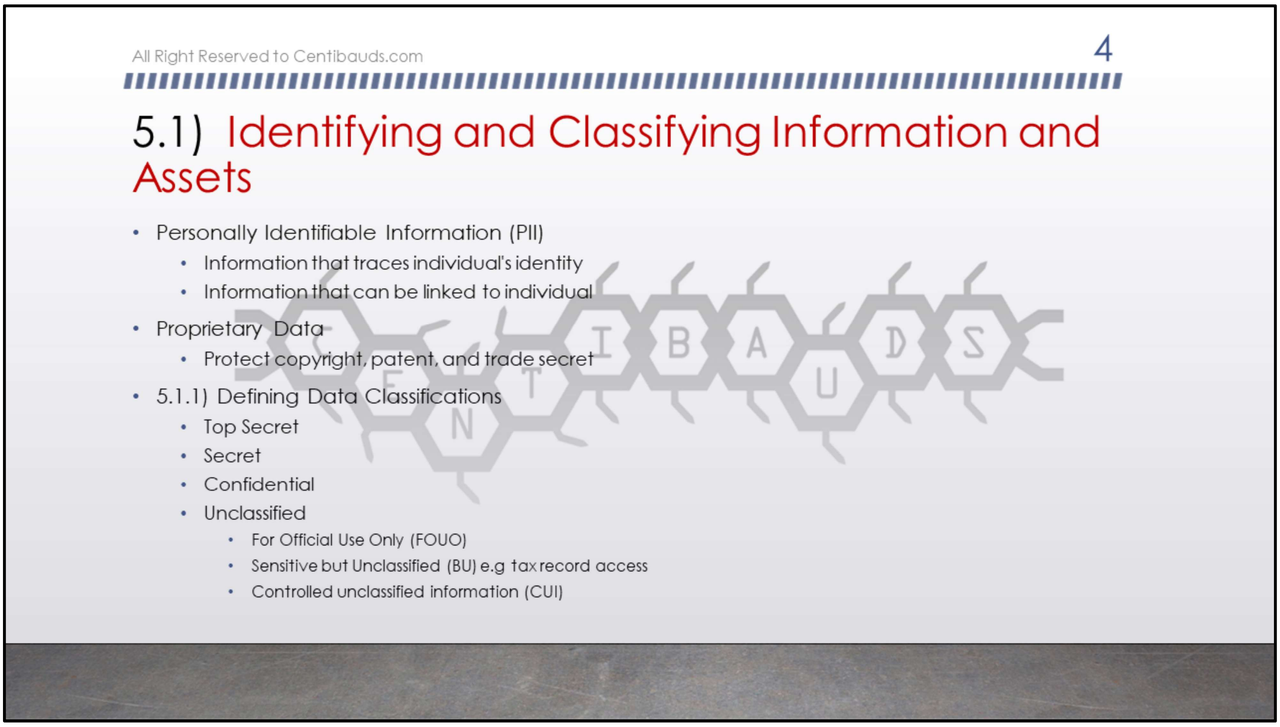
Aitizaz Uddin Syed (M.Engg, CISSP, CISSP-ISSAP, CCSP, CRISC, GICSP, TOGAF)

All Right Reserved to Centibauds.com

Domain 2
Asset Security

CHAPTER 5

Protecting Security of Assets



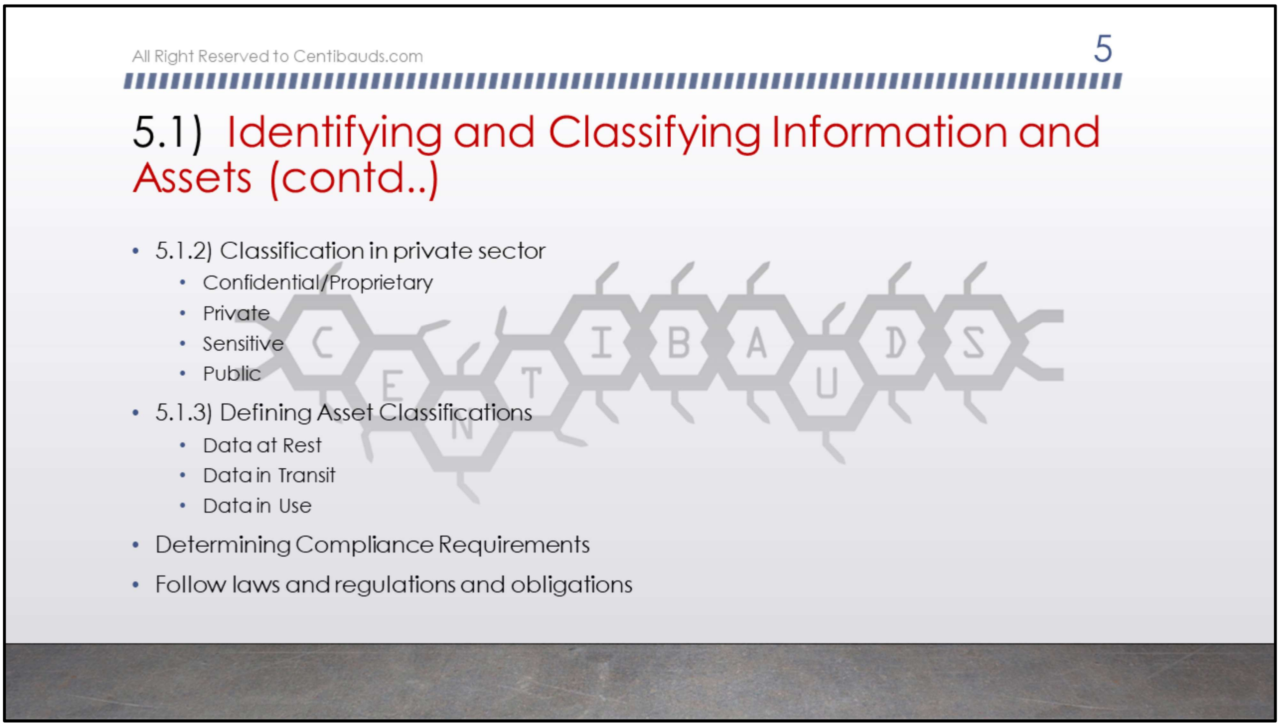
All Right Reserved to Centibauds.com

5.1) Identifying and Classifying Information and Assets

- Personally Identifiable Information (PII)
  - Information that traces individual's identity
  - Information that can be linked to individual
- Proprietary Data
  - Protect copyright, patent, and trade secret
- 5.1.1) Defining Data Classifications
  - Top Secret
  - Secret
  - Confidential
  - Unclassified
    - For Official Use Only (FOUO)
    - Sensitive but Unclassified (BU) e.g tax record access
    - Controlled unclassified information (CUI)

CENTIBAUDS

-Top Secret: Grave damage to national security upon disclosure
-Secret: Cause serious damage to national security upon disclosure
-Confidential: Might cause significant damage to national security upon disclosure
-Unclassified: Based on Freedom of Information Act (FoIA) it should be allowed to view for anyone



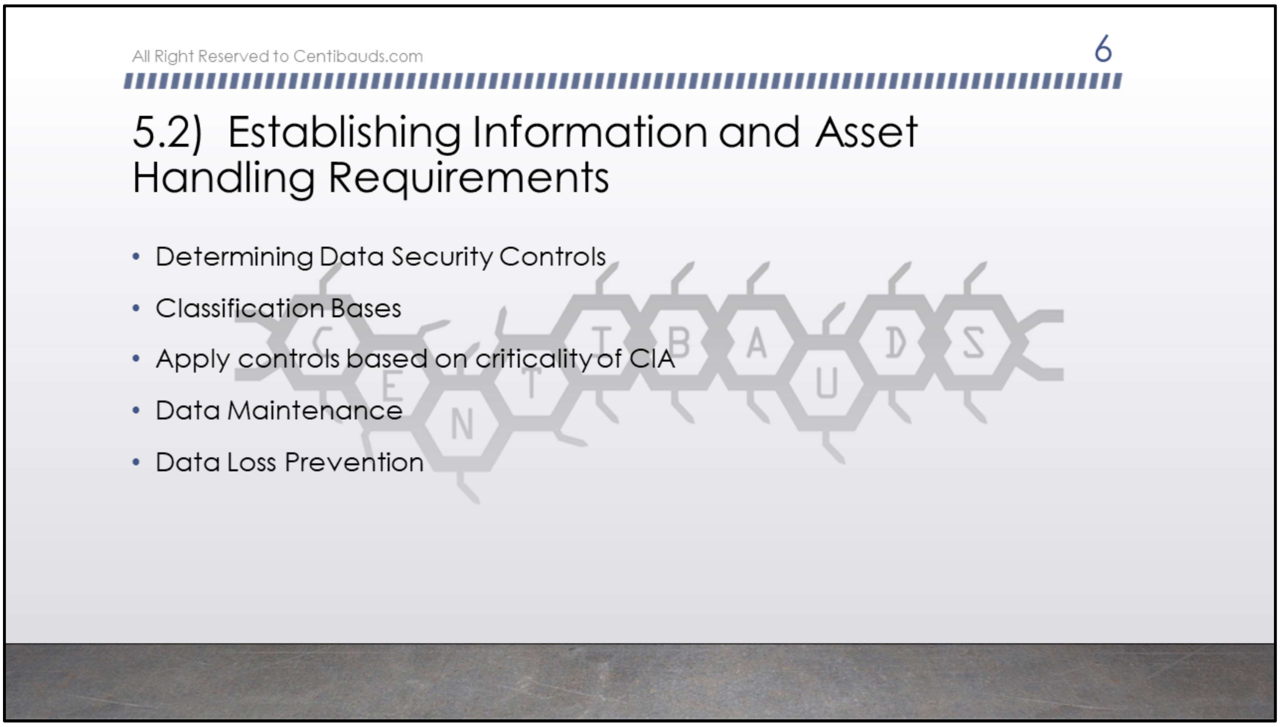
All Right Reserved to Centibauds.com

5

5.1) Identifying and Classifying Information and Assets (contd..)

- 5.1.2) Classification in private sector
  - Confidential/Proprietary
  - Private
  - Sensitive
  - Public
- 5.1.3) Defining Asset Classifications
  - Data at Rest
  - Data in Transit
  - Data in Use
- Determining Compliance Requirements
- Follow laws and regulations and obligations

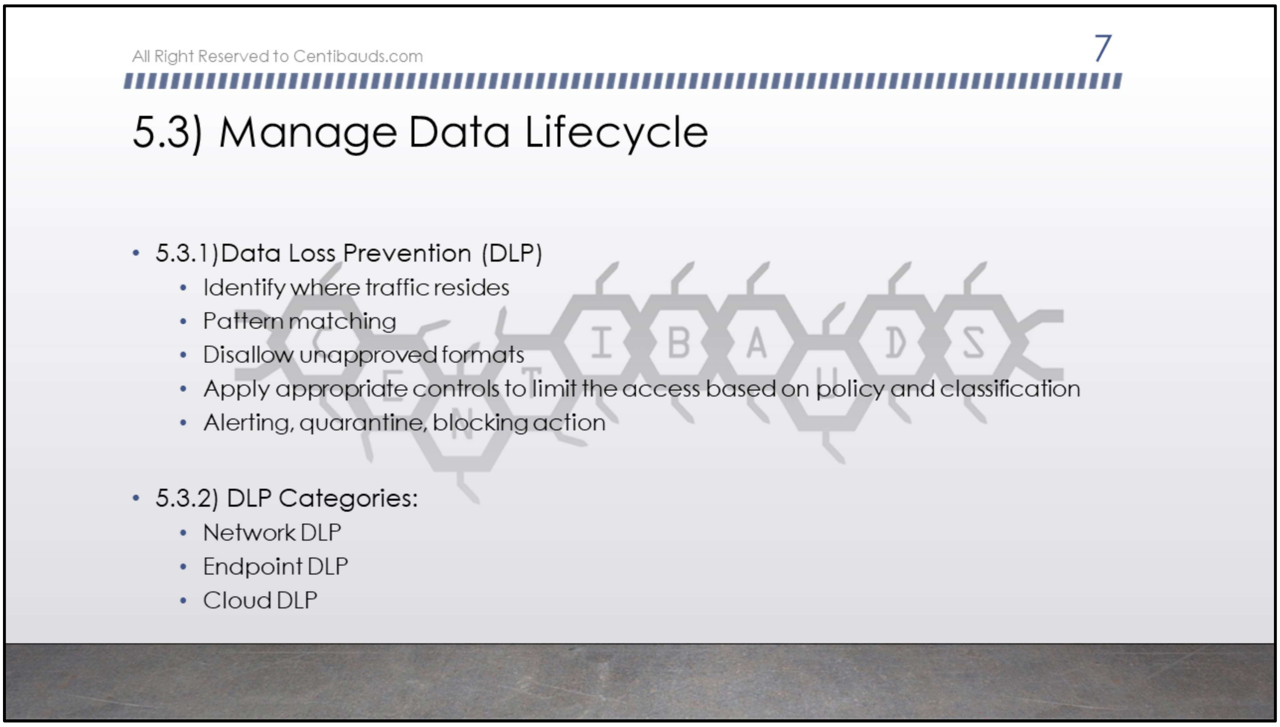
-Confidential/Proprietary	e.g the data, proprietary business knowledge
-Private	PII, PHI
-Sensitive	S/W, IP, functions, network LLD, HLD
-Public	Social media and marketing content, Price list etc



All Right Reserved to Centibauds.com

5.2) Establishing Information and Asset Handling Requirements

- Determining Data Security Controls
- Classification Bases
- Apply controls based on criticality of CIA
- Data Maintenance
- Data Loss Prevention



All Right Reserved to Centibauds.com

5.3) Manage Data Lifecycle

- 5.3.1)Data Loss Prevention (DLP)
  - Identify where traffic resides
  - Pattern matching
  - Disallow unapproved formats
  - Apply appropriate controls to limit the access based on policy and classification
  - Alerting, quarantine, blocking action
- 5.3.2) DLP Categories:
  - Network DLP
  - Endpoint DLP
  - Cloud DLP

-Network DLP

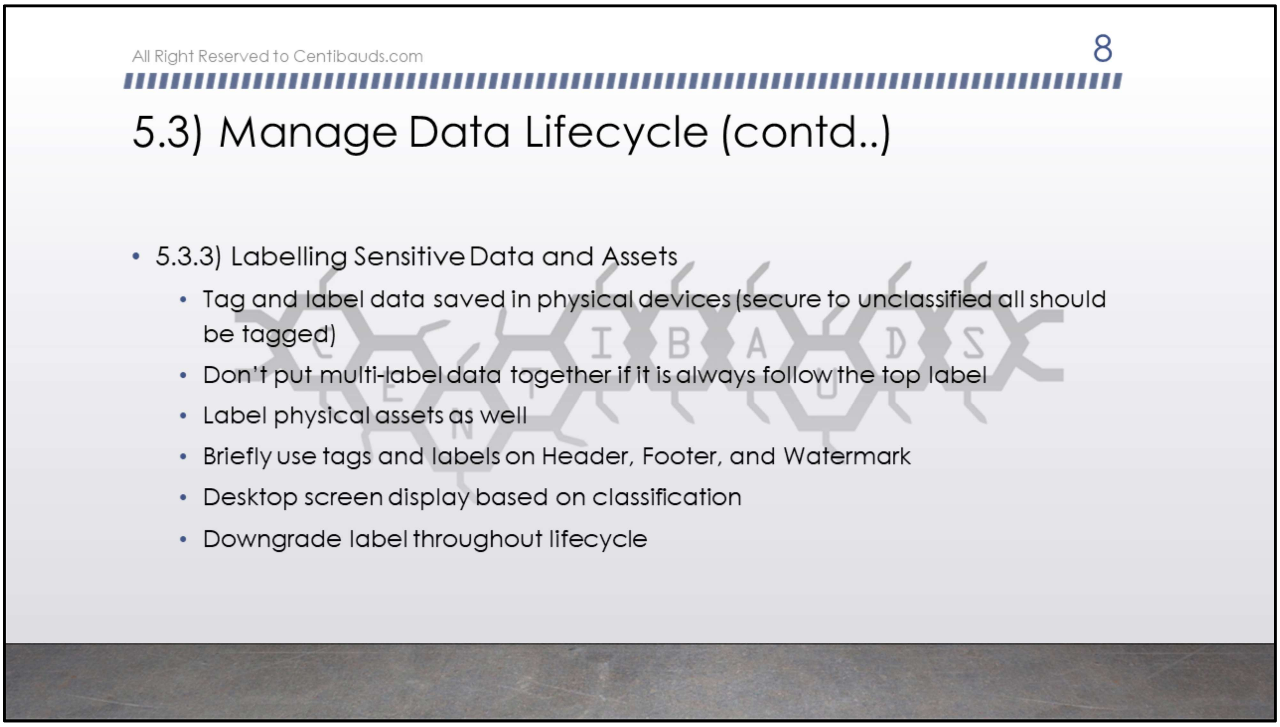
- Scan traffic passing through
- Prevent asset leaves organization

Endpoint DLP

- Discover and Scan for assets
- Prevent file or document movement
- Snapshot, USB, email and other control

Cloud DLP

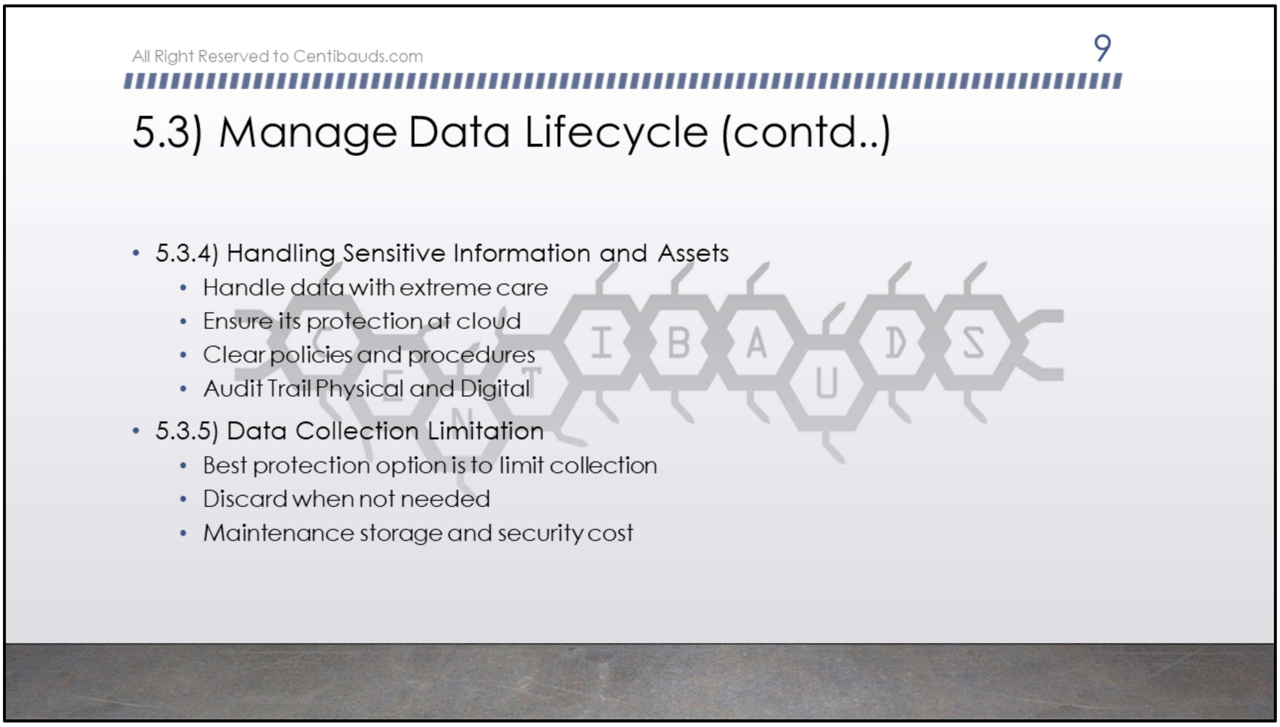
- Multiple services on cloud related to DLP e.g exiting traffic scan
- Brand protection
- CASB



All Right Reserved to Centibauds.com

5.3) Manage Data Lifecycle (contd..)

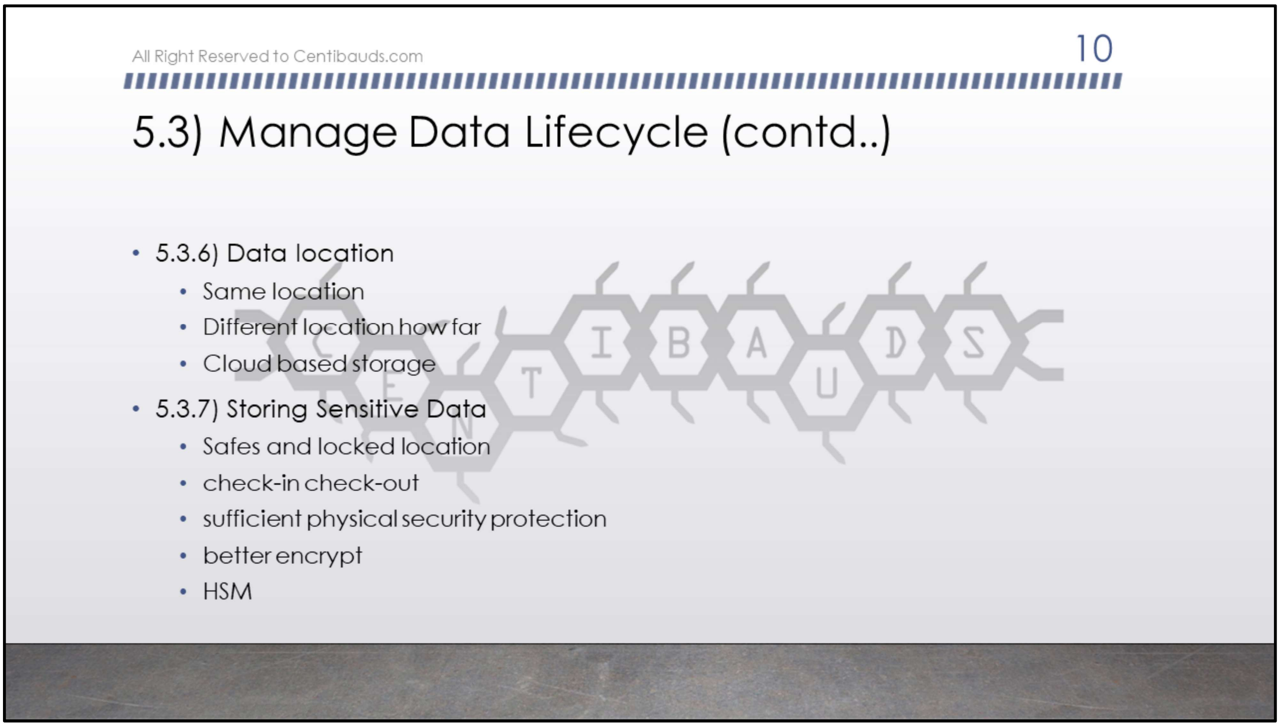
- 5.3.3) Labelling Sensitive Data and Assets
  - Tag and label data saved in physical devices (secure to unclassified all should be tagged)
  - Don't put multi-label data together if it is always follow the top label
  - Label physical assets as well
  - Briefly use tags and labels on Header, Footer, and Watermark
  - Desktop screen display based on classification
  - Downgrade label throughout lifecycle



All Right Reserved to Centibauds.com

5.3) Manage Data Lifecycle (contd..)

- 5.3.4) Handling Sensitive Information and Assets
  - Handle data with extreme care
  - Ensure its protection at cloud
  - Clear policies and procedures
  - Audit Trail Physical and Digital
- 5.3.5) Data Collection Limitation
  - Best protection option is to limit collection
  - Discard when not needed
  - Maintenance storage and security cost

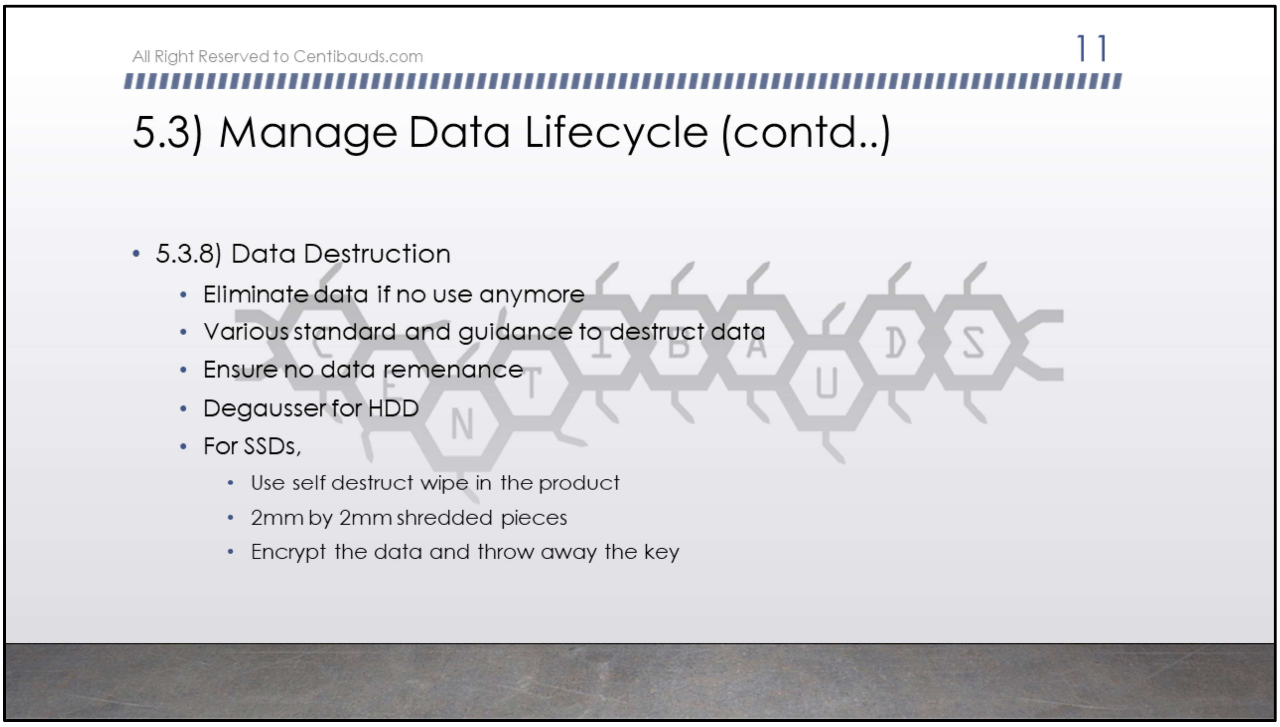


All Right Reserved to Centibauds.com

5.3) Manage Data Lifecycle (contd..)

- 5.3.6) Data location
  - Same location
  - Different location how far
  - Cloud based storage
- 5.3.7) Storing Sensitive Data
  - Safes and locked location
  - check-in check-out
  - sufficient physical security protection
  - better encrypt
  - HSM

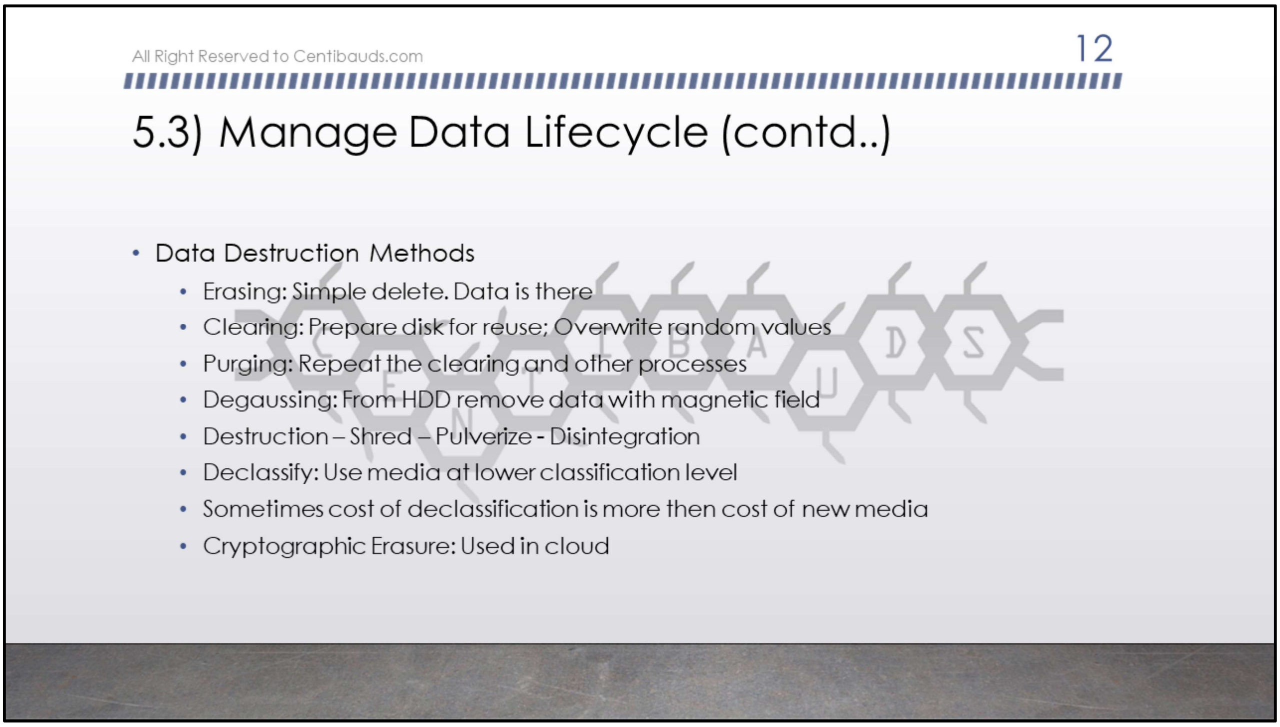
CENTIBAUDS



All Right Reserved to Centibauds.com

5.3) Manage Data Lifecycle (contd..)

- 5.3.8) Data Destruction
  - Eliminate data if no use anymore
  - Various standard and guidance to destruct data
  - Ensure no data remenance
  - Degausser for HDD
  - For SSDs,
    - Use self destruct wipe in the product
    - 2mm by 2mm shredded pieces
    - Encrypt the data and throw away the key

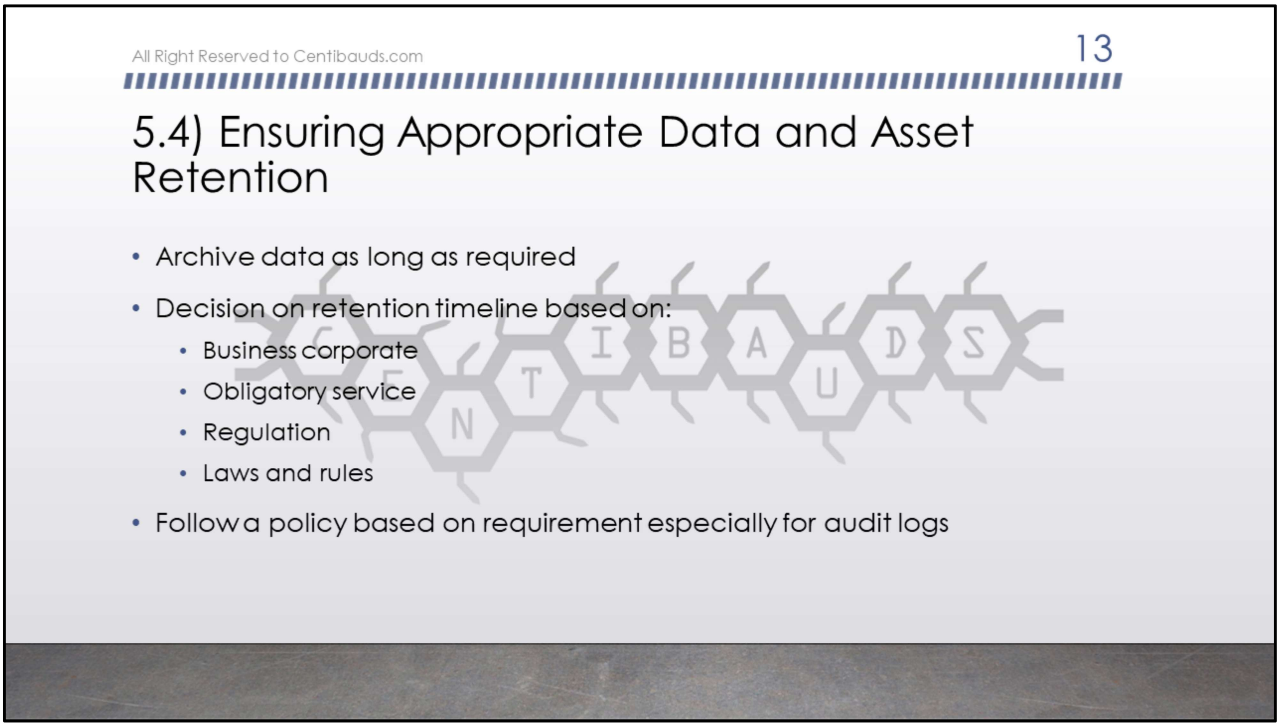


All Right Reserved to Centibauds.com

5.3) Manage Data Lifecycle (contd..)

- Data Destruction Methods
  - Erasing: Simple delete. Data is there
  - Clearing: Prepare disk for reuse; Overwrite random values
  - Purging: Repeat the clearing and other processes
  - Degaussing: From HDD remove data with magnetic field
  - Destruction – Shred – Pulverize - Disintegration
  - Declassify: Use media at lower classification level
  - Sometimes cost of declassification is more then cost of new media
  - Cryptographic Erasure: Used in cloud

-Pulverize means make something unusable to the purpose

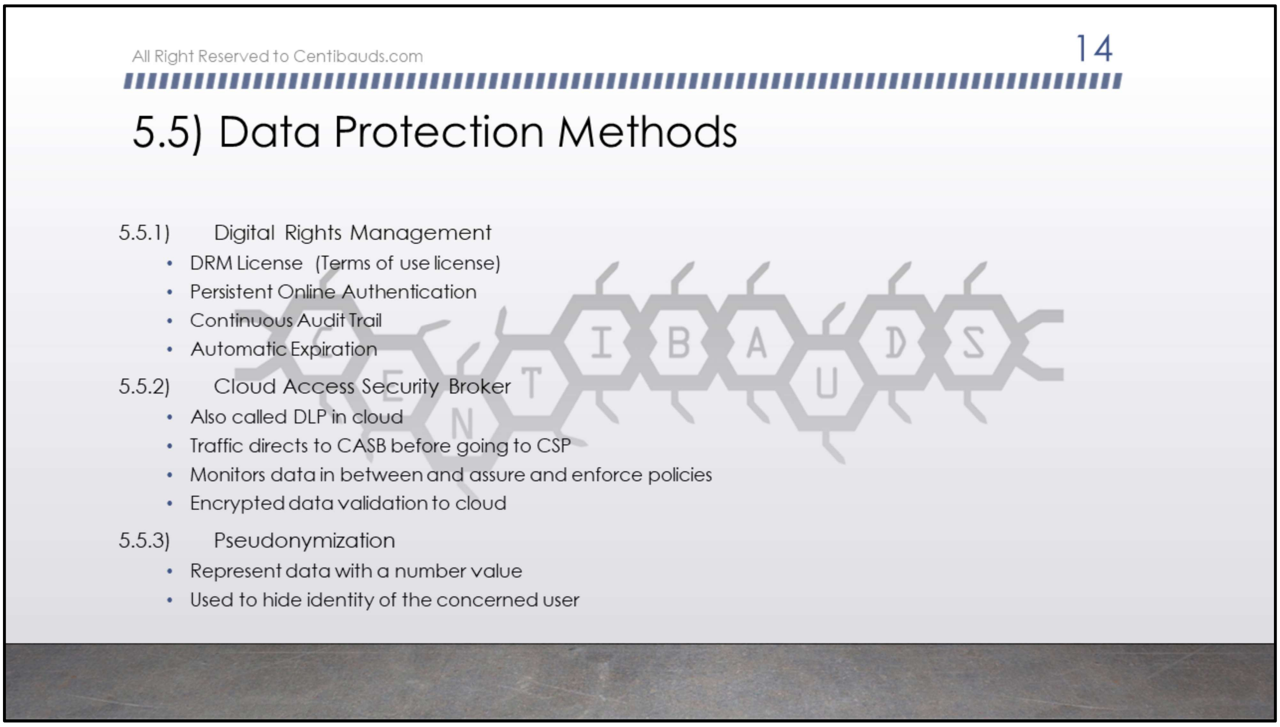


All Right Reserved to Centibauds.com

5.4) Ensuring Appropriate Data and Asset Retention

- Archive data as long as required
- Decision on retention timeline based on:
  - Business corporate
  - Obligatory service
  - Regulation
  - Laws and rules
- Follow a policy based on requirement especially for audit logs

CENTIBAUDS



All Right Reserved to Centibauds.com

5.5) Data Protection Methods

5.5.1) Digital Rights Management

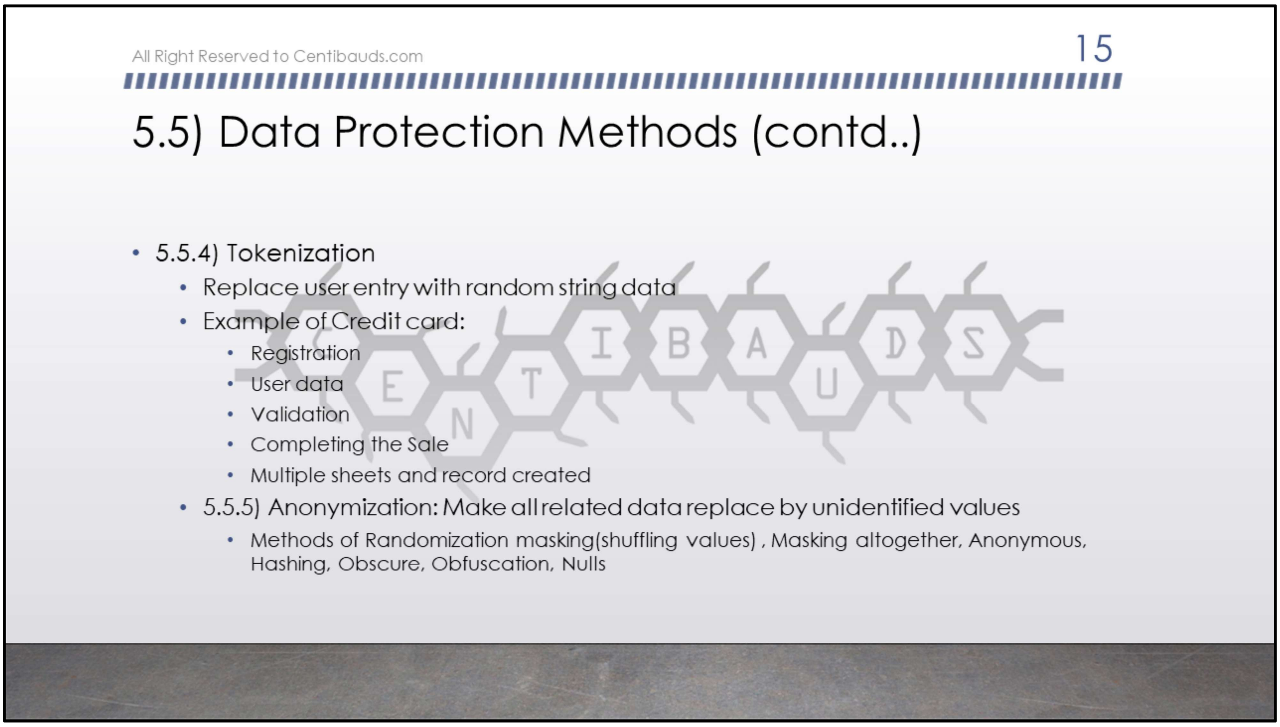
- DRM License (Terms of use license)
- Persistent Online Authentication
- Continuous Audit Trail
- Automatic Expiration

5.5.2) Cloud Access Security Broker

- Also called DLP in cloud
- Traffic directs to CASB before going to CSP
- Monitors data in between and assure and enforce policies
- Encrypted data validation to cloud

5.5.3) Pseudonymization

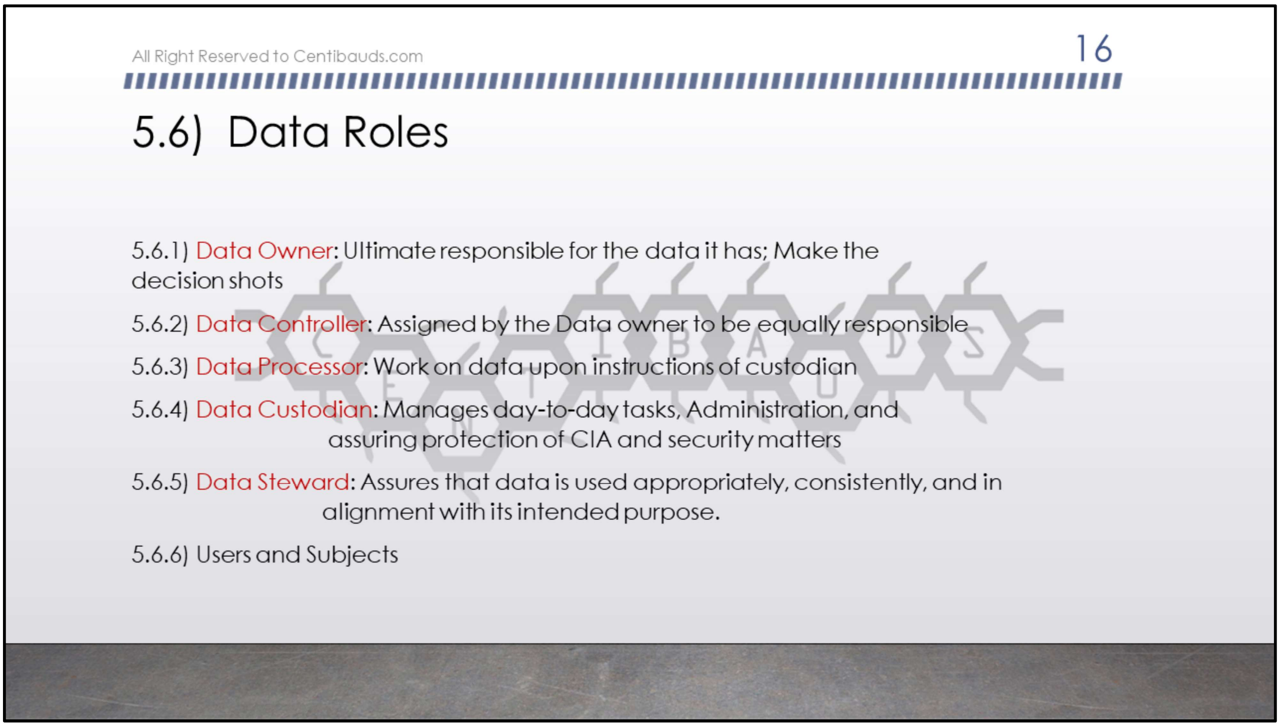
- Represent data with a number value
- Used to hide identity of the concerned user



5.5) Data Protection Methods (contd..)

- 5.5.4) Tokenization
  - Replace user entry with random string data
  - Example of Credit card:
    - Registration
    - User data
    - Validation
    - Completing the Sale
    - Multiple sheets and record created
  - 5.5.5) Anonymization: Make all related data replace by unidentified values
    - Methods of Randomization masking(shuffling values) , Masking altogether, Anonymous, Hashing, Obscure, Obfuscation, Nulls

-Only database and Tokenization vault knows who actual user is. The rest is all hidden
-Pseudinmization has only one table where change is made; In tokenization multiple database and record is made



All Right Reserved to Centibauds.com

5.6) Data Roles

5.6.1) Data Owner: Ultimate responsible for the data it has; Make the decision shots

5.6.2) Data Controller: Assigned by the Data owner to be equally responsible

5.6.3) Data Processor: Work on data upon instructions of custodian

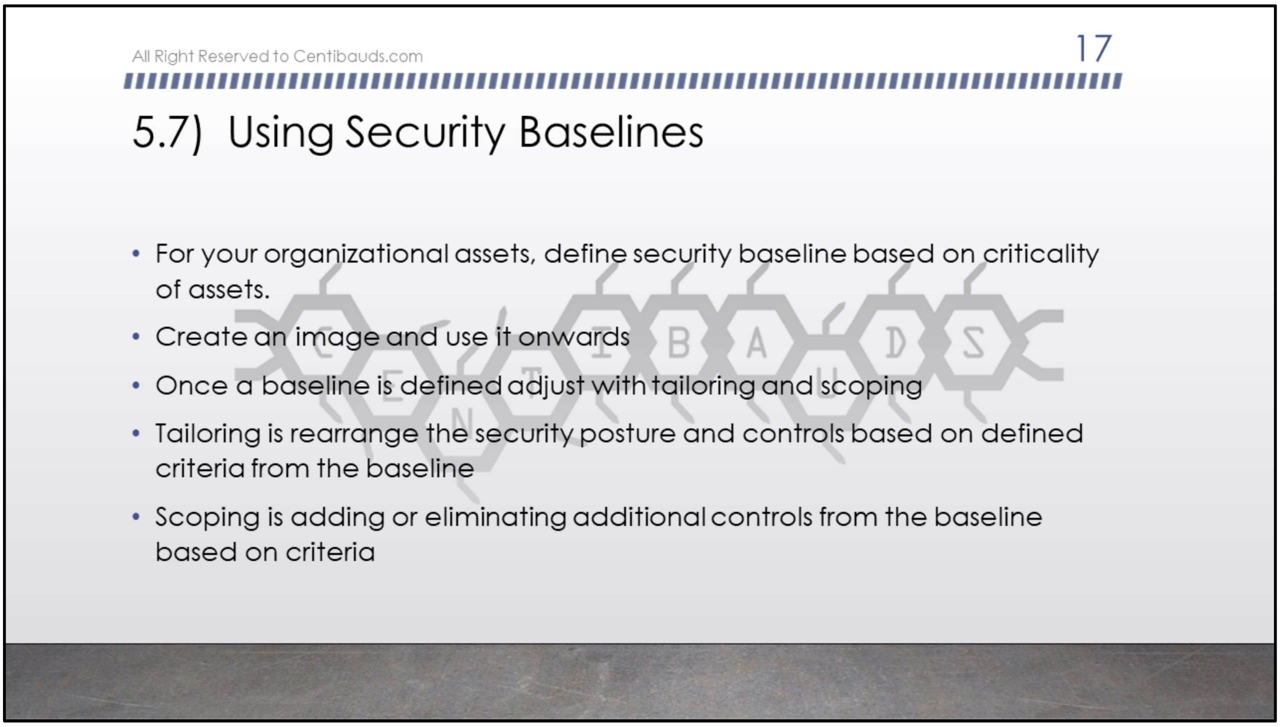
5.6.4) Data Custodian: Manages day-to-day tasks, Administration, and assuring protection of CIA and security matters

5.6.5) Data Steward: Assures that data is used appropriately, consistently, and in alignment with its intended purpose.

5.6.6) Users and Subjects

-NOTE: Well defined in various standards

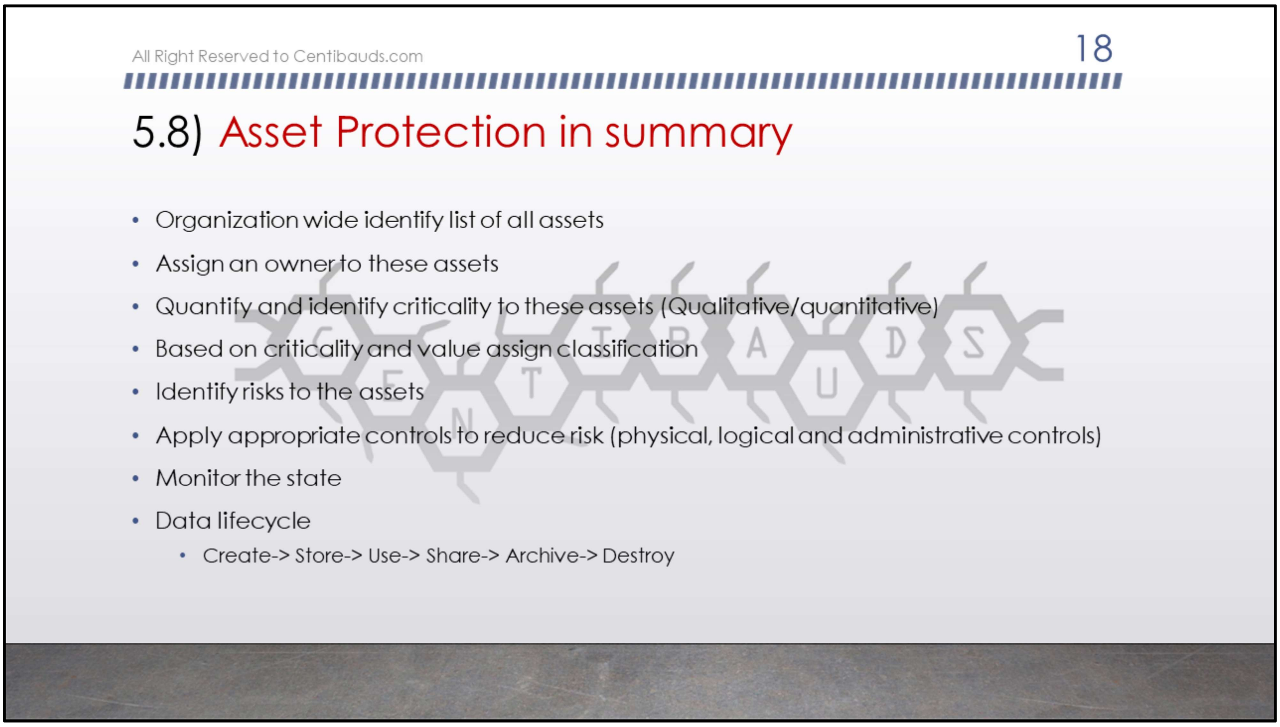
-Data Owner: Business owner department head etc.
-Data Controller: Defines how to collect data and what to use it for
-Data Processor: 3rd party, CSP and vendor



All Right Reserved to Centibauds.com

5.7) Using Security Baselines

- For your organizational assets, define security baseline based on criticality of assets.
- Create an image and use it onwards
- Once a baseline is defined adjust with tailoring and scoping
- Tailoring is rearrange the security posture and controls based on defined criteria from the baseline
- Scoping is adding or eliminating additional controls from the baseline based on criteria



All Right Reserved to Centibauds.com

5.8) Asset Protection in summary

- Organization wide identify list of all assets
- Assign an owner to these assets
- Quantify and identify criticality to these assets (Qualitative/quantitative)
- Based on criticality and value assign classification
- Identify risks to the assets
- Apply appropriate controls to reduce risk (physical, logical and administrative controls)
- Monitor the state
- Data lifecycle
  - Create-> Store-> Use-> Share-> Archive-> Destroy