THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

COMPX527 Week 9: Lecture 1

Cloud Data Security

Topics (Week 9-Week 14)

- Cloud Data Security
- Cloud Application Security
- Legal and Compliance
- Guest Lecture
- Presentations
- In-class Test

Data

All computing systems are built to consume, serve and / or manipulate data

Data

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

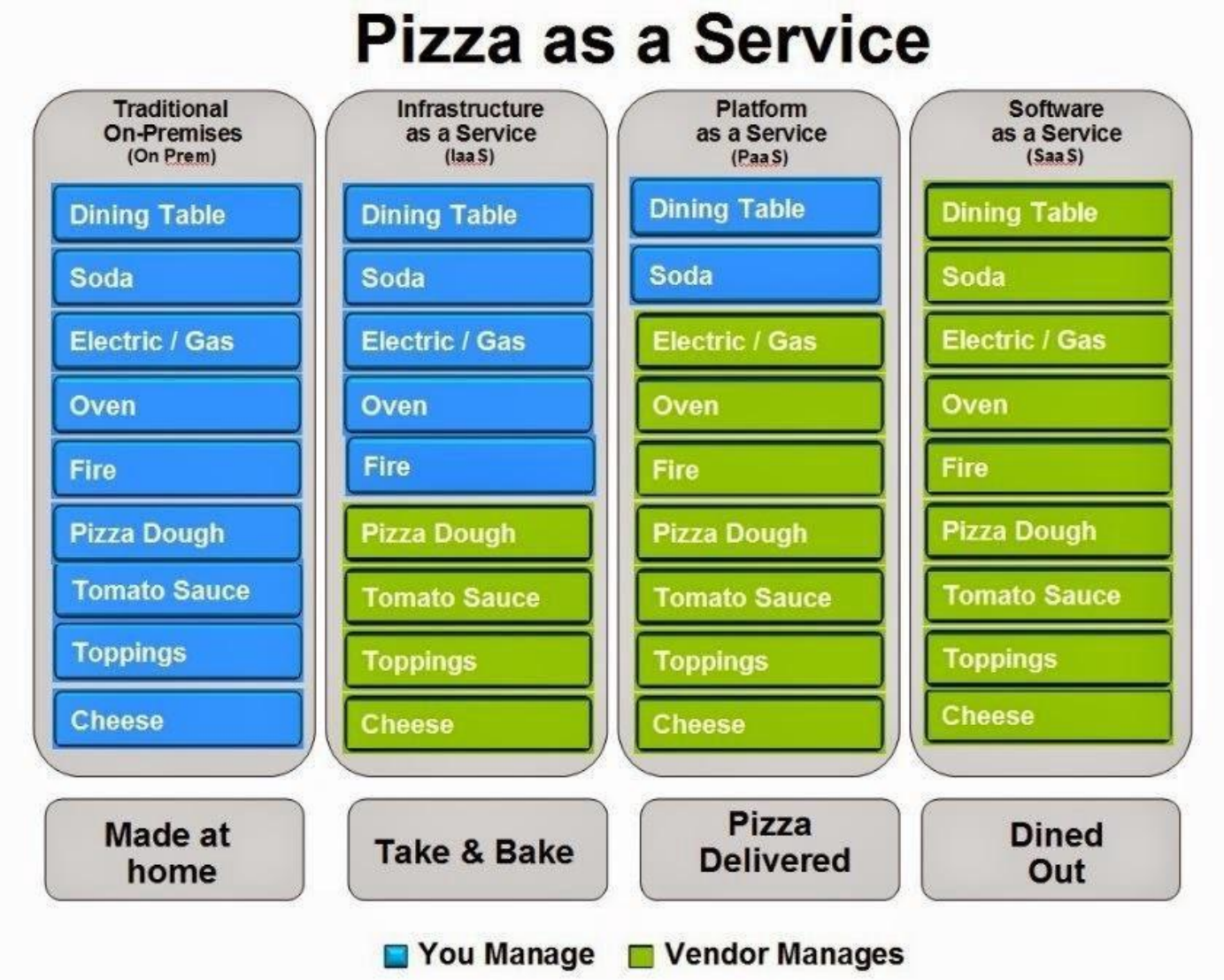
Personal Data	Name, date of birth, phone number, email address, passport number, IRD number, photos, medical information, etc.
Financial Data	Credit card info, Bank account number, insurance information, etc.
Digital Identities	Username/Passwords, digital certificates, security tokens, etc.
Operational Data	Building floor plans, network organization plan, enterprise organization information, program codes, etc.
Business Data	Client information, student records, customer records, product information, intellectual property, etc.
Security Data	keys, information used for MFA

Why do we need data security?

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- Risk Management
  - Financial Loss
  - Reputation harm
  - Operational Discontinuity
- Laws and Regulations
- Confidentiality
- Integrity
- Availability

Data in various cloud service models



Data in various cloud service models

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- Data in IaaS
  - Volume Storage
    - Volumes attached to IaaS instances, usually as a virtual hard drive. Examples Amazon EBS.
  - Object Storage
    - Object storage also referred as file storage. Instead of virtual hard drives, object storage is like shared file accessed via APIs or web interface. Example: Amazon S3
  - Raw Storage
    - Includes physical media where data is stored. May be mapped for direct access in certain private cloud configuration.

Data in various service models

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- Data in PaaS
  - Structured Data (Database as a Service)
    - A multitenant database architecture that is directly consumable as a service. Databases may be relational, or flat. Example AWS RDS, Azure MSSQL.
  - Unstructured Data (Big Data as a Service)
    - Data is typically stored in Object Storage or another distributed file system. Data typically needs to be close to the processing environment. Example Google Big Table , Dynamo DB.

Data in various service models

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

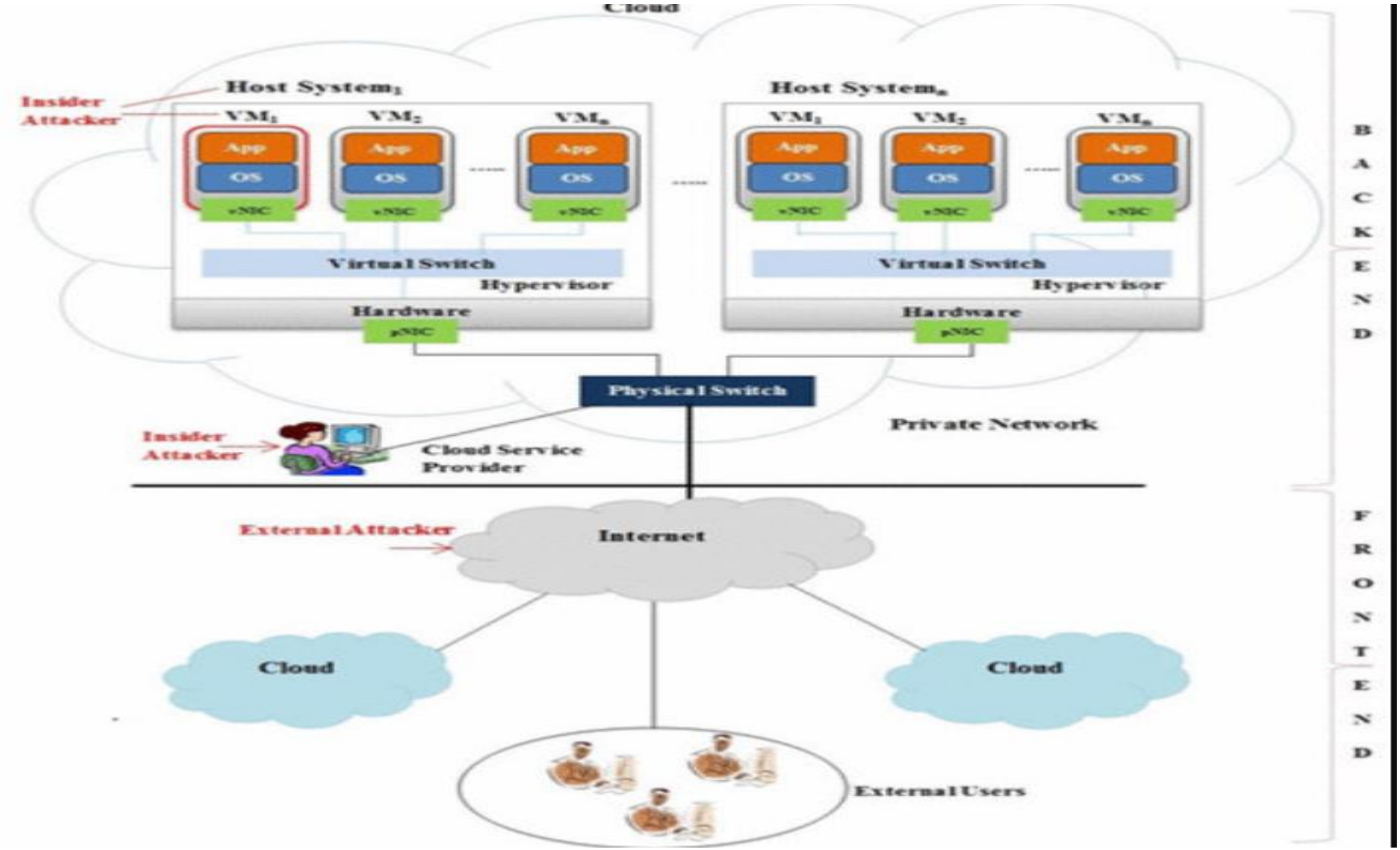
- Data in SaaS
  - Information Storage and Management
    - Data entered into the system e.g using a web interface. This data may further be stored on other PaaS or IaaS data storages. Example Gmail etc.
  - Content/File Storage
    - File-based content is stored within the SaaS application (reports, image files and documents). Example Dropbox etc.

What data to protect?

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- How do I know what data to protect?
  - Threat Model your business/application
  - Data Inventory and Classification
    - High-level description of important information categories.
    - Label information into categories according to sensitivity and value to the organisation
  - Laws and Industry Regulation for Compliance
    - GDPR, PCI-DSS, Privacy Act 2020, HIPAA(US)

Cloud Threat Model



Source: Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review

Cloud and GDPR

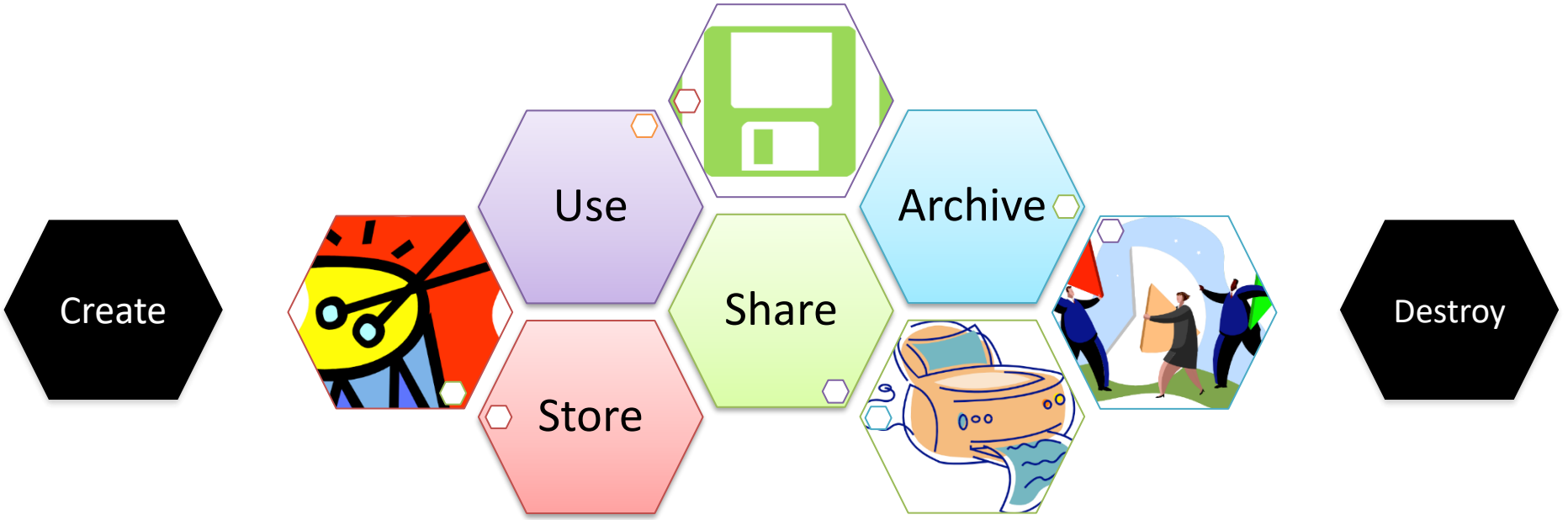
https://www.xorlogics.com/2018/09/24/gdpr-requirements-for-cloud-services-and-online-privacy/

What data to protect?

- Information Management Policies
  - Policies to define what activities are allowed for different information types

- Location and Jurisdiction Policies
  - Where data may be geographically located, which also has important legal and regulatory ramifications

Data Security Life Cycle

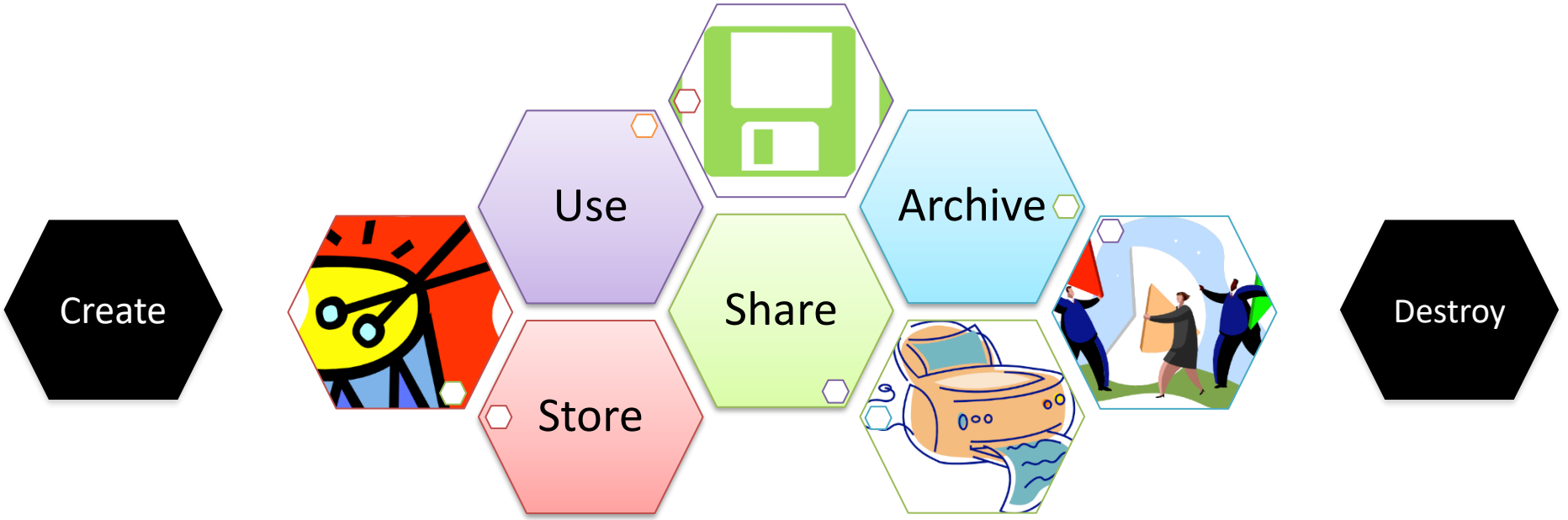


Data Security Life Cycle

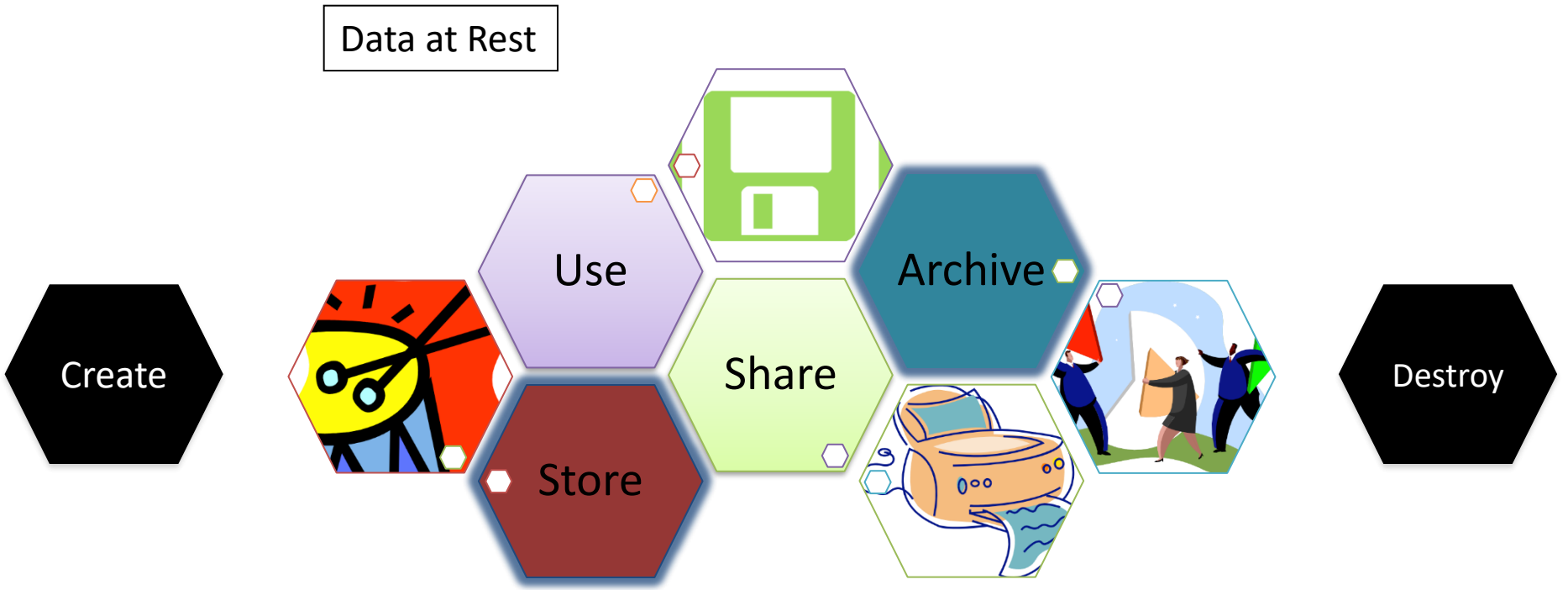
THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- Creation
  - Creation is the generation of new digital content, or the alteration/updating of existing content.
  - This phase can take place in the cloud or can be external to the cloud
  - Classify data according to
    - Sensitivity
    - Value to the organisation

Data Security Life Cycle



Data Security Life Cycle



Data Security Life Cycle

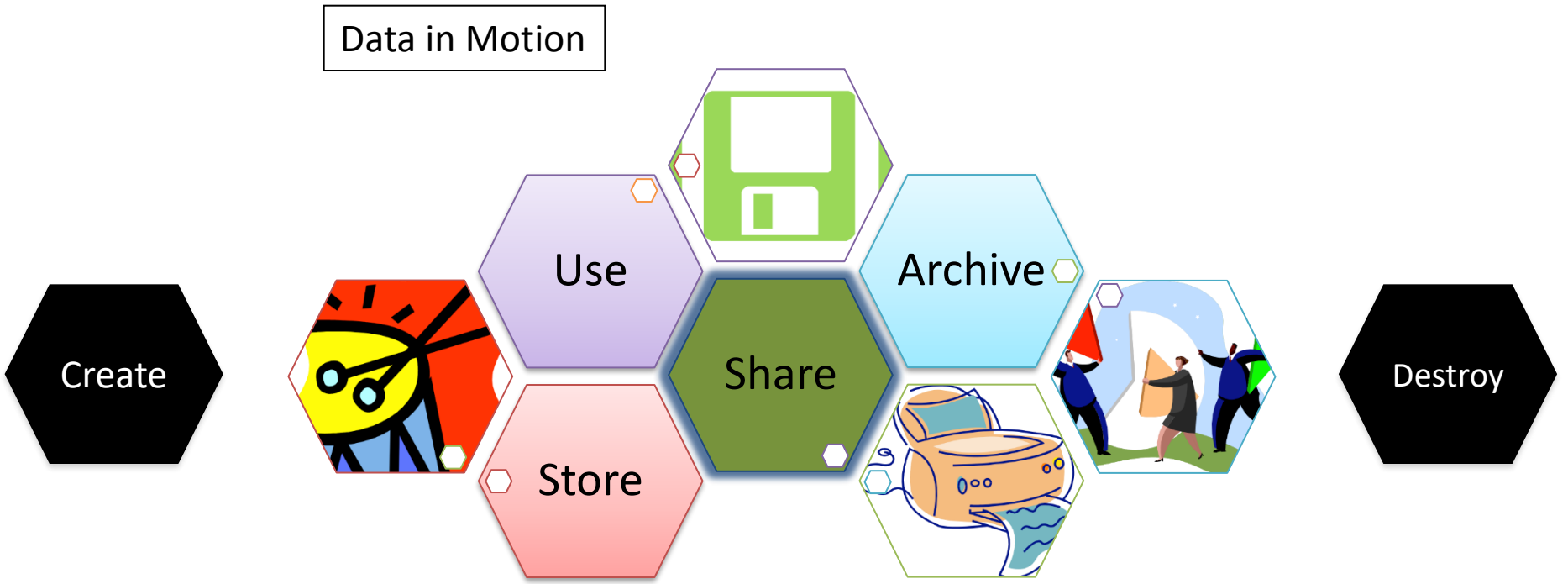
THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- Data at Rest
  - Data is stored after creation or is archived after leaving active use
  - Data spends most of its time in this phase
  - Data should be protected in accordance to its classification

Is data securely stored? How are the keys managed? Is data secure from malicious insiders? Tamper protection?

  - Controls such as encryption, integrity control, monitoring, and backup mechanisms should be implemented.

Data Security Life Cycle



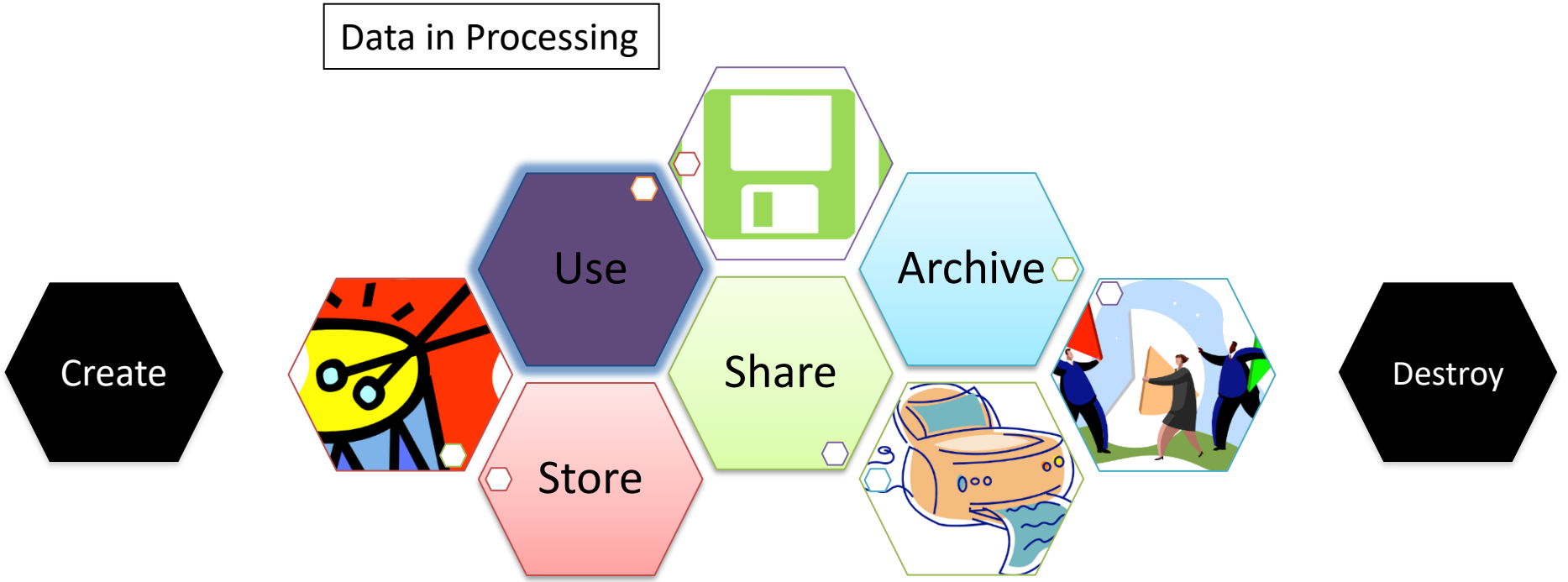
Data Security Life Cycle

- Data in motion
  - Data is being transported between clouds or between cloud and the user
  - Data is being shared

Secure Transmission? Data integrity? Information rights management?

  - Secure channels must be established before data is put in motion (in accordance with the classification level)
  - Mechanisms for maintaining data integrity should be implemented

Data Security Life Cycle



Data Security Life Cycle

- Data in use/processing
  - Data is being viewed, processed or otherwise being used in some sort of activity.
  - Data is most vulnerable at this stage
    - Some security controls may need to be turned off for data to be used
    - Data may have been transported to unsecure locations for processing

Information leakage? Unauthorized access?

  - Data should be monitored for checking malicious activity and audit purposes

Data Security Life Cycle

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- Destroy
  - Data ceases to be available for use
  - This can mean different things based on the usage of data, data content and its application
  - Data destruction can mean
    - Logically erasing pointers
      - Is the data truly deleted?
    - Physically permanent data deletion