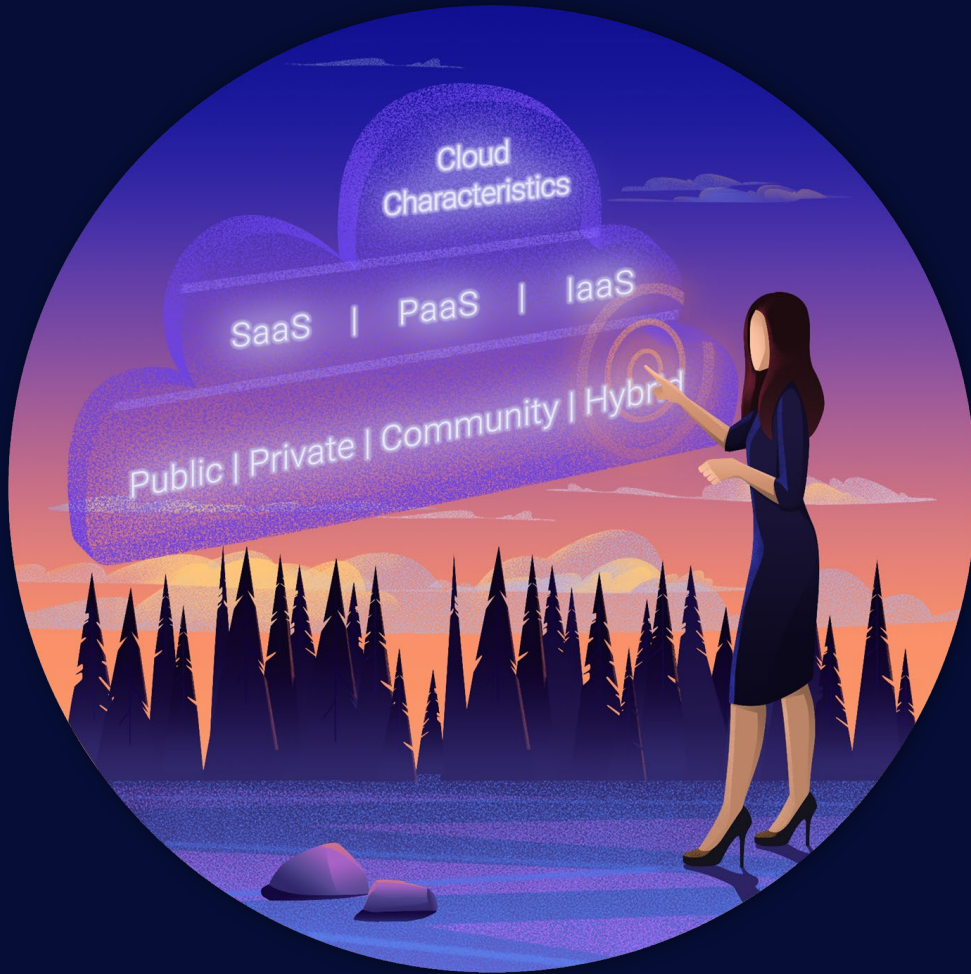




**DESTINATION**  
CERTIFICATION

# CCSP

# MindMaps



1

# Cloud Concepts, Architecture and Design

# Cloud Computing

| Characteristics        |                      |                  |                  |                  |               | Roles                             |                     |          |           |                 |                     |                       |                                |                                  |                          | Service Models  |      | Deployment Models |      |                            |        |         |           |        |       |
|------------------------|----------------------|------------------|------------------|------------------|---------------|-----------------------------------|---------------------|----------|-----------|-----------------|---------------------|-----------------------|--------------------------------|----------------------------------|--------------------------|-----------------|------|-------------------|------|----------------------------|--------|---------|-----------|--------|-------|
| On-Demand Self Service | Broad Network Access | Resource Pooling | Rapid Elasticity | Measured Service | Multi-tenancy | Accountability vs. Responsibility | Customer / Consumer | Provider | Broker    | Cloud Developer | Cloud Administrator | Cloud Service Manager | Cloud Service Business Manager | Cloud Service Deployment Manager | Cloud Service Integrator | Cloud Regulator | IaaS | PaaS              | SaaS | XaaS: IDaaS, NaaS, CompaaS | Public | Private | Community | Hybrid | Multi |
|                        |                      |                  |                  |                  |               |                                   |                     |          |           |                 |                     |                       |                                |                                  |                          |                 |      |                   |      |                            |        |         |           |        |       |
|                        |                      |                  |                  |                  |               |                                   |                     |          |           |                 |                     |                       |                                |                                  |                          |                 |      |                   |      |                            |        |         |           |        |       |
|                        |                      |                  |                  |                  |               | Aggregation                       |                     |          | Arbitrage |                 |                     | Intermediation        |                                |                                  |                          |                 |      |                   |      |                            |        |         |           |        |       |

# Alignment of Security Function to Business Strategy

## Corporate Governance

## Security Governance

Focus of Security

Goals of Information Security

Clearly Defined Roles &  
Responsibilities

Privacy

Corporate Laws

Overarching Security  
Policy

Risk Management

Functional Security  
Policies

Enable Business

Increase Value

Confidentiality

Integrity

Availability

Accountability

Responsibility

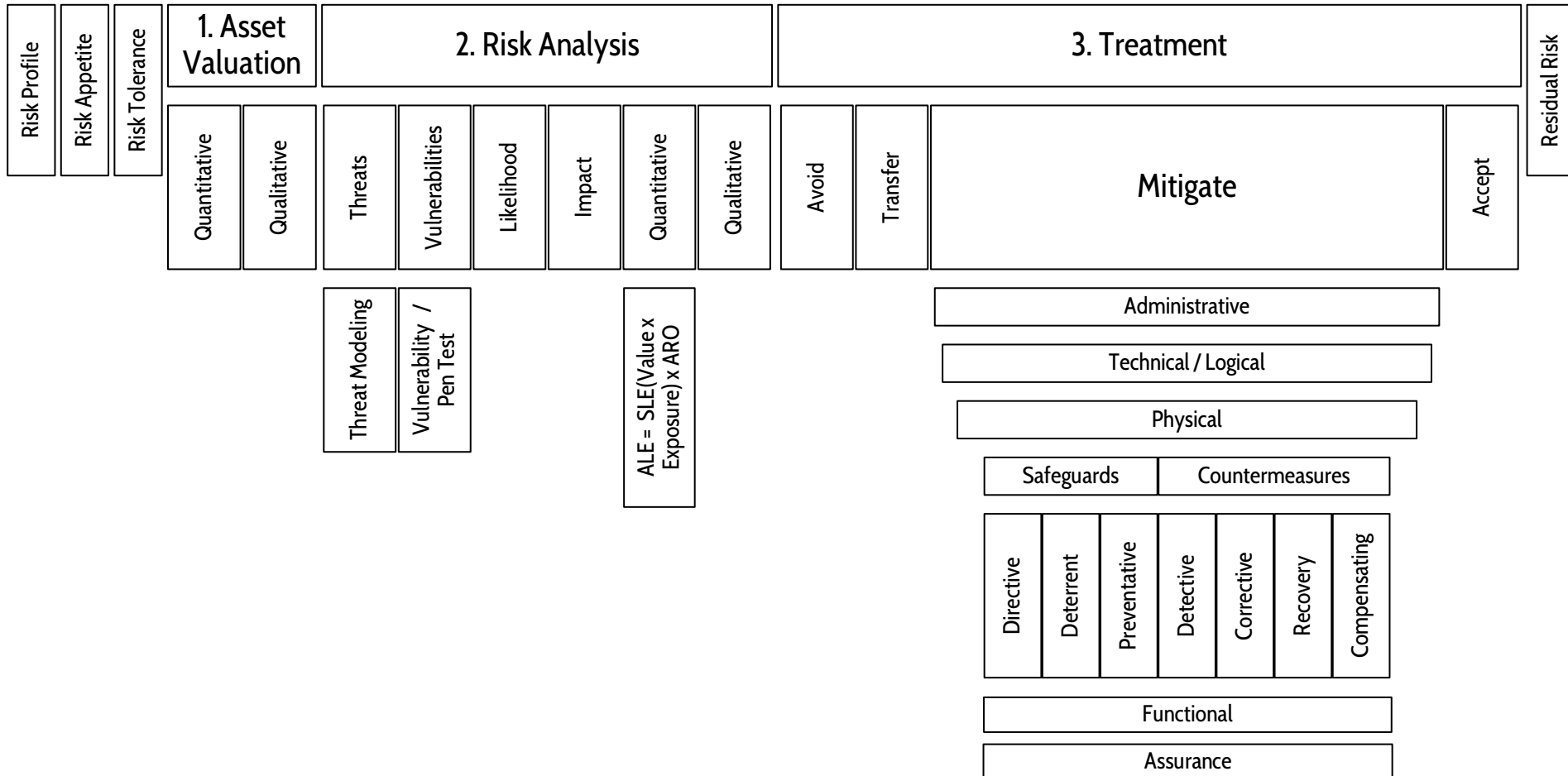
Standards

Procedures

Baselines

Guidelines

# Risk Management



# Cloud Shared Considerations

Cloud must be a business decision

Interoperability

Data  
Portability

Application  
Portability

Reversibility

Availability

Security

Privacy

Resiliency

Performance

Governance

Service Level  
Agreements  
(SLAs)

Auditability

Regulatory

# Frameworks

Provide Comprehensive Guidance

Security Control  
Frameworks

Cloud Security Control  
Frameworks

Cloud Design Patterns

Risk Frameworks

ISO 27001

ISO 27002

CSA Cloud  
Controls  
Matrix (CCM)

ISO 27017

ISO 27018

SANS  
security  
principles

Well-  
Architected  
Framework

CSA  
Enterprise  
Architecture

ISO 31000

ENISA

CSA

NIST

Microsoft

# Cost Benefit Analysis

Pay per usage

CapEx to  
OpEx

Depreciation

Datacenter /  
utility costs

Resource  
pooling

Software  
licensing

Personnel &  
operational  
costs

Shift in focus

# Evaluation Criteria

Certification

Accreditation

Common Criteria

FIPS 140-2

EAL1 – EAL7

Levels 1 - 4

# AI/ML Foundations, Risks, and Governance

AI systems need validated data, ongoing monitoring, and ethical/legal guardrails.

| AI and ML Fundamentals  |  | Cloud Threat Detection    |  | Data Sources           |  | Ethical Concerns in AI  |  |                           |  | Regulatory Requirements      |  |                 |  |                      |  |                  |  |                 |  |                   |  |                 |  |                      |  |                           |  |                             |  |             |  |                  |  |                        |  |                               |  |                              |  |
|-------------------------|--|---------------------------|--|------------------------|--|-------------------------|--|---------------------------|--|------------------------------|--|-----------------|--|----------------------|--|------------------|--|-----------------|--|-------------------|--|-----------------|--|----------------------|--|---------------------------|--|-----------------------------|--|-------------|--|------------------|--|------------------------|--|-------------------------------|--|------------------------------|--|
| Artificial Intelligence |  | AI Use Cases              |  | Detection              |  | Response and Resilience |  | Data Origin and Integrity |  | Data Preparation and Quality |  | Model Assurance |  | Privacy Preservation |  | Misuse           |  | Dual-use Risk   |  | Bias              |  | Decision-making |  | Regulatory Landscape |  |                           |  |                             |  |             |  |                  |  |                        |  |                               |  |                              |  |
| Machine Learning        |  | Inputs and Monitoring     |  | Techniques and Metrics |  | Automated Response      |  | Data Provenance           |  | Training Data Integrity      |  | Threats         |  | Feature Engineering  |  | Model Validation |  | Automation Bias |  | Confirmation Bias |  | Historical Bias |  | Sampling Bias        |  | Automated Decision-making |  | Human Oversight             |  | EU AI Act   |  | Other Regulation |  | AI-adjacent Regulation |  | Frameworks                    |  | Governance and Documentation |  |
| Deep Learning           |  | Threat Intelligence Feeds |  | Real-Time Monitoring   |  | Behavioral Baselines    |  | Anomaly Detection         |  | Data Poisoning               |  | HITL            |  | HOTL                 |  | HOOTL            |  | Brazil          |  | Colorado          |  | Texas           |  | China                |  | GDPR and AI Alignment     |  | Sector-Specific Obligations |  | NIST AI RMF |  | DPIA             |  | FRIA                   |  | Algorithmic Impact Assessment |  |                              |  |



# 2

## Cloud Data Security

# Cloud Data Lifecycle

## Phases

Create

Store

Use

Share

Archive

Destroy

Classification

## Data Roles

Owner / controller

Processor

Custodian

Steward

Subject

## Controlling Access

Actors

Functions

Locations

Possible

Allowed

# Cloud Data Storage

| Types              |           |           |          | Storage method             | Storage controllers |    |      | Storage clusters |                 | By service model |                           |                            |        |                            |
|--------------------|-----------|-----------|----------|----------------------------|---------------------|----|------|------------------|-----------------|------------------|---------------------------|----------------------------|--------|----------------------------|
| Virtual constructs | Long-term | Ephemeral | Raw-disk | Fragmentation & dispersion | iSCSI               | FC | FCoE | Tightly coupled  | Loosely coupled | SaaS             | PaaS                      | IaaS                       |        |                            |
|                    |           |           |          |                            |                     |    |      |                  |                 |                  |                           |                            |        |                            |
| Volume             | Object    | CDN       |          | SSMS                       |                     |    |      |                  |                 | Web interface    | Structured & Unstructured | Databases, NoSQL, Big data | Object | Volume                     |
|                    |           |           |          | AONT-RS                    |                     |    |      |                  |                 |                  |                           |                            |        |                            |
|                    |           |           |          |                            |                     |    |      |                  |                 |                  |                           |                            |        | Object                     |
|                    |           |           |          |                            |                     |    |      |                  |                 |                  |                           |                            |        | Raw-disk                   |
|                    |           |           |          |                            |                     |    |      |                  |                 |                  |                           |                            |        | Ephemeral                  |
|                    |           |           |          |                            |                     |    |      |                  |                 |                  |                           |                            |        | Databases, NoSQL, Big data |

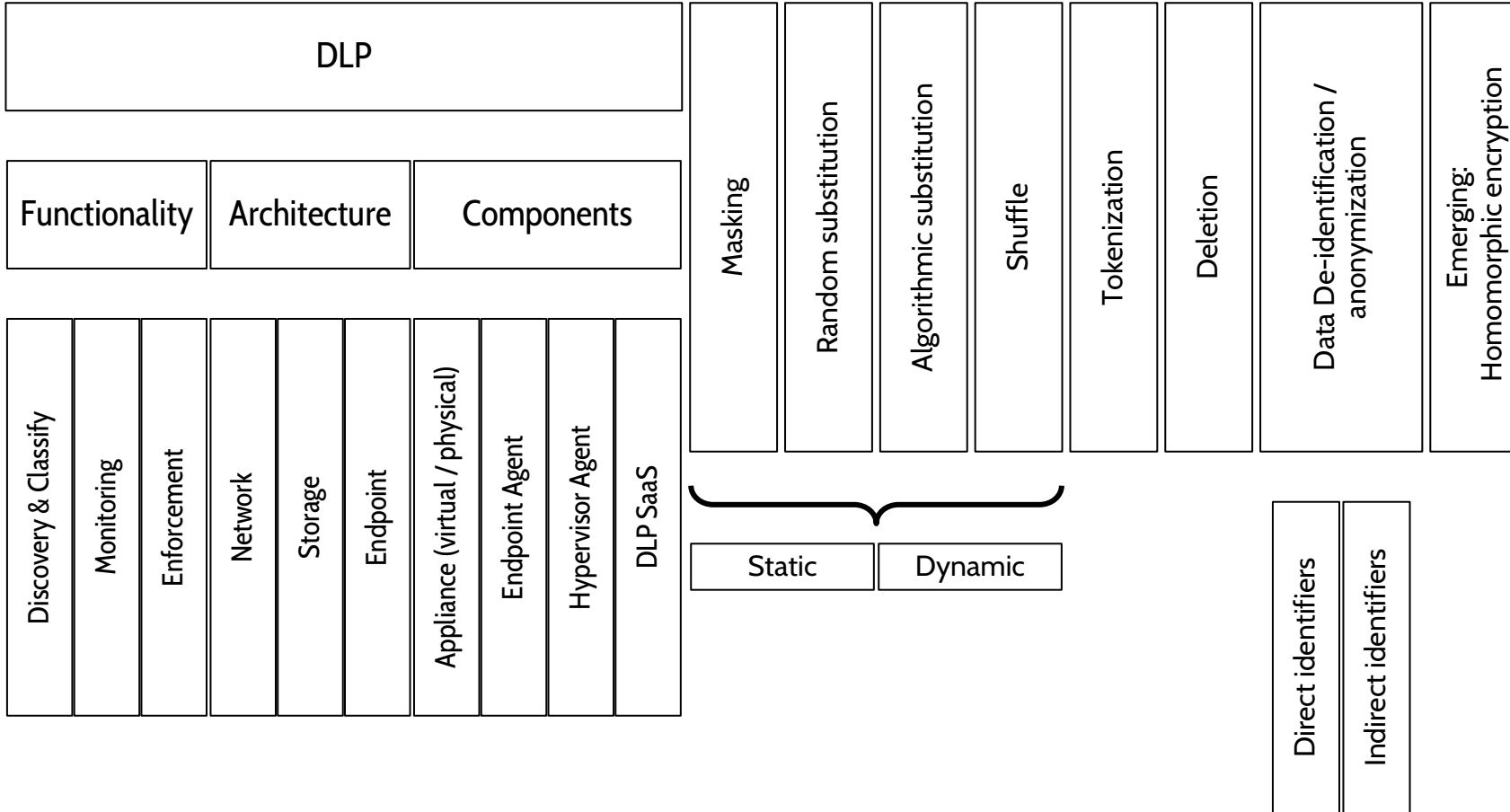
# Threats to Storage

|                    |                     |                           |                         |                          |         |                 |
|--------------------|---------------------|---------------------------|-------------------------|--------------------------|---------|-----------------|
| Unauthorized usage | Unauthorized access | Regulatory non-compliance | Denial of Service (DoS) | Theft or accidental loss | Malware | No sanitization |
|--------------------|---------------------|---------------------------|-------------------------|--------------------------|---------|-----------------|

# Data Security Strategies

## Encryption

## DRM



# Data Discovery

Types of data

Metadata

Structured

Unstructured

# Asset Classification

Asset Inventory

Assign Ownership

Classify

Sensitive Data

Classification

Categorization

Personal Data

Labeling

Marking

# Log Review & Analysis

Monitor for

Logging & Monitoring Service  
(SIEM systems)

Continuous  
updates &  
Continuous  
optimization  
(tuning)

Chain-of-custody

Non-  
repudiation

Errors

Modification

Breaches

Aggregation

Normalization

Correlation

Secure Storage

Analysis

Reporting

# Digital Rights Management (DRM)

Consumer DRM

Enterprise DRM

Cloud DRM  
Challenges

Information Rights Management (IRM)

Auditing of access /  
use

Signing / sealing

Rights based on  
classification

Controlling copy &  
pasting, screenshots

# Data Retention, Archiving & Deletion

Data retention  
policies

Migration to  
slower storage

Defensible Destruction

Destruction

Purging

Clearing

Media  
Destruction

Shred /  
Disintegrate /  
Drill

Degauss

Crypto  
shredding

Overwrite /  
Wipe / Erasure

Format

# AI/ML Data Protection

Trustworthy AI starts with secure data, privacy protection, and responsible oversight.

| Dataset and Model Privacy     |                    |                   |                 |              | Dataset and Model Security |                 |                       |                             |                                |                  |                   |                                    |  |  |
|-------------------------------|--------------------|-------------------|-----------------|--------------|----------------------------|-----------------|-----------------------|-----------------------------|--------------------------------|------------------|-------------------|------------------------------------|--|--|
| Privacy-Preserving Techniques |                    |                   | Privacy Threats |              | Dual Attack Surface        |                 | Build-Time Controls   |                             | Pre-Deployment Assurance       | Runtime Controls |                   |                                    |  |  |
| Differential Privacy          | Federated Learning | Data Minimization | Model Inversion | Data Leakage | Training Data              | Model Artifacts | Supply Chain Security | Model Integrity and Signing | Adversarial Robustness Testing | Access Controls  | Incident Response | Continuous Model Monitoring        |  |  |
| Privacy-accuracy Trade-off    |                    |                   |                 |              |                            |                 |                       |                             |                                |                  | Model Drift       | Metrics                            |  |  |
|                               |                    |                   |                 |              |                            |                 |                       |                             |                                |                  |                   | Prediction Confidence Distribution |  |  |
|                               |                    |                   |                 |              |                            |                 |                       |                             |                                |                  |                   | Error Rate                         |  |  |
|                               |                    |                   |                 |              |                            |                 |                       |                             |                                |                  |                   | FP Rate                            |  |  |
|                               |                    |                   |                 |              |                            |                 |                       |                             |                                |                  |                   | FN Rate                            |  |  |



# 3

## Cloud Platform and Infrastructure Security

# Cloud Infrastructure Components

## Major cloud components

Compute

Network

Storage

Virtualization

Management  
Plane

Virtual Machines

Containers

Serverless  
Computing

Dedicated  
Isolated Networks

Networking  
Models

Virtual Networks

Cloud Data Storage

Abstraction

Hypervisors

Containerization  
Engine

Immutable workloads

Service

Storage

Management

Non-converged

Converged

VLAN

SDN

Type 1: Hardware

Type 2: Operating  
System

Infrastructure as Code (IaC)

# Management Plane

Single most significant difference

## Capabilities

## Access

Scheduling

Orchestration

Maintenance

Service Catalog

Self-Provisioning

Identity and Access  
Management

Management APIs

Configuration  
Management

Key Management &  
Encryption

Financial Tracking &  
Reporting

Service / Helpdesk

Web console

APIs

SDKs & CLIs

# Data Center Design

|                                      |                |                 |                       |                         |                     |                                                                                                                                   |                                |  |  |                  |                             |              |             |                  |  |  |  |
|--------------------------------------|----------------|-----------------|-----------------------|-------------------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------|--|--|------------------|-----------------------------|--------------|-------------|------------------|--|--|--|
| Security Survey<br>(Risk Management) | Logical Design | Physical Design | Design Considerations |                         |                     |                                                                                                                                   |                                |  |  |                  |                             |              |             |                  |  |  |  |
|                                      |                |                 | Location              | Services to be provided | Tenant Partitioning | Build or buy                                                                                                                      | (HVAC)                         |  |  | Cable Management | MVPC                        | Availability | Maintenance | Design Resilient |  |  |  |
|                                      |                |                 |                       |                         |                     | Temperature<br>Humidity<br>Air Quality<br>Latent Cooling<br>(remove moisture)<br>Sensible Cooling<br>(remove heat)<br>Containment | 64.4°F / 18°C<br>80.6°F / 27°C |  |  |                  | Uptime Institute's Standard |              |             |                  |  |  |  |
|                                      |                |                 |                       |                         |                     |                                                                                                                                   | 40 – 60%                       |  |  |                  |                             |              |             |                  |  |  |  |
|                                      |                |                 |                       |                         |                     |                                                                                                                                   | Positive Pressurization        |  |  |                  |                             |              |             |                  |  |  |  |
|                                      |                |                 |                       |                         |                     |                                                                                                                                   | Hot Aisle<br>Cold Aisle        |  |  |                  |                             |              |             |                  |  |  |  |
|                                      |                |                 |                       |                         |                     |                                                                                                                                   |                                |  |  |                  |                             |              |             |                  |  |  |  |
|                                      |                |                 |                       |                         |                     |                                                                                                                                   |                                |  |  |                  | Tier 4 (2N+1)               |              |             |                  |  |  |  |
|                                      |                |                 |                       |                         |                     |                                                                                                                                   |                                |  |  |                  | Tier 3 (2N)                 |              |             |                  |  |  |  |
|                                      |                |                 |                       |                         |                     |                                                                                                                                   |                                |  |  |                  | Tier 2 (N+1)                |              |             |                  |  |  |  |
|                                      |                |                 |                       |                         |                     |                                                                                                                                   |                                |  |  |                  | Tier 1 (N)                  |              |             |                  |  |  |  |
|                                      |                |                 |                       |                         |                     |                                                                                                                                   |                                |  |  |                  | Maintenance Mode            |              |             |                  |  |  |  |
|                                      |                |                 |                       |                         |                     |                                                                                                                                   |                                |  |  |                  | Uptime                      |              |             |                  |  |  |  |
|                                      |                |                 |                       |                         |                     |                                                                                                                                   |                                |  |  |                  | MTBF                        |              |             |                  |  |  |  |
|                                      |                |                 |                       |                         |                     |                                                                                                                                   |                                |  |  |                  | MTTR                        |              |             |                  |  |  |  |

# Attack Vectors

## Common

## Specific to Cloud

Denial of Service

Malware

System vulnerabilities

XSS, CSRF, SQL Injection, etc.

Malicious insiders

Social engineering

Advanced Persistent Threats

Insufficient Due Diligence

Guest Escape / VM Hopping

Hyperjacking attack

Hyperstack attack

Insecure Interfaces / APIs

Provider's infrastructure

Shared technology

Account hijacking

# Risks

## Common

## Specific to Cloud

Data Loss / Breach

Data Integrity

Compliance & regulatory

VM Sprawl

Sensitive data within a VM

Dormant VMs

Instant-on gaps

Resource exhaustion

Hypervisor security

Data comingling

Inter-VM communication (blindspots)

# Physical Security

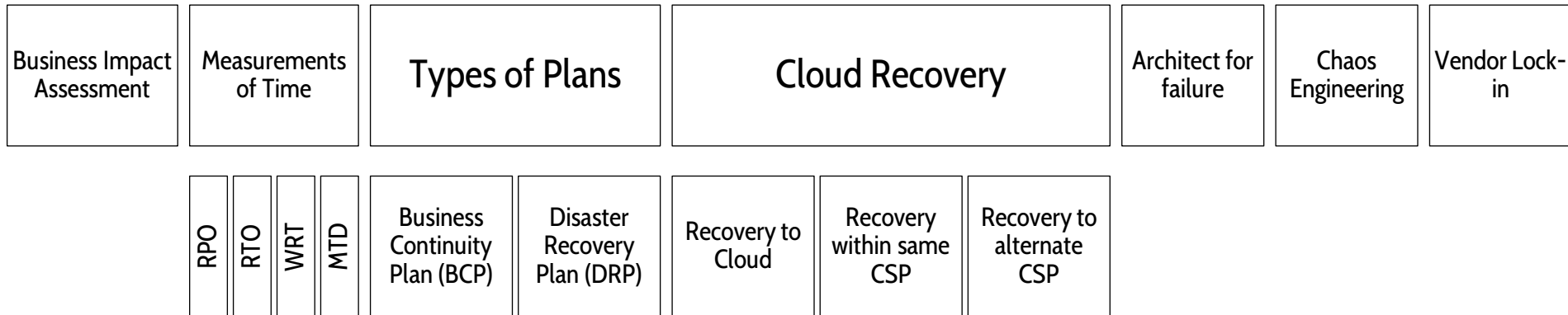
## Safety of people

| Security Survey                               | Categories of Controls                                                                                            | Layered Defense |  |         |  |           |  |                                    |  |                                         |  |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-----------------|--|---------|--|-----------|--|------------------------------------|--|-----------------------------------------|--|
| Deter<br>Delay<br>Detect<br>Assess<br>Respond | Perimeter<br><br>Doors / Mantraps<br><br>Infrastructure<br><br>NFPA<br><br>Fire Detection<br><br>Fire Suppression |                 |  |         |  |           |  |                                    |  |                                         |  |
|                                               |                                                                                                                   | Landscape       |  | Network |  | Power     |  | Flame                              |  | Smoke                                   |  |
|                                               |                                                                                                                   | Grading         |  | HVAC    |  | Heat      |  | Water                              |  | Gas                                     |  |
|                                               |                                                                                                                   |                 |  |         |  |           |  |                                    |  |                                         |  |
|                                               |                                                                                                                   |                 |  | UPS     |  | Generator |  |                                    |  |                                         |  |
|                                               |                                                                                                                   |                 |  |         |  |           |  | Wet<br>Dry<br>Pre-action<br>Deluge |  | INERGEN<br>Argonite<br>FM-200<br>Aero-K |  |

# Network Defense

|                  |                           |                   |                        |     |                  |                             |               |                        |         |                       |                    |                     |                   |         |
|------------------|---------------------------|-------------------|------------------------|-----|------------------|-----------------------------|---------------|------------------------|---------|-----------------------|--------------------|---------------------|-------------------|---------|
| Defense in Depth | Zero Trust                | Firewalls         | Inspection             |     |                  |                             |               |                        |         |                       |                    |                     | Endpoint Security |         |
| Types            |                           |                   | IDS                    | IPS | IDS/IPS Location | IDS / IPS Detection Methods |               |                        |         | Honeypots & honeynets | Ingress vs. Egress |                     |                   |         |
| Packet Filtering | Stateful Packet Filtering | Application       | Firewalls in the Cloud |     |                  | Host Based                  | Network Based | Placement in the Cloud | Pattern | Anomaly               |                    | White & Black Lists | Sandbox           |         |
| Virtual          | Physical                  | Microsegmentation |                        |     |                  |                             |               |                        |         | Signature analysis    | Stateful matching  | Statistical         | Protocol          | Traffic |
|                  |                           |                   |                        |     |                  |                             |               |                        |         |                       |                    |                     |                   |         |

# Business Continuity Management (BCM)





# 4

## Cloud Application Security

# Cloud Development

OWASP Top 10

SANS / CWE Top 25

## Common Pitfalls

On-premise may not transfer

New knowledge & skills required

Different risk profiles

Integration complexity

Legacy applications

Multitenancy

Higher baseline security

Responsiveness

Isolated environments

Micro-service architectures

Elasticity

DevOps

Unified management interface

Immutable infrastructure

Limited logging visibility

Increased application scope

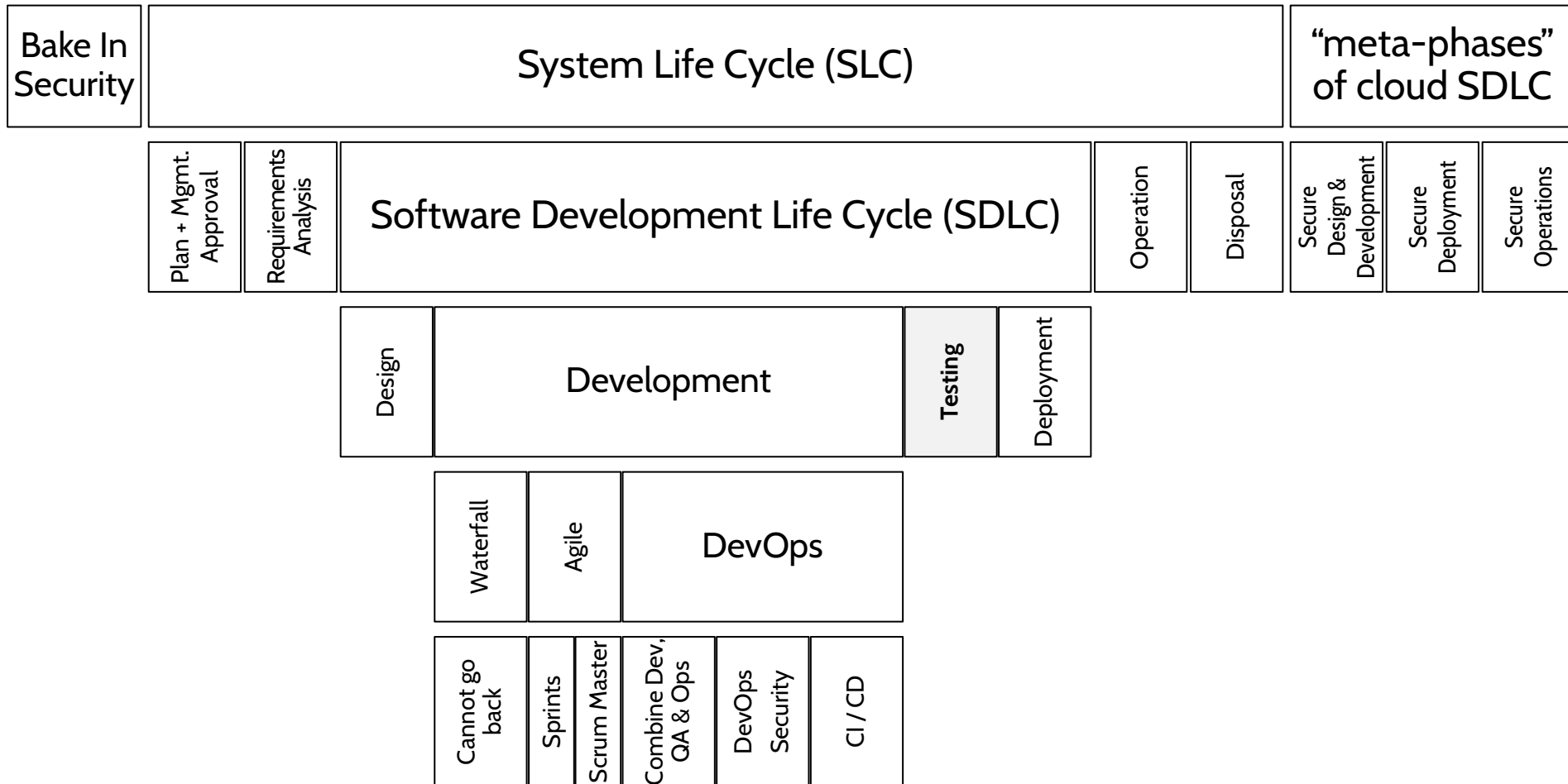
Changing threat models

Reduced transparency

## Opportunities

## Challenges

# Secure Software Development



# Security Assessment and Testing

## Software Testing Techniques

| Software Testing Techniques       |  |  |                                  |  |  |                                      |  |  |                                     |  |  |
|-----------------------------------|--|--|----------------------------------|--|--|--------------------------------------|--|--|-------------------------------------|--|--|
| Validation                        |  |  | Verification                     |  |  | Rigor based on Value                 |  |  |                                     |  |  |
| Methods & Tools                   |  |  | Runtime                          |  |  | Access to Code                       |  |  | Software Composition Analysis (SCA) |  |  |
| Manual                            |  |  | Automated                        |  |  | Static (SAST)                        |  |  | Dynamic (DAST)                      |  |  |
| Fuzz                              |  |  | Interactive (IAST)               |  |  | White                                |  |  | Black                               |  |  |
| Vulnerability Assessment          |  |  | Penetration Test                 |  |  | Process                              |  |  | Testing Techniques                  |  |  |
| Types of Scans                    |  |  | Banner grabbing & Fingerprinting |  |  | Interpreting & understanding results |  |  | False positive vs. False negative   |  |  |
| Reconnaissance                    |  |  | Enumeration                      |  |  | Vulnerability Analysis               |  |  | Execution                           |  |  |
| Document Findings                 |  |  | Perspective                      |  |  | Approach                             |  |  | Knowledge                           |  |  |
| Internal                          |  |  | External                         |  |  | Blind                                |  |  | Double-blind                        |  |  |
| Zero (black)                      |  |  | Partial (gray)                   |  |  | Full (white)                         |  |  | Credentialed / Authenticated        |  |  |
| Unauthenticated / Unauthenticated |  |  | CVE                              |  |  | CVSS                                 |  |  |                                     |  |  |

# Common Vulnerabilities & Threat Modeling

Cross Site Scripting (XSS)

Cross Site  
Request  
Forgery  
(CSRF)

SQL  
Injection

Insecure  
Direct Object  
Reference

Buffer  
Overflow

Threat Modeling

Stored  
(Persistent)

Reflected

DOM

Parameter /  
bounds  
checking

ATASM

STRIDE

PASTA

DREAD

Input Validation

# Verified Secure Software

Application Programming Interfaces (APIs)

Approved APIs

Software / API Supply chain  
management

REST

SOAP

Simple  
Fast  
Most Widely Used

More capabilities  
More complexity

# Cryptographic Services

Confidentiality

Integrity

Authenticity

Non-Repudiation

Access Control

= Hashing

Origin

Delivery

# Cryptography

One-way

Two-way

Digital Signatures

Digital Certificates

Hashing

Symmetric

Asymmetric

Integrity  
Authenticity  
Non-repudiation

Verify owner of public key

X.509

# Key Management

Kirchhoff's Law

Generation

Distribution

Storage

Rotation

Disposition

Recovery

Out-of-band  
Hybrid

TPM  
HSM

Crypto-shredding  
Key Destruction

Split Knowledge  
Dual Control  
Key Escrow

# Crypto in the Clouds

| Use         | Motion                       | Rest          |                    |                 |             | Major components |                   |                    |
|-------------|------------------------------|---------------|--------------------|-----------------|-------------|------------------|-------------------|--------------------|
| Homomorphic | VPN (Tunneling + Encryption) | Storage level | Volume             | Object          | Database    | Data             | Encryption Engine | Keys               |
|             | IPSec                        |               |                    |                 |             |                  |                   |                    |
|             | SSL / TLS                    |               |                    |                 |             |                  |                   |                    |
|             | Transport Mode               | Tunnel Mode   | Handshake Protocol | Record Protocol | Application | Proxy            | Database          | File               |
|             |                              |               |                    |                 |             |                  |                   | Internally Managed |
|             |                              |               |                    |                 |             |                  |                   | Externally Managed |
|             |                              |               |                    |                 |             |                  |                   | Escrow Managed     |

## Proxies

|     |     |     |             |
|-----|-----|-----|-------------|
| WAF | DAM | FAM | API Gateway |
|-----|-----|-----|-------------|

## Access Control

|                           |              |                 |            |                          |                |               |                |                                                                    |                                                                          |                    |      |                                  |                            |                    |                                  |        |                           |
|---------------------------|--------------|-----------------|------------|--------------------------|----------------|---------------|----------------|--------------------------------------------------------------------|--------------------------------------------------------------------------|--------------------|------|----------------------------------|----------------------------|--------------------|----------------------------------|--------|---------------------------|
| Access Control Principles |              |                 | Entity     | Access Controls Services |                |               |                |                                                                    | Allows users to access multiple systems with a single set of credentials |                    |      |                                  | Privileged User Management | Secrets Management | CASB                             |        |                           |
| Separation of Duties      | Need to Know | Least Privilege | Identity   | Identification           | Authentication | Authorization | Accountability | Single Sign-on<br>Access systems only within the same organization | Federated Access<br>Access systems across multiple entities              |                    |      |                                  |                            |                    |                                  |        |                           |
|                           |              |                 | Identifier | Attributes               |                |               |                |                                                                    |                                                                          |                    |      |                                  |                            |                    |                                  |        |                           |
|                           |              |                 |            |                          |                |               |                |                                                                    |                                                                          |                    |      |                                  |                            |                    |                                  |        |                           |
|                           |              |                 |            |                          | Knowledge      | Ownership     | Characteristic | Single / Multifactor                                               | Kerberos                                                                 | Trust Relationship | SAML | WS-Federation<br>OpenID<br>OAuth |                            |                    |                                  |        |                           |
|                           |              |                 |            |                          |                |               |                |                                                                    |                                                                          |                    |      |                                  | Principal / User           | Identity Provider  | Relying Party / Service Provider | Tokens | Assertions written in XML |



5

# Cloud Security Operations

# Cloud Operations

|        |  |         |  |                        |  |           |              |                      |  |            |  |            |  |                              |  |                 |  |                    |  |                         |  |          |  |                      |  |                                  |  |                                    |  |                      |  |                 |  |             |  |           |  |           |  |
|--------|--|---------|--|------------------------|--|-----------|--------------|----------------------|--|------------|--|------------|--|------------------------------|--|-----------------|--|--------------------|--|-------------------------|--|----------|--|----------------------|--|----------------------------------|--|------------------------------------|--|----------------------|--|-----------------|--|-------------|--|-----------|--|-----------|--|
| Access |  |         |  | Hardware Configuration |  | Hardening | Availability | Monitoring & Control |  |            |  |            |  | Distributed Resource Sharing |  |                 |  | Backup and Restore |  |                         |  |          |  |                      |  |                                  |  |                                    |  |                      |  |                 |  |             |  |           |  |           |  |
|        |  |         |  |                        |  |           |              |                      |  |            |  |            |  |                              |  |                 |  |                    |  |                         |  |          |  |                      |  |                                  |  |                                    |  |                      |  |                 |  |             |  |           |  |           |  |
| Local  |  | Remote  |  | BIOS                   |  | TPM & HSM |              | Baseline             |  | Clustering |  | Redundancy |  | VM                           |  | Performance     |  | Network            |  | Application             |  | Hardware |  | Reservations         |  | Limits                           |  | Shares                             |  | Dynamic Optimization |  | OS & VM Config. |  | Agent-based |  | Agentless |  | Snapshots |  |
| KVM    |  | Console |  | SSH                    |  | RDP       |              |                      |  |            |  |            |  |                              |  | GuestOS Toolset |  | VM Introspection   |  | CPU, Memory, Disk, etc. |  | SNMP     |  | Real User Monitoring |  | Synthetic Performance Monitoring |  | Temperature, Fan Speed, Disk, etc. |  |                      |  |                 |  |             |  |           |  |           |  |



# Investigations

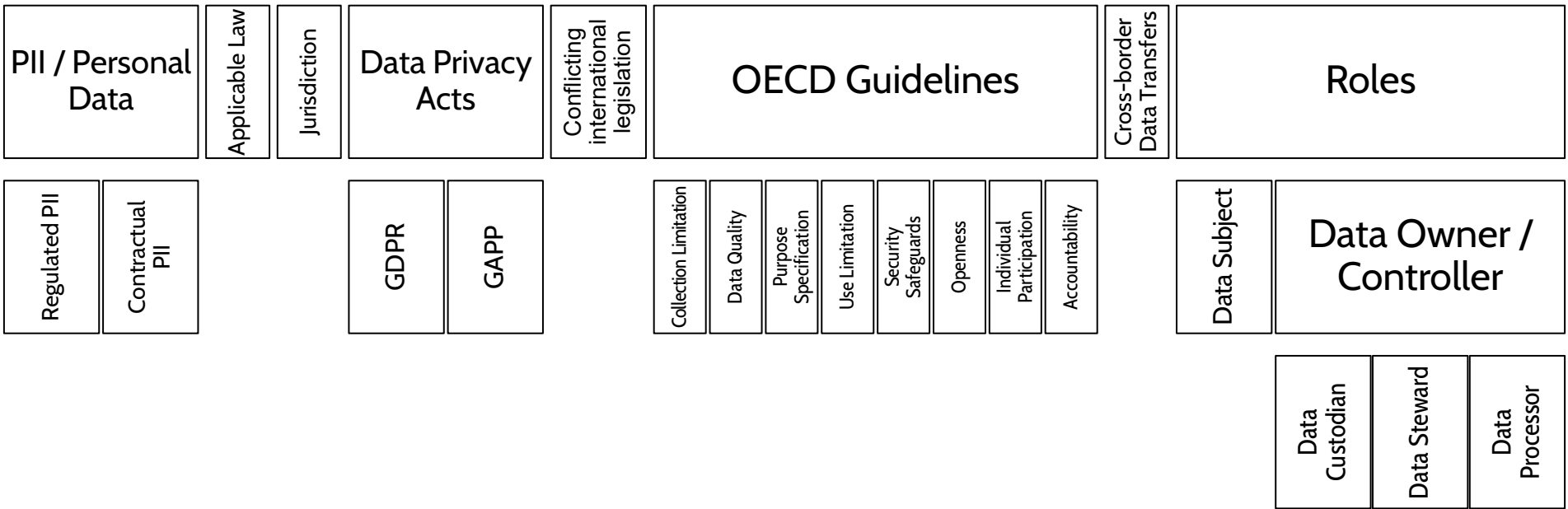
|                           |                            |                                          |                   |                      |                                                  |                                                                      |           |          |          |            |                   |
|---------------------------|----------------------------|------------------------------------------|-------------------|----------------------|--------------------------------------------------|----------------------------------------------------------------------|-----------|----------|----------|------------|-------------------|
| Secure the Scene          | Collect & Control Evidence |                                          |                   |                      |                                                  | Rules of Evidence                                                    |           |          |          |            | Document & Report |
| Sources of Evidence       |                            |                                          | Forensics Support |                      |                                                  | Chain of Custody                                                     | Authentic | Accurate | Complete | Convincing | Admissible        |
| Oral / Written statements | Documents                  | Digital Forensics                        | eDiscovery        | SaaS                 | PaaS                                             | IaaS                                                                 |           |          |          |            |                   |
| Snapshooting MVs          | Live Evidence (Volatile)   | Metadata on Infrastructure Configuration | ISO 27050         | Rely entirely on CSP | CSP for Infrastructure & Consumer for their apps | CSP for Infrastructure & Consumer for their virtual systems and apps |           |          |          |            |                   |



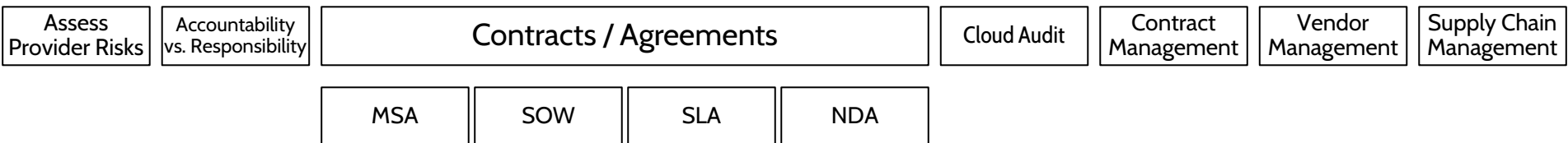
6

# Legal, Risk and Compliance

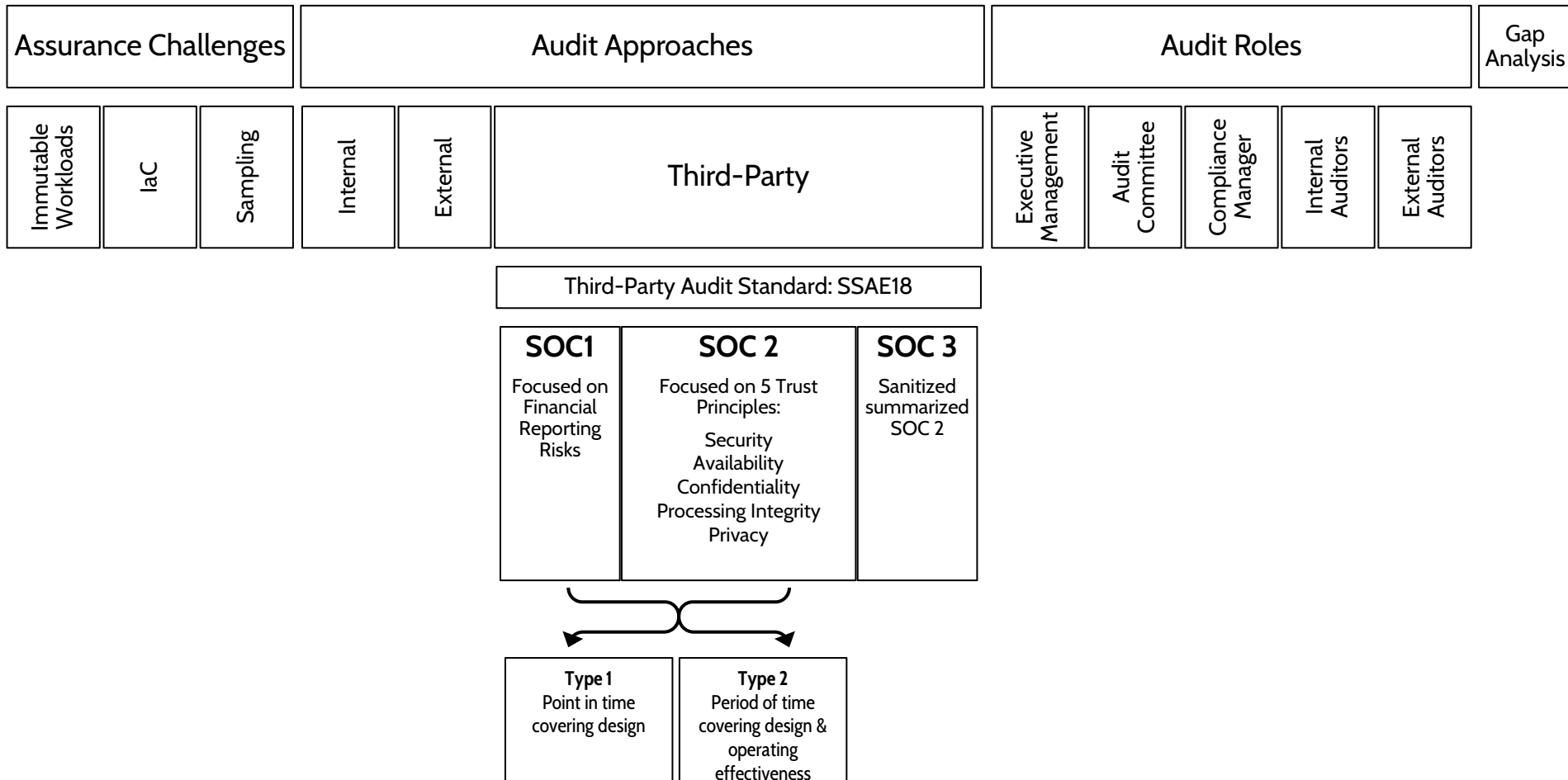
## Privacy



## Outsourcing & Cloud Contracts



# Cloud Audit



# Printable Blank CCSP MindMaps

---

Print out the following blank *MindMaps* and fill them in as you watch our *MindMap* videos!



## Alignment of Security Function to Business Strategy

|  |
|--|
|  |
|--|

|  |
|--|
|  |
|--|

The diagram illustrates a hierarchical tree structure. The root node is a rectangle divided into four equal quadrants. The top-left quadrant is further divided into four smaller rectangles. The top-right quadrant is divided into two smaller rectangles. The bottom-left quadrant is divided into four smaller rectangles. The bottom-right quadrant is divided into four smaller rectangles. The top-right quadrant is shaded gray.



# Cloud Shared Considerations

|  |
|--|
|  |
|--|

|  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|

# Frameworks

|  |
|--|
|  |
|--|

|  |  |  |  |
|--|--|--|--|
|  |  |  |  |
|--|--|--|--|

|  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|

# Cost Benefit Analysis

|  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|

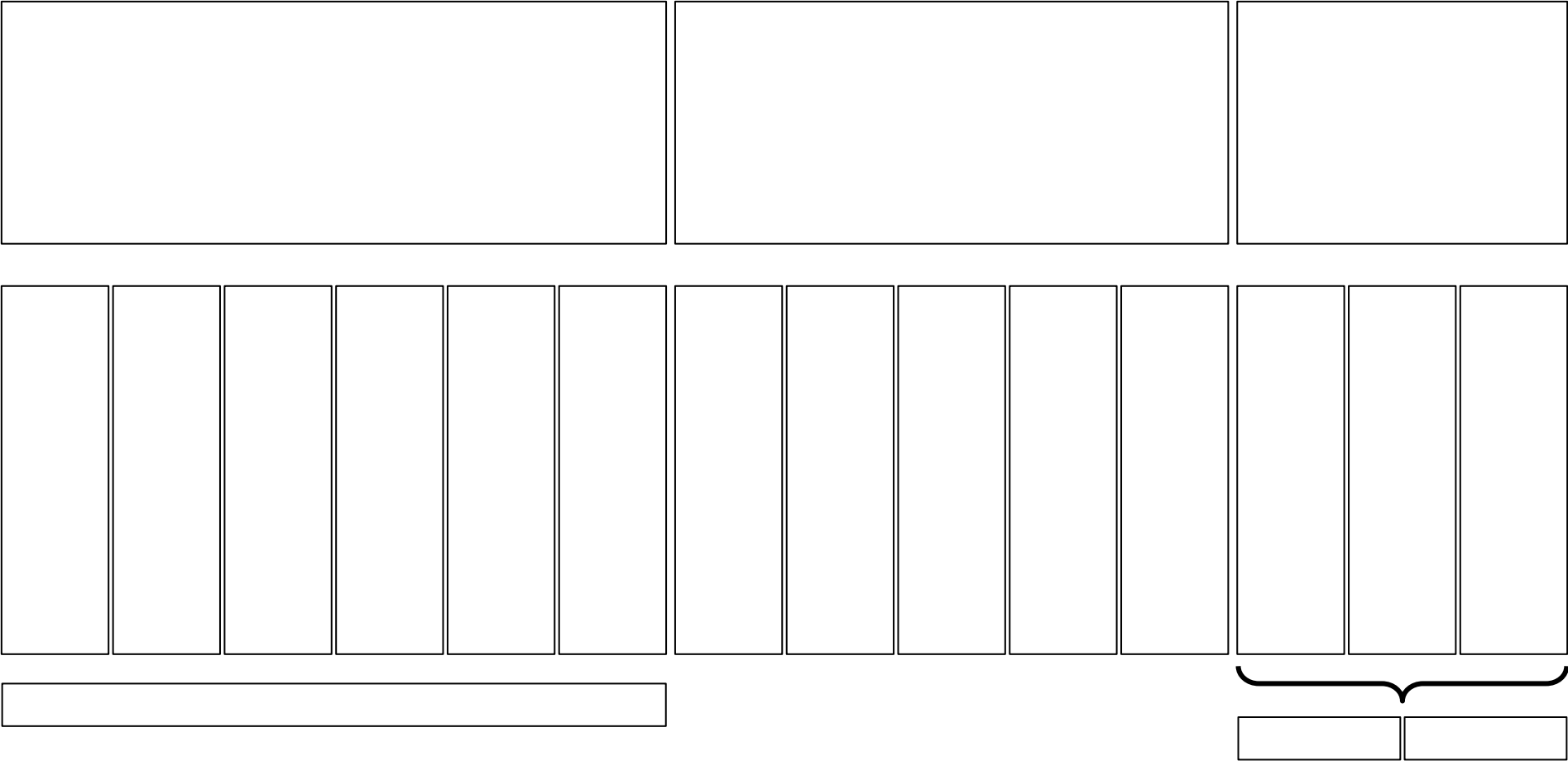
# Evaluation Criteria

|  |  |  |
|--|--|--|
|  |  |  |
|  |  |  |
|  |  |  |

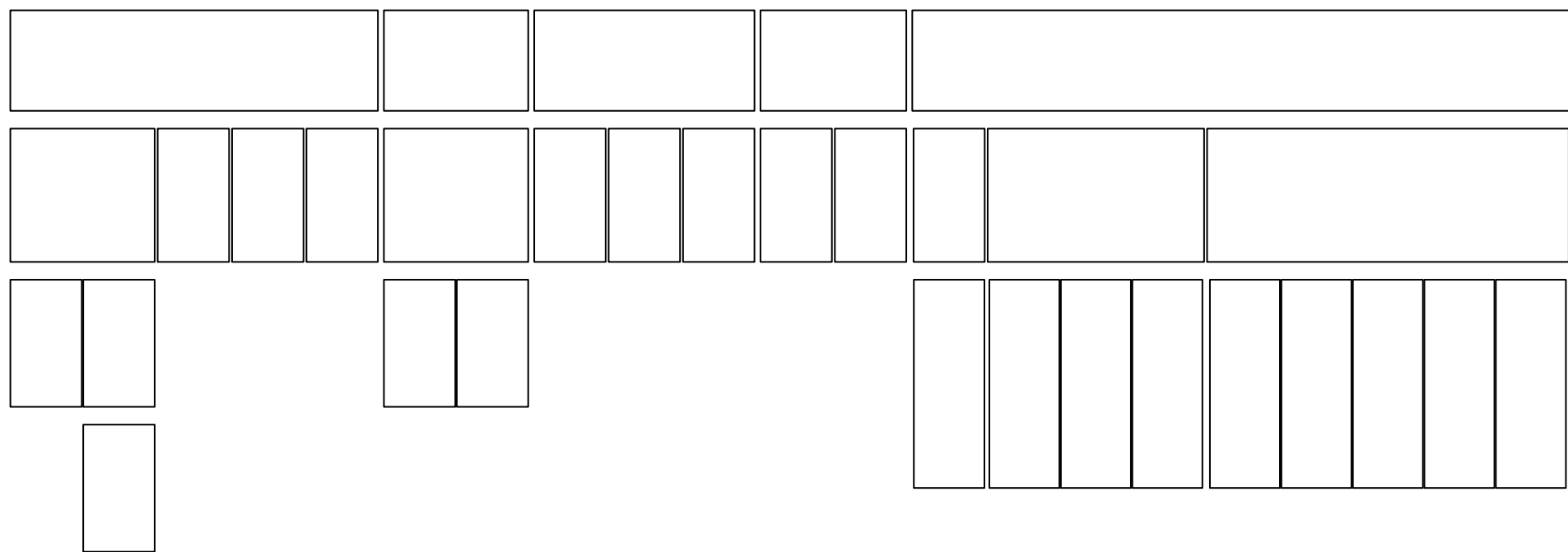
## AI/ML Foundations, Risks, and Governance

[illegible]

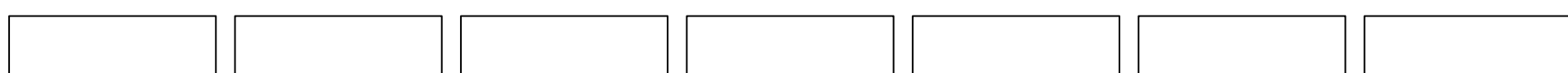
# Cloud Data Lifecycle



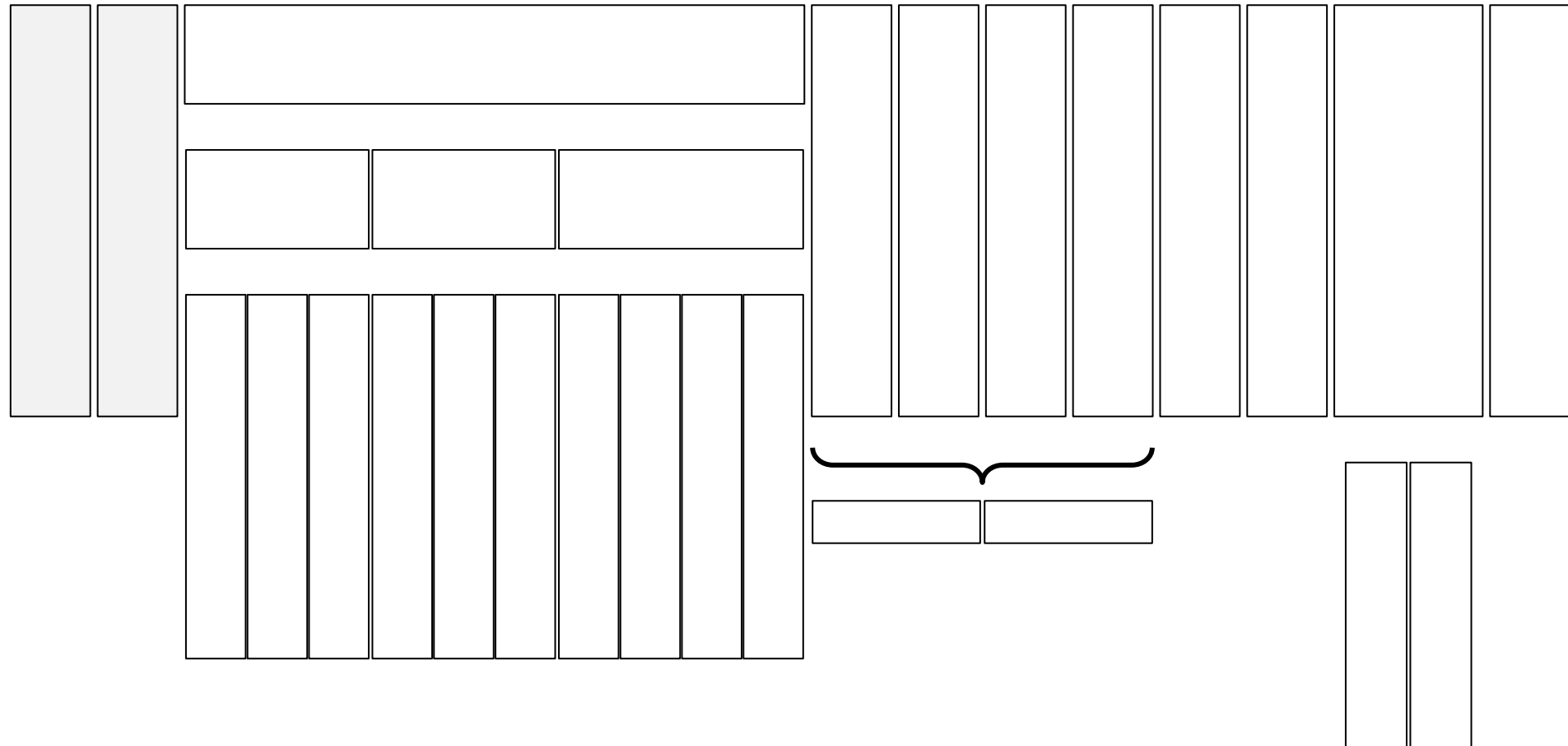
# Cloud Data Storage



# Threats to Storage



# Data Security Strategies



## Data Discovery

|  |  |
|--|--|
|  |  |
|  |  |

## Asset Classification

|  |  |  |  |
|--|--|--|--|
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Log Review & Analysis

|  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

## Digital Rights Management (DRM)

|  |  |  |
|--|--|--|
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

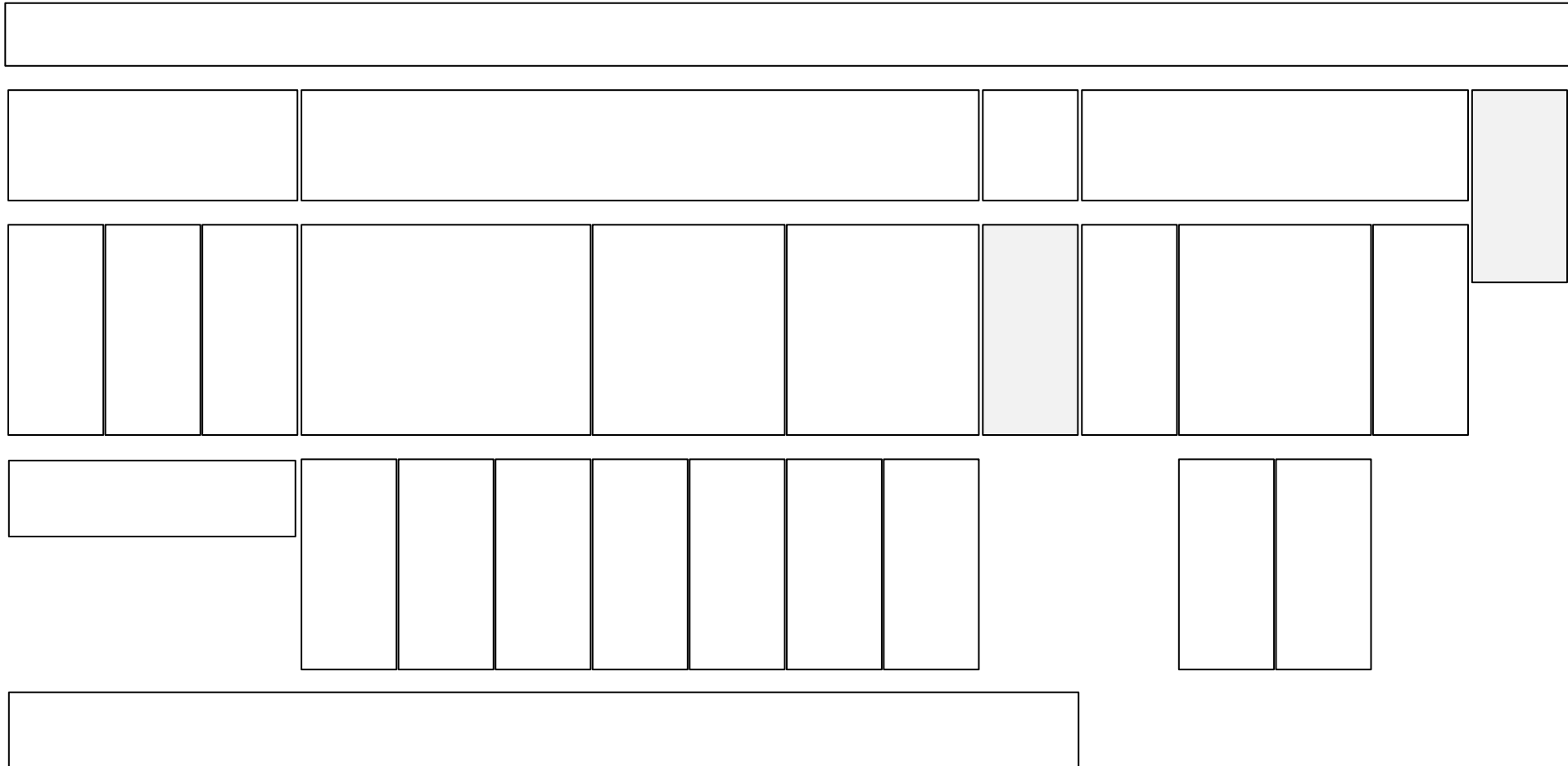
## Data Retention, Archiving & Deletion

|  |  |  |
|--|--|--|
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# AI/ML Data Protection

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

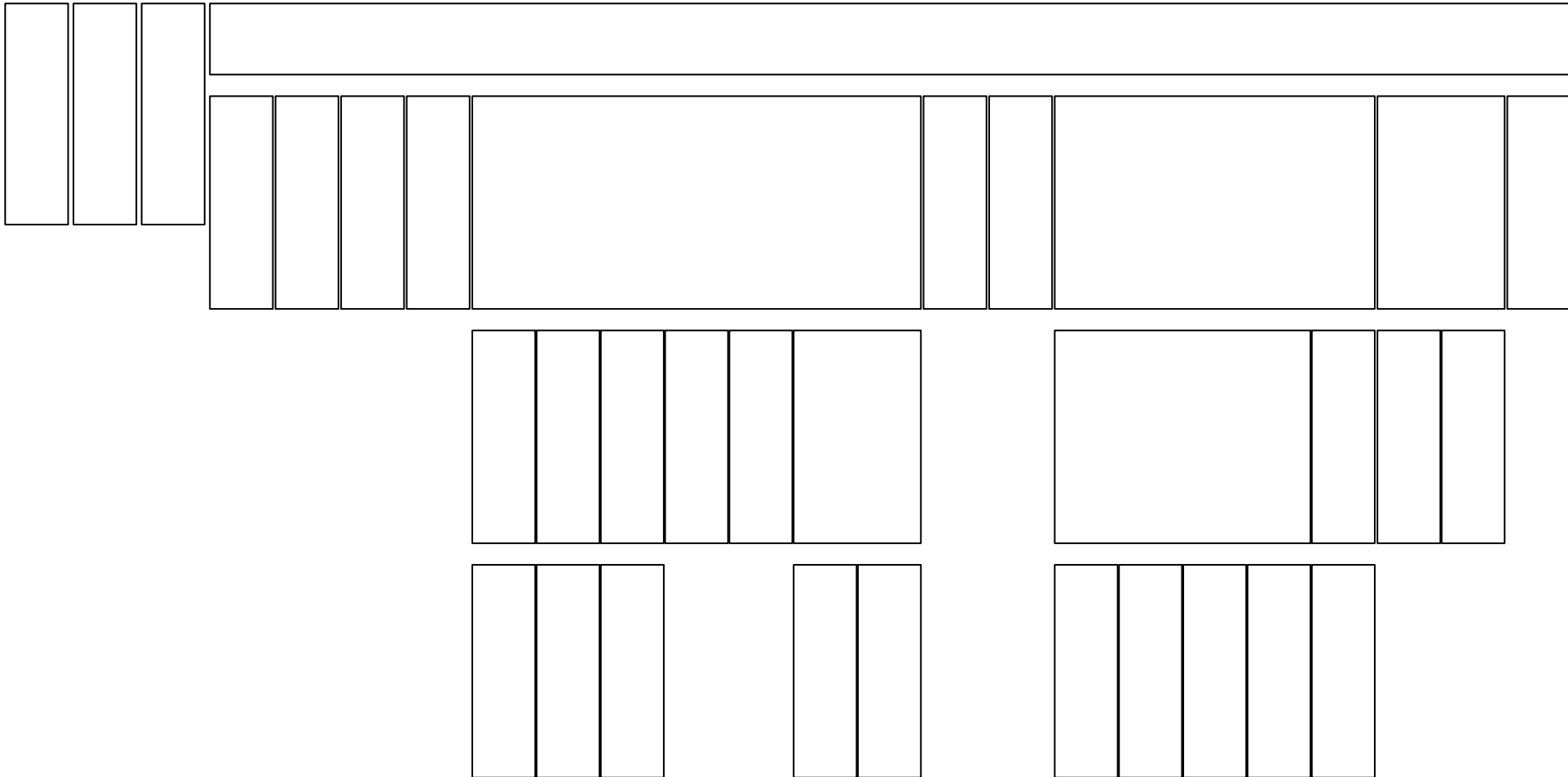
# Cloud Infrastructure Components



# Management Plane

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

# Data Center Design



# Attack Vectors

|  |  |
|--|--|
|  |  |
|--|--|

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

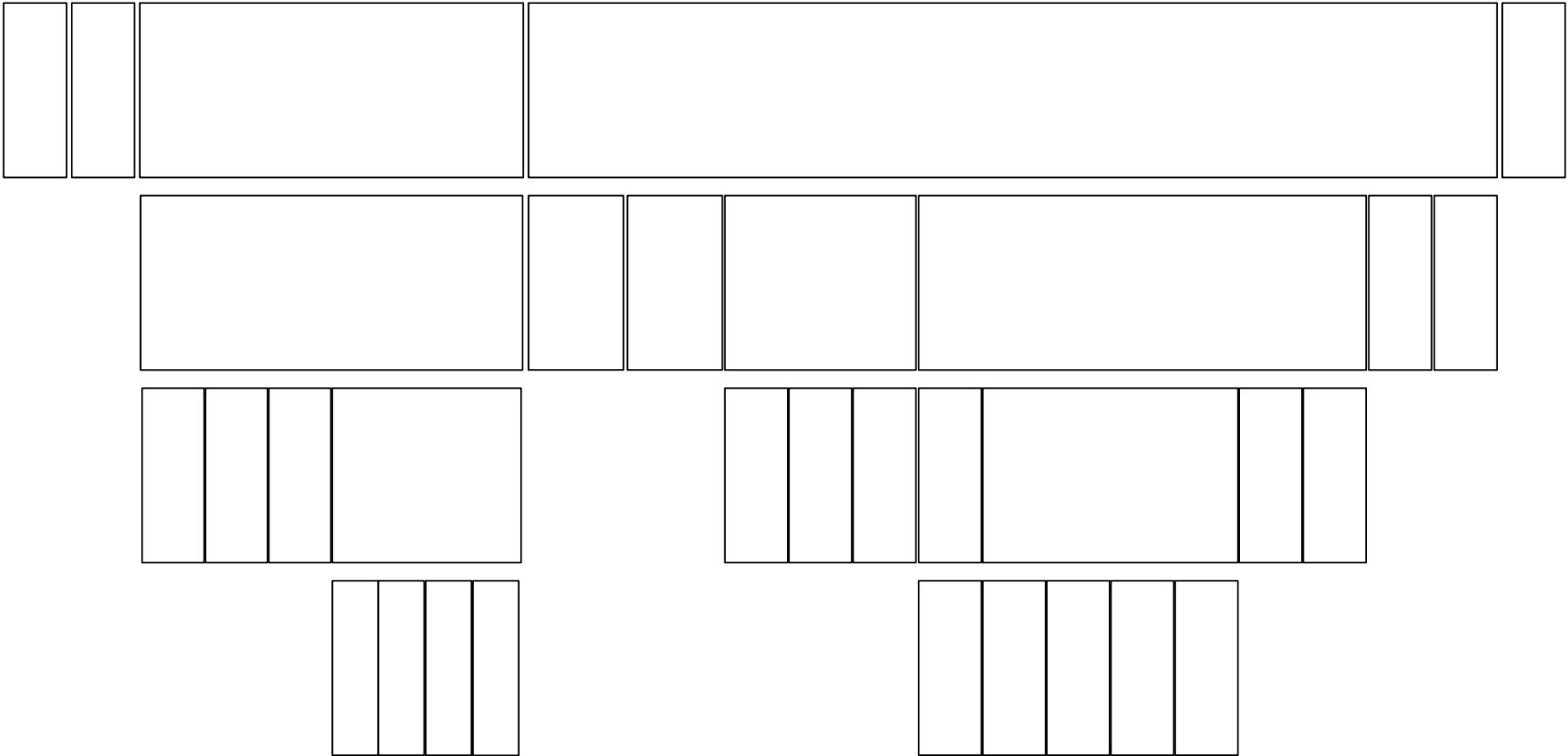
# Risks

|  |  |
|--|--|
|  |  |
|--|--|

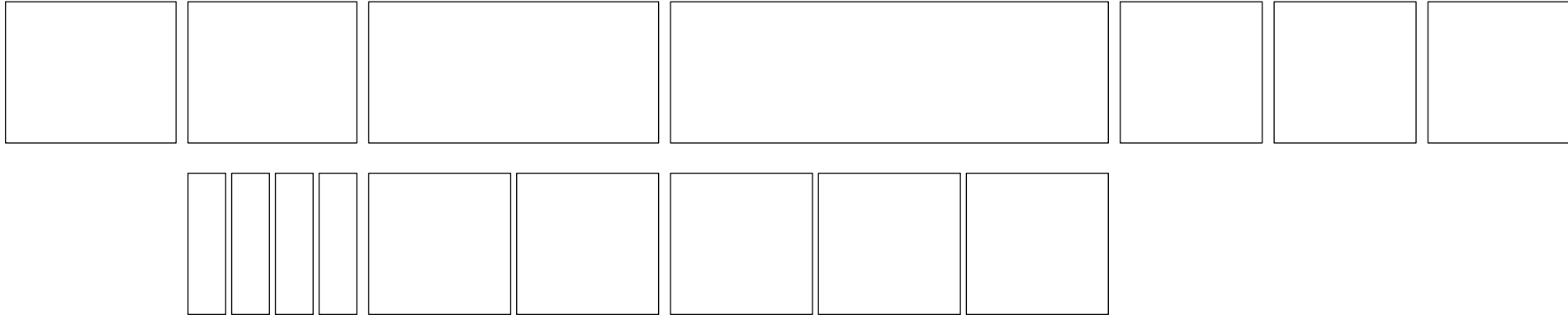
|  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|



# Network Defense



# Business Continuity Management (BCM)



# Cloud Development

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |





# Common Vulnerabilities & Threat Modeling

|  |  |  |  |  |  |
|--|--|--|--|--|--|
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Verified Secure Software

|  |  |  |
|--|--|--|
|  |  |  |
|  |  |  |
|  |  |  |

# Cryptographic Services

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|  |  |  |  |  |

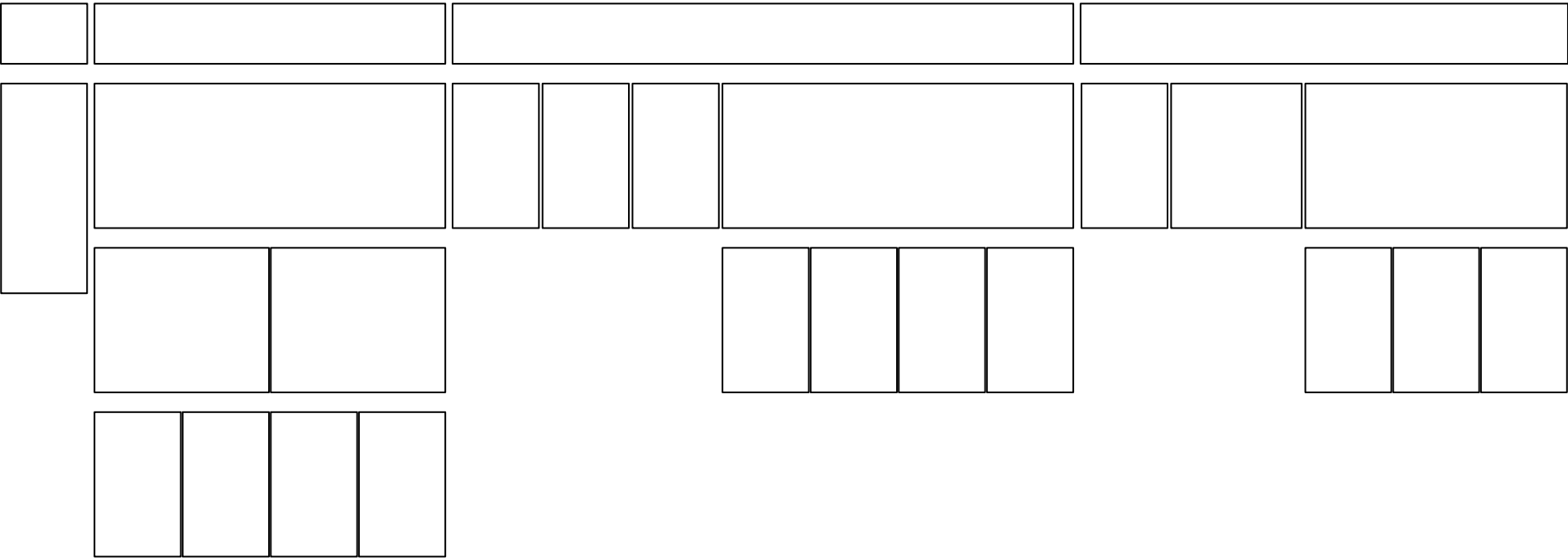
# Cryptography

|  |  |  |  |
|--|--|--|--|
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

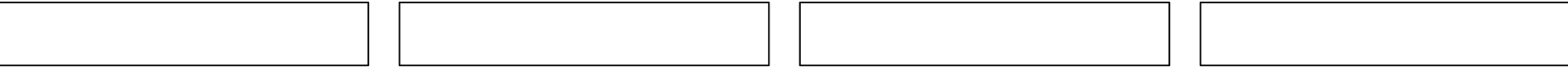
# Key Management

|  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Crypto in the Clouds



# Proxies



# Access Control

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

## Cloud Operations

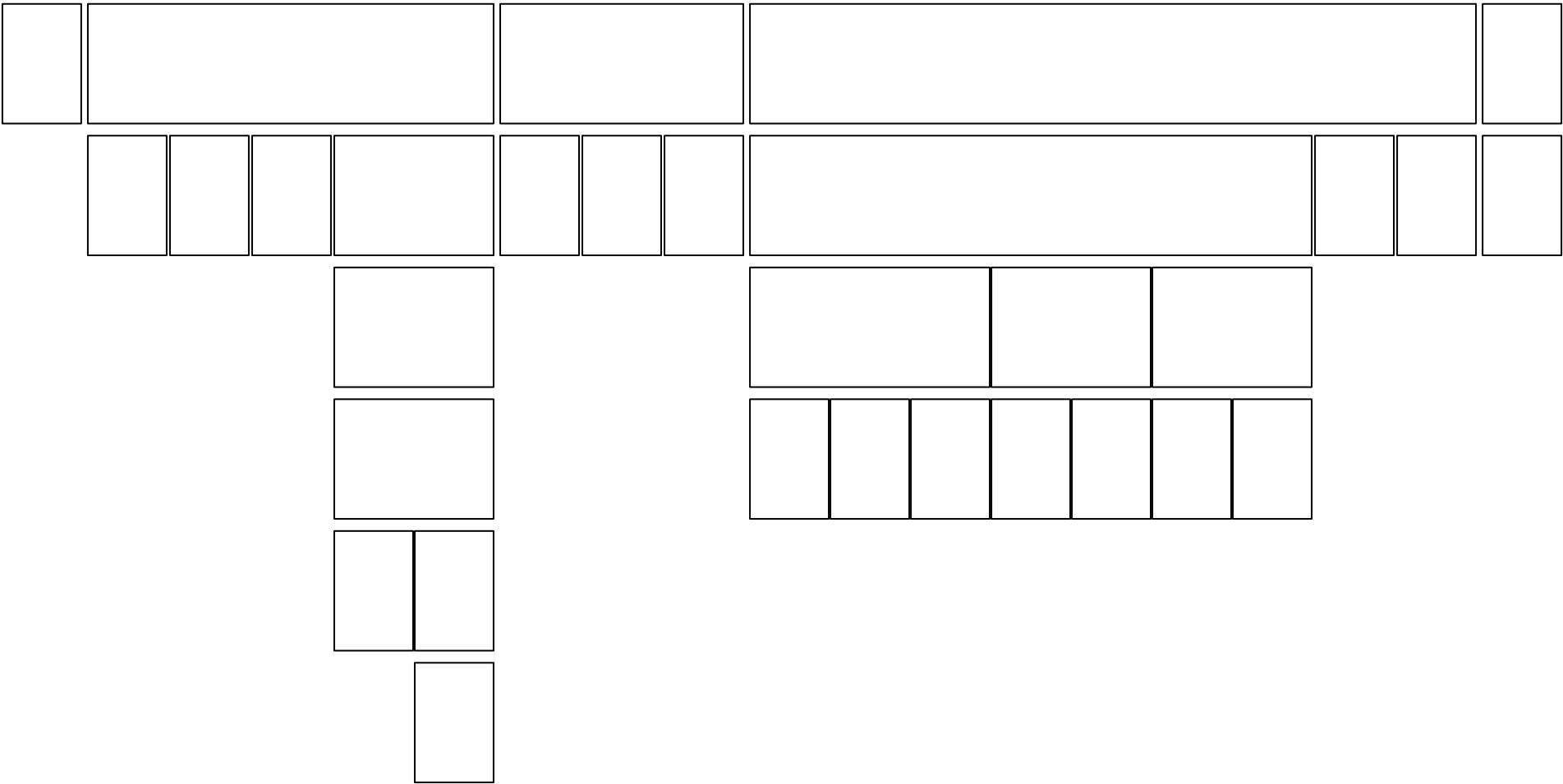
|  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|

[illegible]

|  |  |  |  |
|--|--|--|--|
|  |  |  |  |
|--|--|--|--|

|  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|

# IT Service Management



# Investigations

|  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |





# Hi there!

---

I hope our CCSP MindMaps have helped identify the critical concepts you need to know for the exam!

These MindMaps are a small part of our complete CCSP MasterClass.

If you're looking for detailed explanations of all the concepts covered in these MindMaps + everything else you need to confidently pass the CCSP exam, check out our **CCSP MasterClass** here: [destcert.com/CCSP](https://destcert.com/CCSP)

We have guided thousands of folks to confidently pass the CCSP exam since it launched in 2015. We provide expert instruction and an integrated intelligent personalized system of study resources and tools.

All the best in your studies!



**Rob Witcher**

Co-founder & Master Instructor