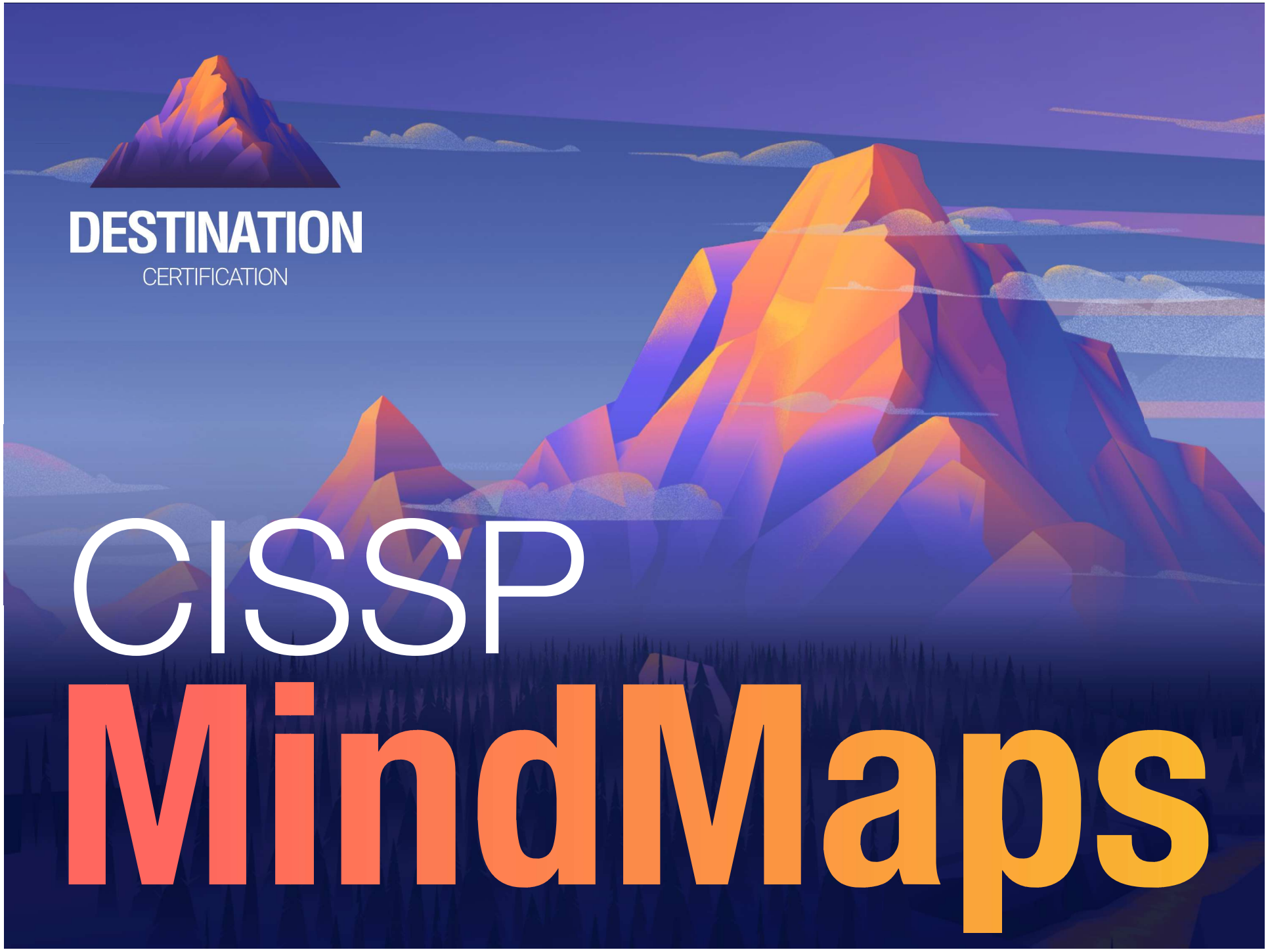
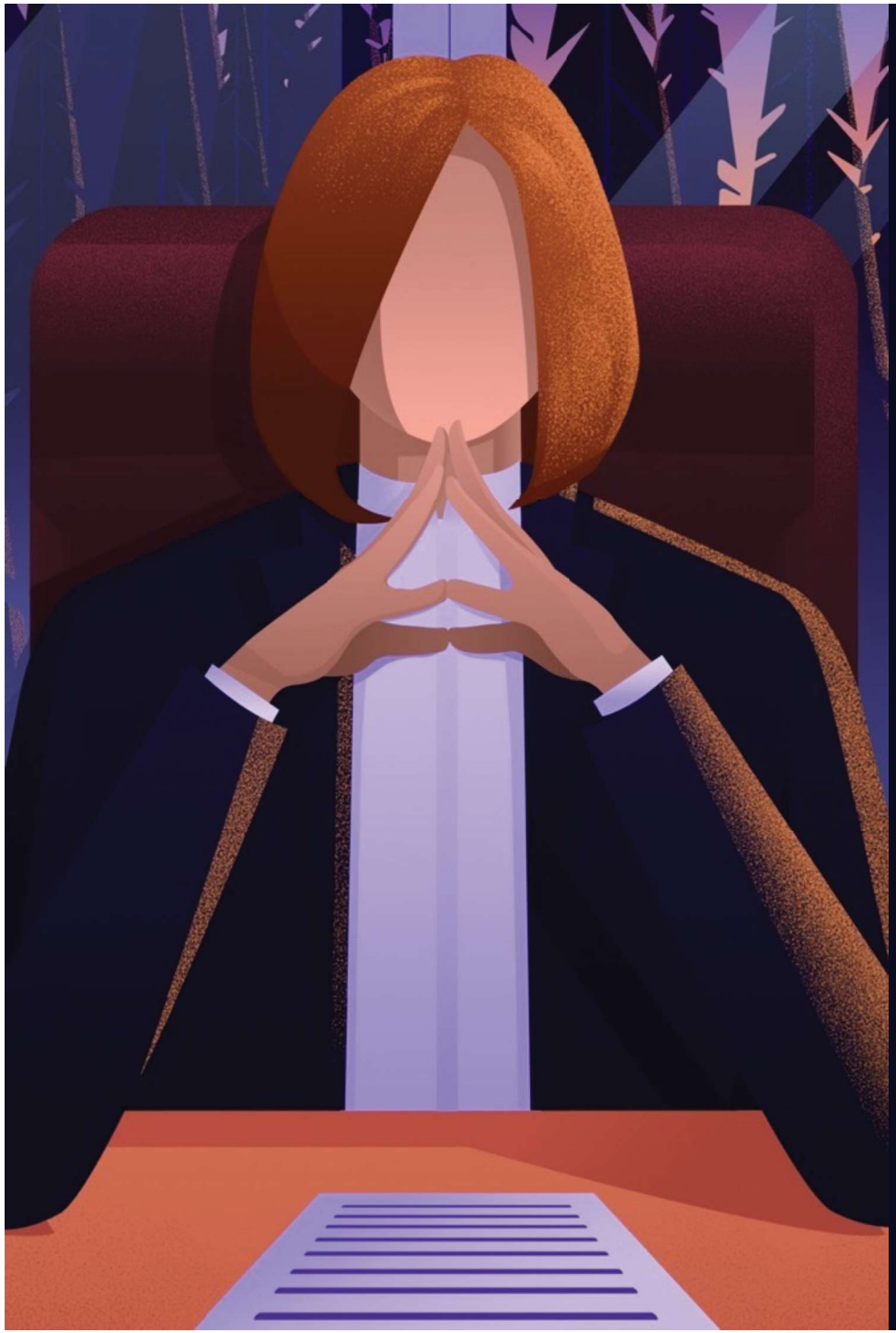
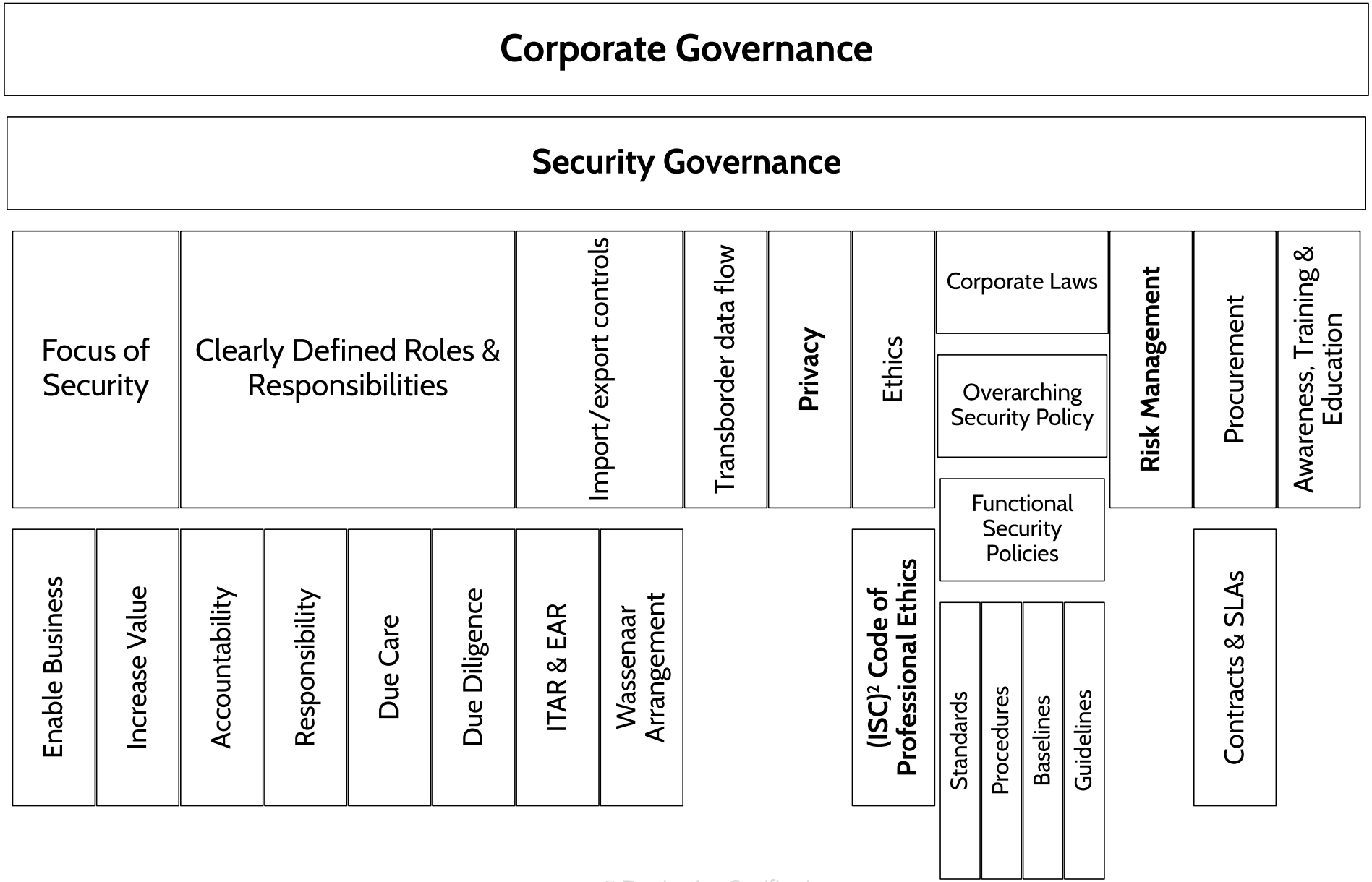

DESTINATION
CERTIFICATION
CISSP
MindMaps



Domain 1

Security and Risk Management

Alignment of Security Function to Business Strategy



Privacy

State or condition of being free from being observed or disturbed by other people

Privacy policy	Personal Data	Data Lifecycle	OECD Guidelines	GDPR	Cannot Achieve Privacy without Security

Standards Procedures Baselines Guidelines	PII SPI PHI PI	Direct Identifiers	Indirect Identifiers	Online Identifiers	Creation / Update	Store	Use	Share	Archive	Destroy	Collection Limitation	Data Quality	Purpose Specification	Use Limitation	Security Safeguards	Openness	Individual Participation	Accountability	Supervisory Authority (SA)	Breaches reported within 72 hours

Intellectual Property

Trade Secret	Patent	Copyright	Trademark

Risk Management

1. Asset Valuation

- Quantitative
- Qualitative

2. Risk Analysis

- Threats
  - Threat Modeling
    - STRIDE
    - PASTA
    - DREAD
- Vulnerabilities
  - Vuln. Assessment & Pen. Testing
- Likelihood
- Impact
- Quantitative
  - ALE = SLE(Value x Exposure) x ARO
- Qualitative

3. Treatment

- Avoid
- Transfer
- Mitigate
  - Administrative
  - Technical / Logical
  - Physical
  - Safeguards
  - Countermeasures
  - Directive
  - Deterrent
  - Preventative
  - Detective
  - Corrective
  - Recovery
  - Compensating
  - Functional
  - Assurance
- Accept

Risk Frameworks

- **RMF** NIST 800-37
  1. Prepare
  2. Categorize
  3. Select
  4. Implement
  5. Assess
  6. Authorize
  7. Monitor
- ISO 31000
- COSO
- ISACA Risk IT

Domain 2

Asset Security

Asset Classification

Asset Inventory

Assign Ownership

Classify

based on Value

Data classification policy

Classification

Categorization

Standards
Procedures
Baselines
Guidelines

Security Label

Security Marking

System Readable

Human Readable

Protect

based on Classification

Roles

Data Owner / Controller
Data Processor
Data Custodian
Data Steward
Data Subject

Rest

Encryption
Access Control
Backups

Motion

End-to-End
Link
Onion

Use

Archive

Retention Period

Defensible Destruction

Destruction

Media Destruction
Shred / Disintegrate / Incinerate / Drill
Degauss
Crypto shredding
Overwrite / Wipe / Erasure
Format

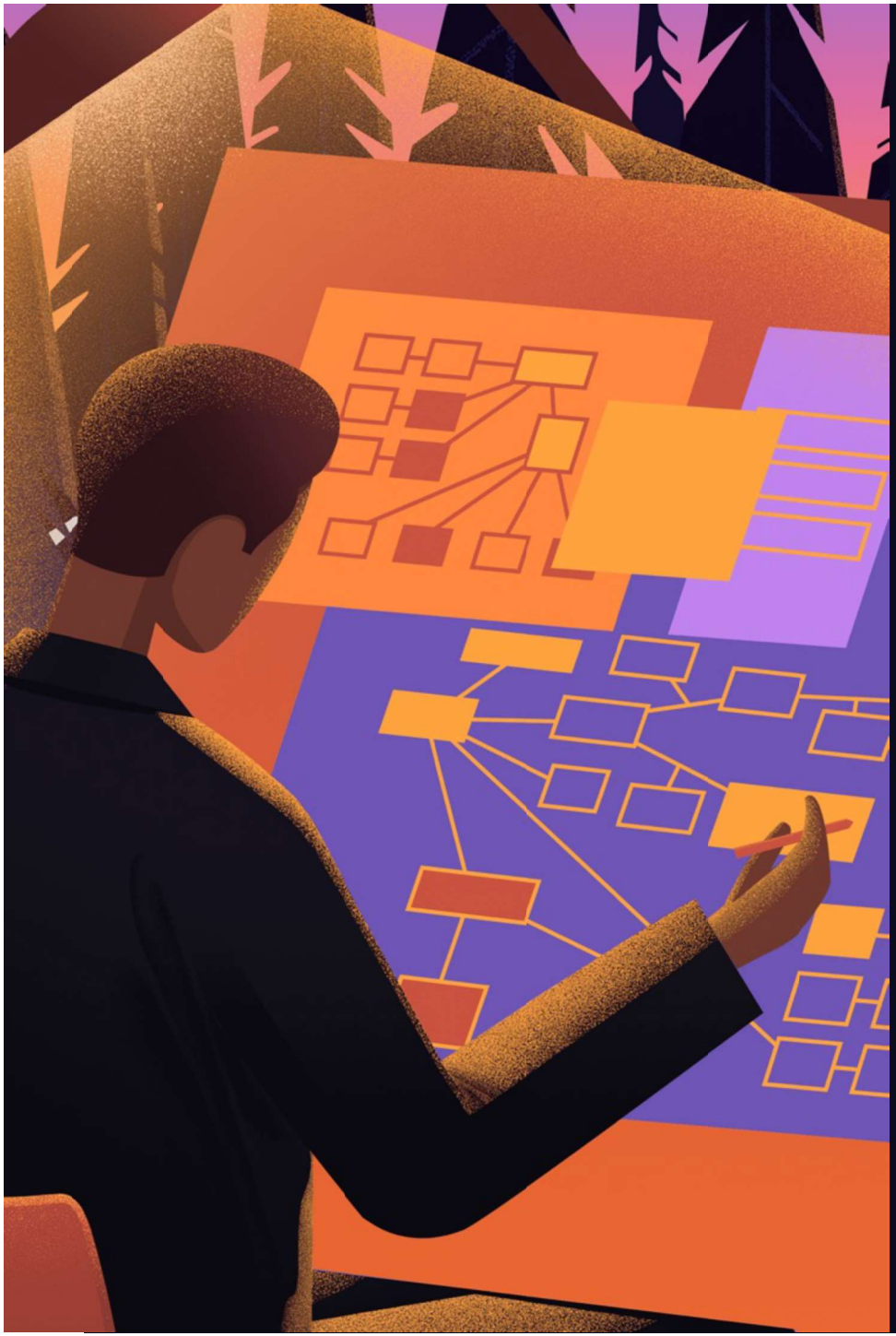
Purging

Clearing

DRM

DLP

Assess & Review



Domain 3

Security Architecture and Engineering

Models

Enterprise Security Architecture

- Zachman
- Sabsa
- TOGAF

Security Models

Lattice Based

Bell- LaPadula

- Confidentiality
- Simple Security Property
- Star Property
- Strong Star Property

Biba

- Integrity
- Simple Integrity Property
- Star Integrity Property

Lipner
Implementation

Rule Based

Clark-Wilson

- 3 goals of integrity
- 3 Clark-Wilson rules

Brewer -Nash

- Prevent conflicts of interest

Graham – Denning

Harrison -Ruzzo- Ullman

Secure Design Principles

- Threat Modeling
- Least Privilege
- Defense in Depth
- Secure Defaults
- Fail Securely
- Separation of Duties (SoD)
- Keep it Simple
- Zero Trust
- Trust But Verify
- Privacy by Design
- Shared Responsibility

Security Frameworks

- ISO 27001
- ISO 27002
- NIST 800-53
- COBIT
- ITIL
- HIPAA
- SOX
- FedRAMP
- FISMA
- Cyber Kill Chain

Evaluation Criteria

Certification

TCSEC (Orange Book)

Confidentiality only

Single Box only

Functional Levels

D1 – failed or not tested

C1 – Weak protection mechanisms

C2 – Strict login procedures

B1 - Security labels

B2 - Security labels and verification of no covert channels

B3 - Security labels, verification of no covert channels, and must stay secure during start-up

A1 – Verified design

ITSEC

Confidentiality + Integrity

Networked devices

Same Functional levels as TCSEC

Assurance Levels

E0

E1

E2

E3

E4

E5

E6

Common Criteria

ISO 15408

Protection Profile

Target of Evaluation

Security Targets

Functional & Assurance Requirements

Assign EAL

EAL1 – Functionally tested

EAL2 – Structurally tested

EAL3 – Methodically tested & checked

EAL4 – Methodically designed, tested & reviewed

EAL5 – Semi formally designed & tested

EAL6 – Semi formally verified designed & tested

EAL7 – Formally verified designed and tested

Accreditation

Trusted Computing Base (TCB)

Reference Monitor Concept

- Subject
- Mediation
- Object

Hardware Components

- Processor
- Storage
- System Kernel

Software Components

- Firmware
- Middleware

Protection Mechanisms

- Process Isolation
- Processor States
- Operating System Modes
- Ring Protection Model
- Secure Memory Management
- Data Hiding
- Defence in depth

Security Kernel

- Rules
- Logging & Monitoring

Storage

- Primary
- Secondary
- Virtual Memory

Process Isolation

- Memory Segmentation
- Time Division Multiplexing

Processor States

- Problem
- Supervisor

Operating System Modes

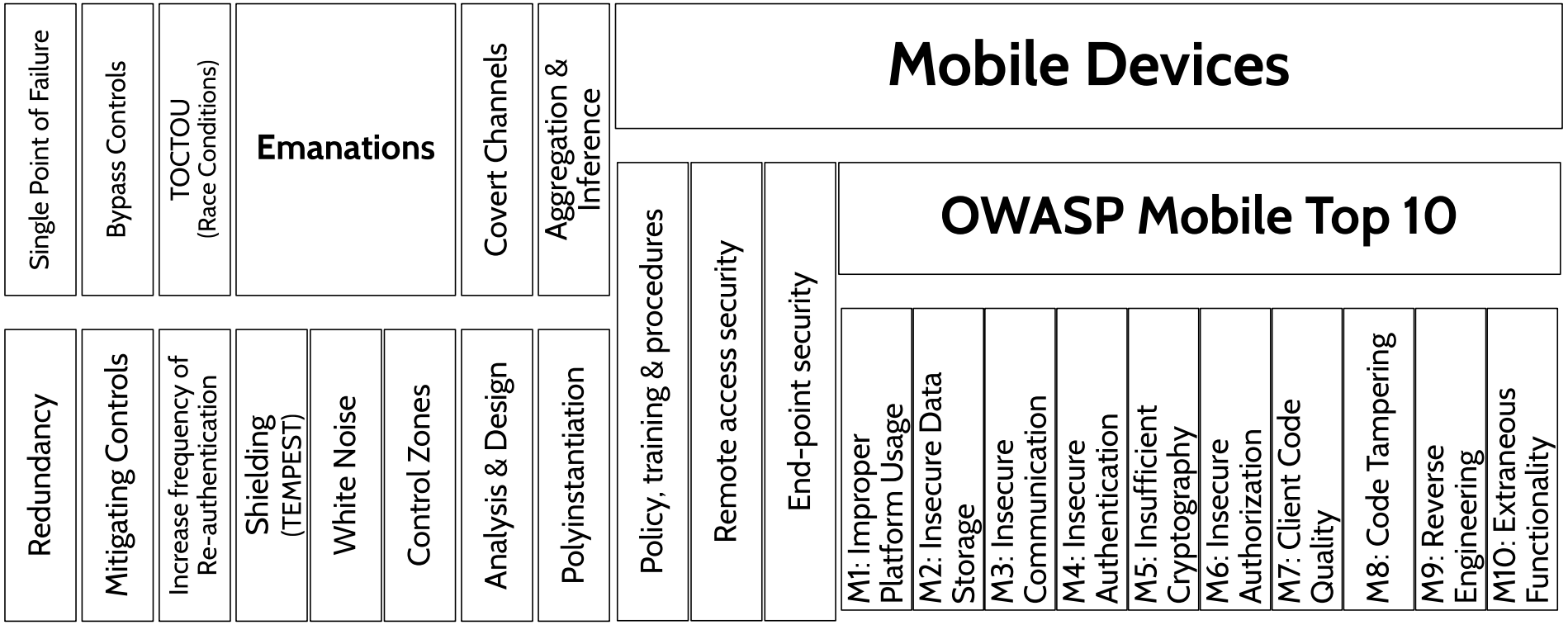
- User Mode
- Kernel Mode

Ring Protection Model

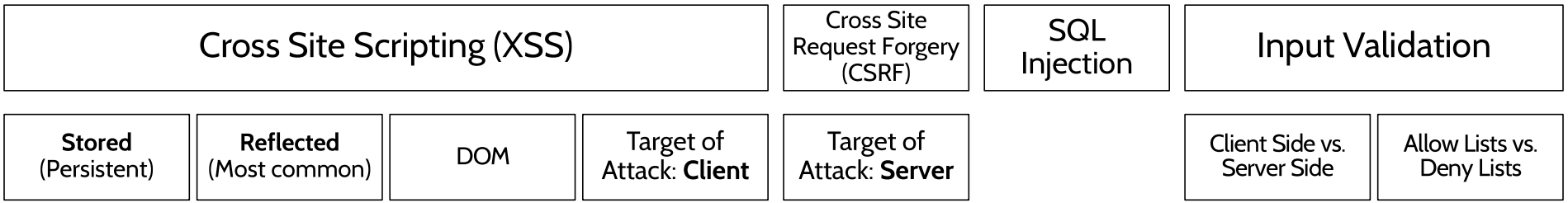
- Ring 3: User Programs
- Ring 0: System Kernel

- Completeness
- Isolation
- Verifiability

Vulnerabilities in Systems



Web-based Vulnerabilities



Cloud Computing

	On-Demand Self Service	Characteristics
	Broad Network Access	
	Resource Pooling	
	Rapid Elasticity	
	Measured Service	
	IaaS	Service Models
	PaaS	
	SaaS	
	Public	Deployment Models
	Private	
	Community	
	Hybrid	
Hypervisor	Virtual Machine	**Virtualized Compute**
Container Engine	Containers	
	Serverless	
	Local	**Identity Provider**
	Cloud	
	Cloud	Cloud identity
	Linked	
	Synced	
	Federated	
Cloud Consumer	Accountable	Roles
Owner / Controller		
Cloud Provider / Processor	Responsible	
Cloud Broker		
Cloud Auditor		
	SPML	**Protocols**
	SAML	
	OpenID	
	OAuth	
	Data Centric	Migration
	SLA	
	Snapshot, Virtual Disk, Image	Forensics
	Crypto Shredding / Crypto Erase	Data Destruction

Cryptographic Services

- **Confidentiality**
- **Integrity**
  - = Hashing
- **Authenticity**
- **Non-Repudiation**
  - **Origin**
  - **Delivery**
- **Access Control**

Cryptographic terminology

- Plaintext
- Encrypt
- Key / Crypto variable
- Decrypt
- Key clustering
- Work factor
- Initialization vector/Nonce
- Confusion
- Diffusion
- Avalanche

Secret Writing

Hidden

- Steganography
- Null Cipher

Scrambled (Cryptography)

One-way

- **Hashing**
  - MD5
  - SHA-1
  - SHA-2
  - SHA-3

Two-way

Symmetric

- **Block**
  - **DES**
  - **3DES**
  - **AES** (Rijndael)
  - CAST-128
  - SAFER
  - Blowfish
  - Twofish
  - RC5/RC6
  - **Block Modes:**
    - **ECB**
    - CBC
    - CFB
    - OFB
    - **CTR**
- **Stream**
  - **RC4**

Asymmetric

- **Factoring**
  - **RSA**
- **Discrete Log**
  - Diffie-Hellmann (key exchange)
  - Elliptic Curve (ECC)
  - El Gamal
  - DSA
- **Digital Certificates**
- **Digital Signatures**

Substitution

- Caesar Cypher
- Monoalphabetic
- Polyalphabetic
- Running
- **One-time Pads**

Transposition

- Spartan Scytale
- Rail Fence (zigzag)

Digital Signatures

- Integrity
- Authenticity
- Non-repudiation
  - Origin
  - Delivery

Digital Certificates

- Verify the owner of a Public Key
  - X.509
  - Replacement
  - Revocation
    - CRL
    - OCSP
  - Pinning

PKI

- Certificate Authority (Root of Trust)
- Registration Authority
- Intermediate / Issuing CA
- Certificate DB (Revocation List)
- Certificate Store (Local)

Key Management

- Kerchhoff's Principle
- Generation
- Distribution
  - Diffie-Hellmann
  - Out-of-band
  - Hybrid
- Storage
  - TPM
  - HSM
- Rotation
- Disposition
  - Crypto-shredding
  - Key Destruction
- Recovery
  - Split Knowledge
  - Dual Control
  - Key Escrow

Cryptanalysis

Cryptanalytic Attacks

- Brute Force
- Ciphertext Only
- Known Plaintext
- Chosen Plaintext
- Chosen Ciphertext
- Linear & Differential
- Factoring

Cryptographic Attacks

- Man-in-the-middle
- Replay
- Pass the Hash
- Temporary Files
- Impleme-ntation
- Side Channel
  - Power
  - Timing
  - Radiation Emissions
- Dictionary Attack
- Rainbow Tables
- Birthday Attack
- Social Engineering
  - Purchase Key
  - Rubber Hose

Physical Security

Safety of people

Categories of Controls

Layered Defense

Deter
Delay
Detect
Assess
Respond

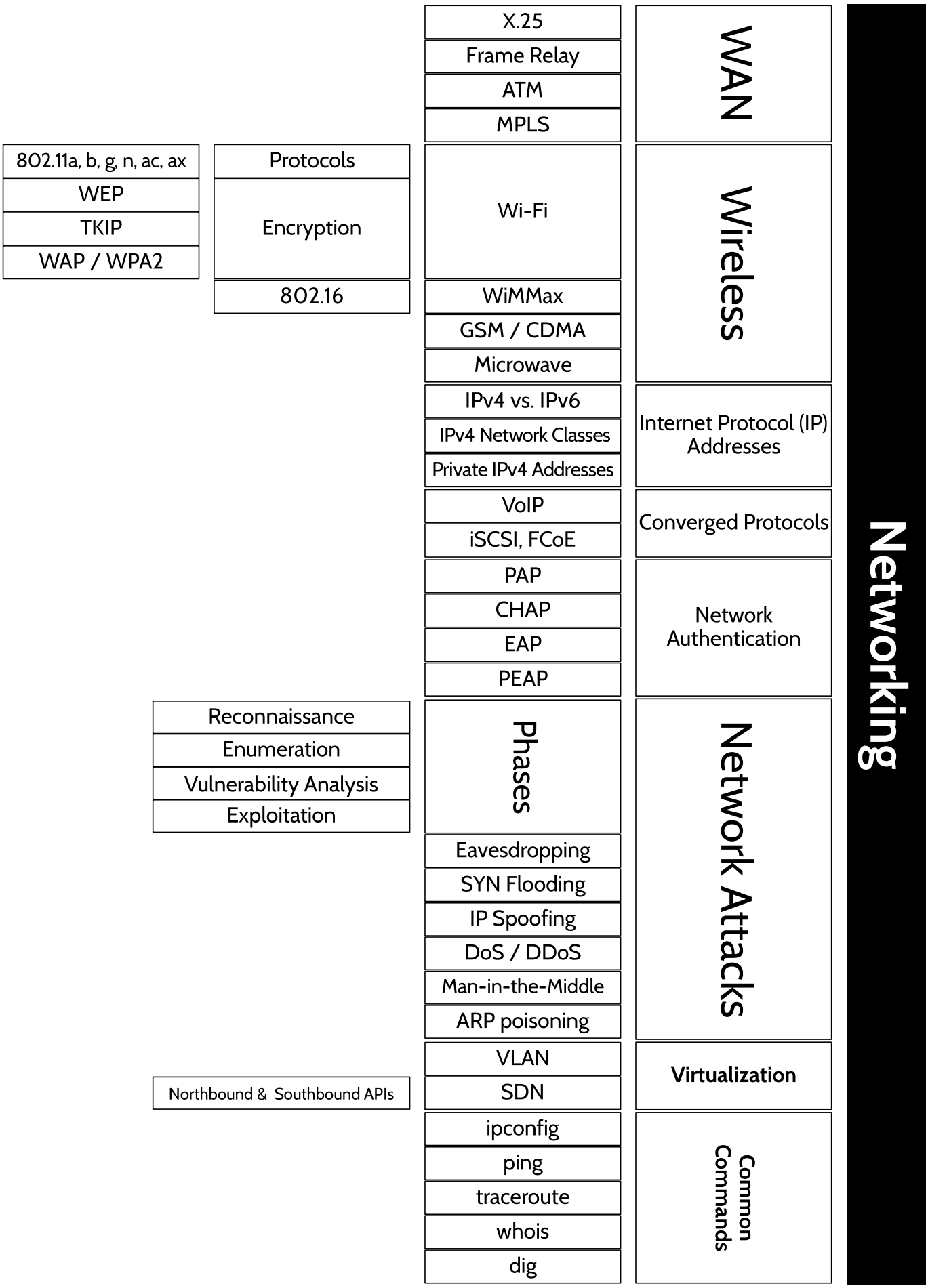
- Perimeter
  - Landscape
  - Grading
- Cameras
- Passive Infrared Devices
- Lighting
- Card Readers / Badges
- Doors / Mantraps
- Locks
  - Mechanical
  - Digital
- Windows
  - Shock
  - Glass break
- Walls
- Skimming
- Infrastructure
  - Network
  - Power
    - UPS
    - Generator
    - Power Outages
    - Power Degradation
  - HVAC
    - Temperature
    - Humidity
    - Air Quality
- Fire Detection
  - Flame (Infrared)
  - Smoke
    - Ionization
    - Photo-electric
    - Dual
  - Heat (Thermal)
- Fire Suppression
  - Water
    - Wet
    - Dry
    - Pre-action
    - Deluge
  - Gas
    - INERGEN
    - Argonite
    - FM-200
    - Aero-K
  - Extinguisher
  - CO_2

Domain 4

Communication and Network Security

Open Systems Interconnection (OSI) Model

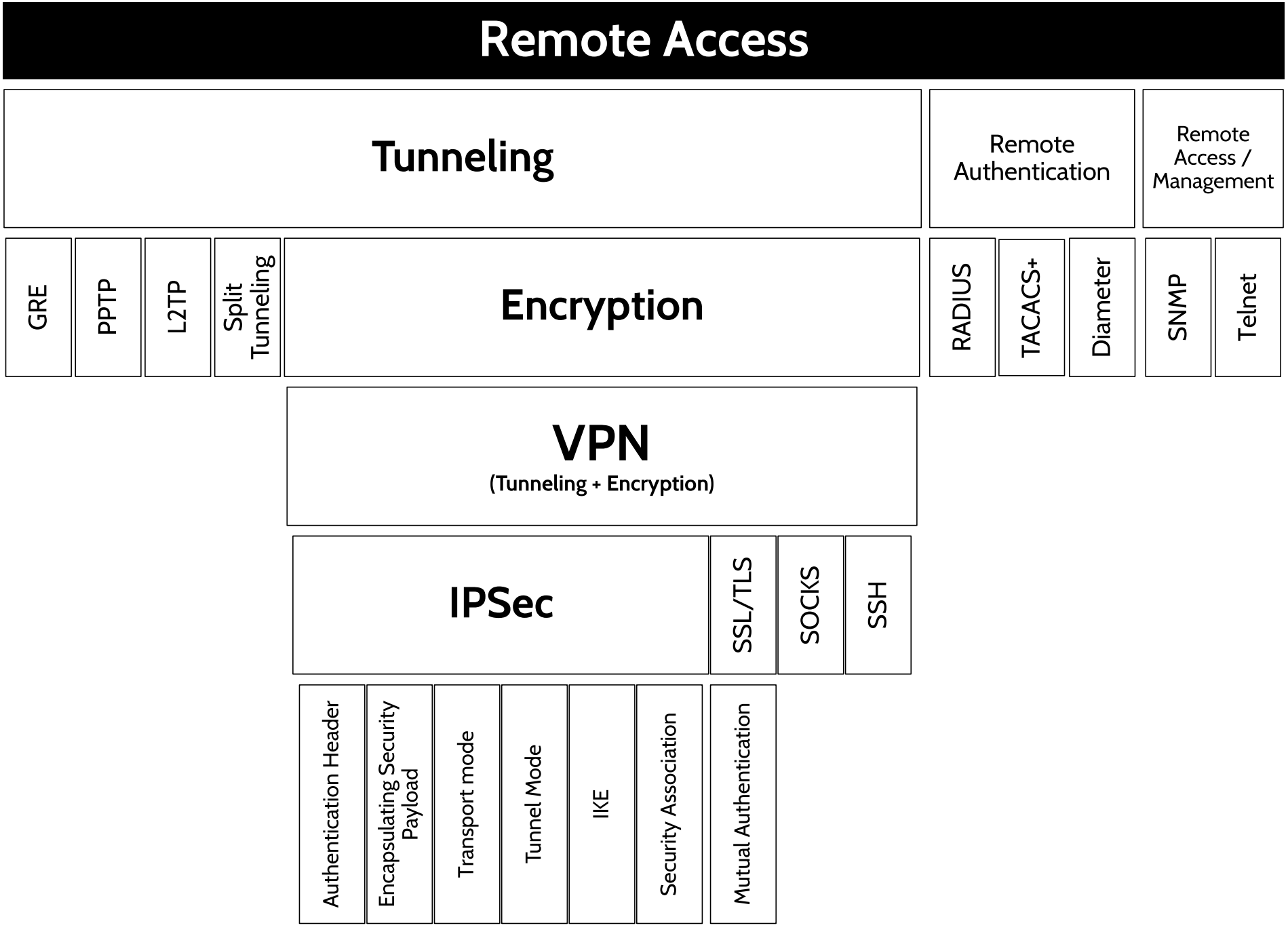
7. Appl.	Devices	Protocols	**Application** Firewalls
			HTTP/S, DNS, SSH, SNMP, LDAP, DHCP
6. Presentation			
5. Session	Devices	Protocols	Circuit Proxy Firewall
			NetBIOS & RPC
4. Transport	Ports = Services	Protocols	TCP/UDP, SSL/TLS & BGP
			Common Ports
3. Network	IP Address	Protocols	ICMP (Ping), IPSec, IGMP
	Devices		Routers & Packet Filtering Firewalls
2. Datalink	MAC Address	Protocols	ARP, PPTP, PPP, PAP, CHAP, EAP
	Devices		Switches & Bridges
1. Physical	Collisions	Protocols	802.1x
	Topologies	Devices	Hubs, Repeaters, Concentrators
			CSMA/CD
			CSMA/CA
			Ring
			Mesh
			Star
			Tree
			Bus
	Media		**Wireless:** Radio Frequency, Infrared, Microwave
			Wired: Twisted Pair, Coaxial, Fiber Optic

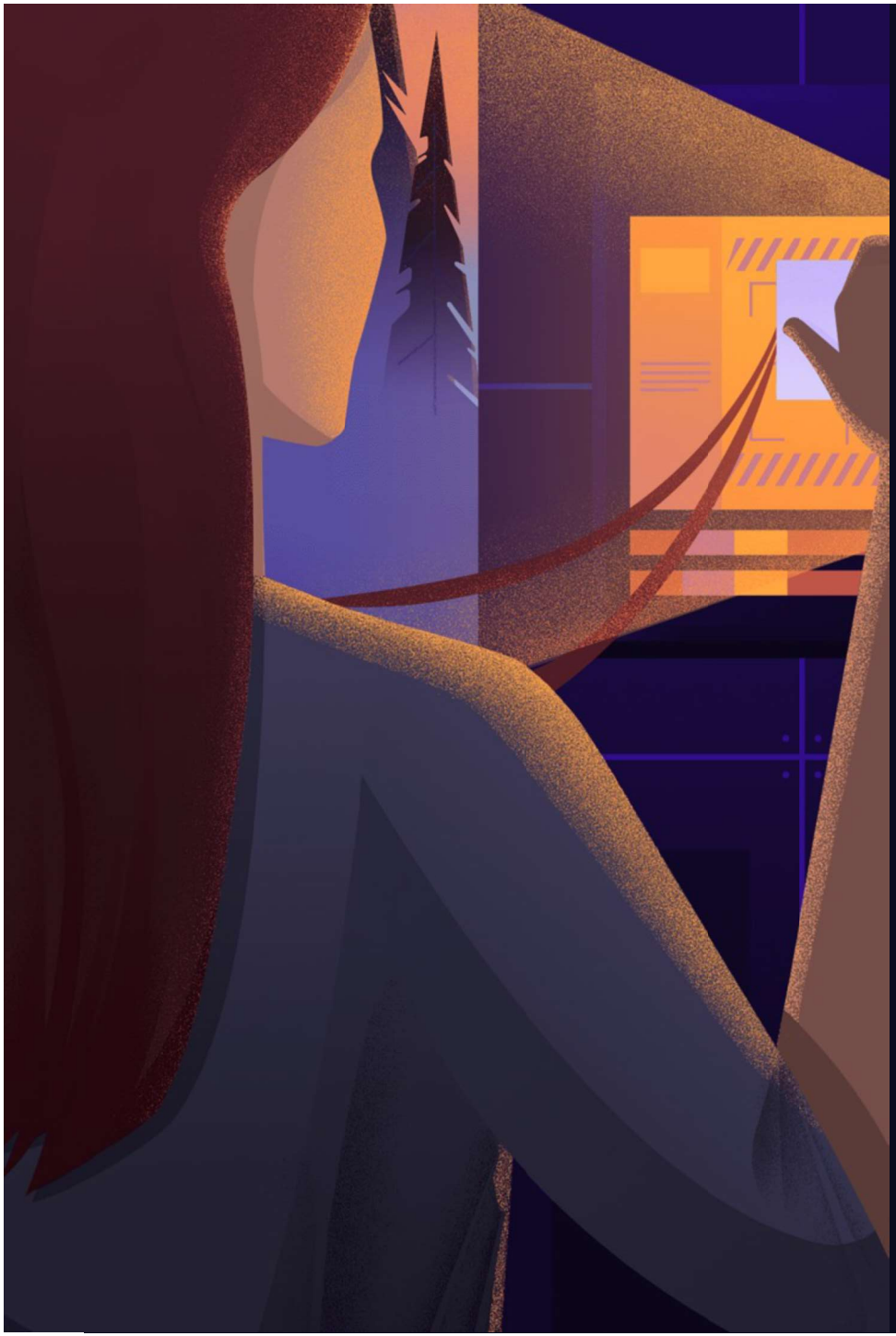


Network Defense

- Defense in Depth
  - Network Segmentation / Partitioning
    - Network Perimeter
    - DMZ
    - Bastion Host
    - Proxy
    - NAT / PAT
  - Firewalls
    - Types
      - Packet Filtering
      - Stateful Packet Filtering
      - Circuit Proxy
      - Application
  - Inspection
    - IDS
    - IPS
    - IDS/IPS Location
      - Host Based
      - Network Based
        - In-line
        - Mirror, Span, Promiscuous
    - IDS / IPS Detection Methods
      - Pattern
        - Signature analysis
        - Stateful matching
      - Anomaly
        - Statistical
        - Protocol
        - Traffic
      - White & Black Lists
      - Sandbox
    - Honeypots & honeynets
    - Ingress vs. Egress
- Endpoint Security

Remote Access





Domain 5

Identity and Access Management

Access Control

Access Controls Services

Access Control Principles

- Separation of Duties
- Need to Know
- Least Privilege

Administration Approaches

- Centralized
- Decentralized
- Hybrid

Authentication

- Identification
- Authorization
- Accountability

Authorization

- Discretionary
  - Non-discretionary
  - Mandatory
  - Principle of Access Control
- Just-in-time Access

Identification

- Knowledge
  - Password
  - Passphrase
  - Questions
- Ownership
  - Smart / Memory Cards
  - One-time Passwords
    - Hard Tokens
    - Soft Tokens
    - Synchronous
    - Asynchronous
- Characteristic
  - Physiological
    - Fingerprint
    - Hand Geometry
    - Vascular Pattern
    - Facial
    - Iris
    - Retina
    - Voice
  - Behavioural
    - Signature
    - Key Stroke
    - Gait
  - Templates
  - Type 1: False Reject
  - Type 2: False Accept
  - Crossover Error Rate
- Single / Multifactor
- Authenticator Assurance Levels (AAL)

Types of RBAC

- Rule
- Role
- Attribute / Content

Session Management

Session Hijacking

Single Sign-on / Federated Access

Allows users to access multiple systems with a single set of credentials

Single Sign-on

Access systems **within the same organization**

Federated Identity Management (FIM)

Access systems across **multiple entities**

Kerberos

- Components
  - User / Client
  - Key Distribution Center
  - Authentication Service
  - Ticket Granting Ticket (TGT)
  - Ticket Granting Service
  - Service Tickets
  - Service
- Symmetric encryption only

Sesame

- Symmetric & Asymmetric encryption

Trust Relationship

- Principal / User
- Identity Provider
- Relying Party / Service Provider

SAML

- Tokens
- Assertions written in XML
- Components
  - Profiles
  - Bindings
  - Protocol
  - Assertion

WS-Federation

OpenID

OAuth

Domain 6

Security Assessment and Testing

Security Assessment and Testing

- Validation
- Verification
- Rigour

Testing a System

- Unit
- Interface
- Integration
- System

Testing Techniques

Methods & Tools

- Manual
- Automated
- Static
- Dynamic
- Fuzz

Runtime

- White
- Black
- Positive
- Negative
- Misuse

Access to Code

Techniques

- Decision table analysis
- State-based analysis
- Boundary Value Analysis
- Equivalence Partitioning

Efficiency

- Real User Monitoring
- Synthetic Performance Monitoring

Operational

- Regression Testing

Testers / Assessors

Internal

External

Third-Party

- SOC 1
- SOC 2
- SOC 3

Type 1

Type 2

Roles

- Executive Management
- Audit Committee
- Security Officer
- Compliance Manager
- Internal Auditors
- External Auditors

Metrics

Focus

KPIs

KRIs

Mutation

Generation

Identifying Vulnerabilities

- Vulnerability Assessment
- Penetration Testing

Process

- Reconnaissance
- Enumeration
- Vulnerability Analysis
- Execution
- Document Findings

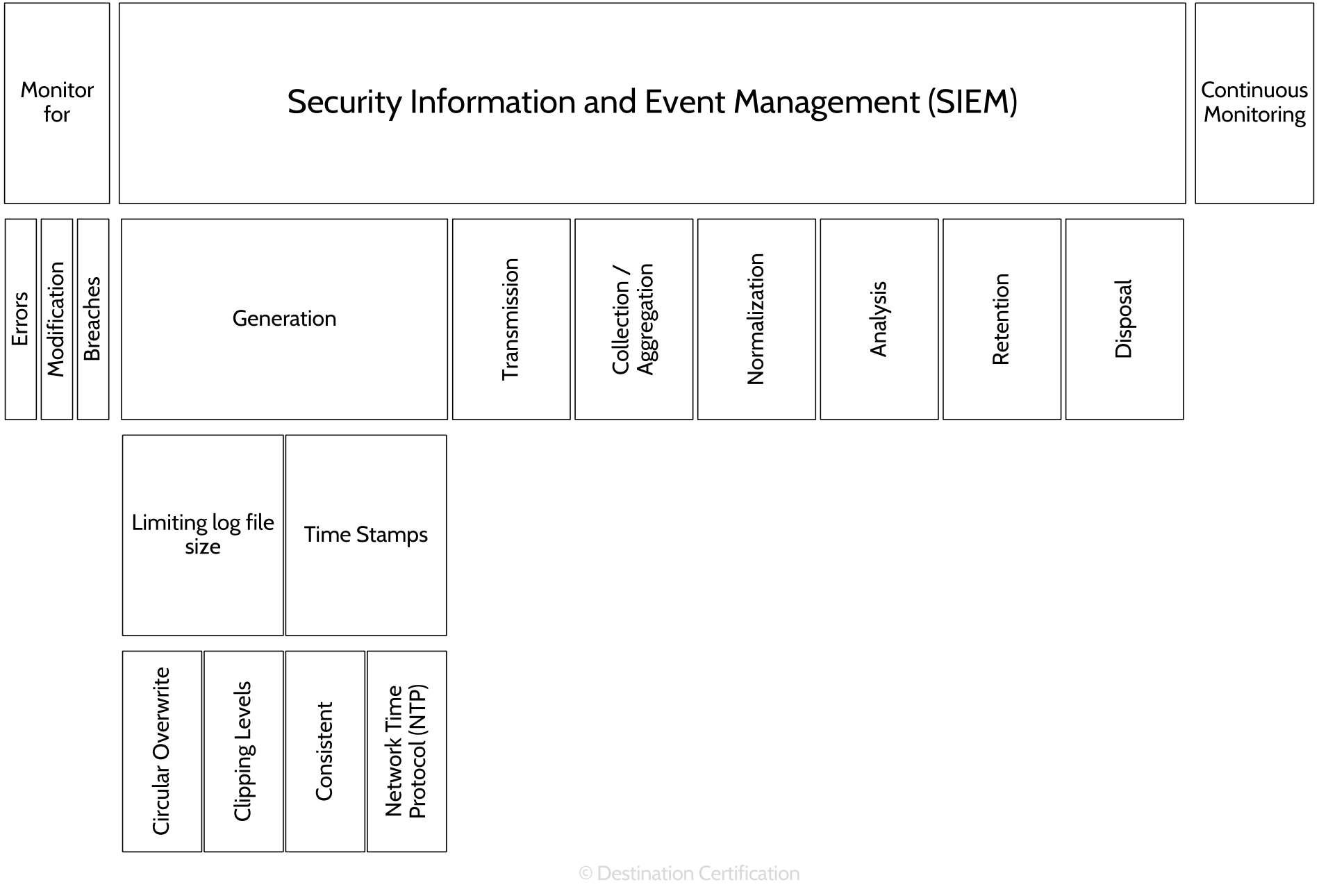
Testing Techniques

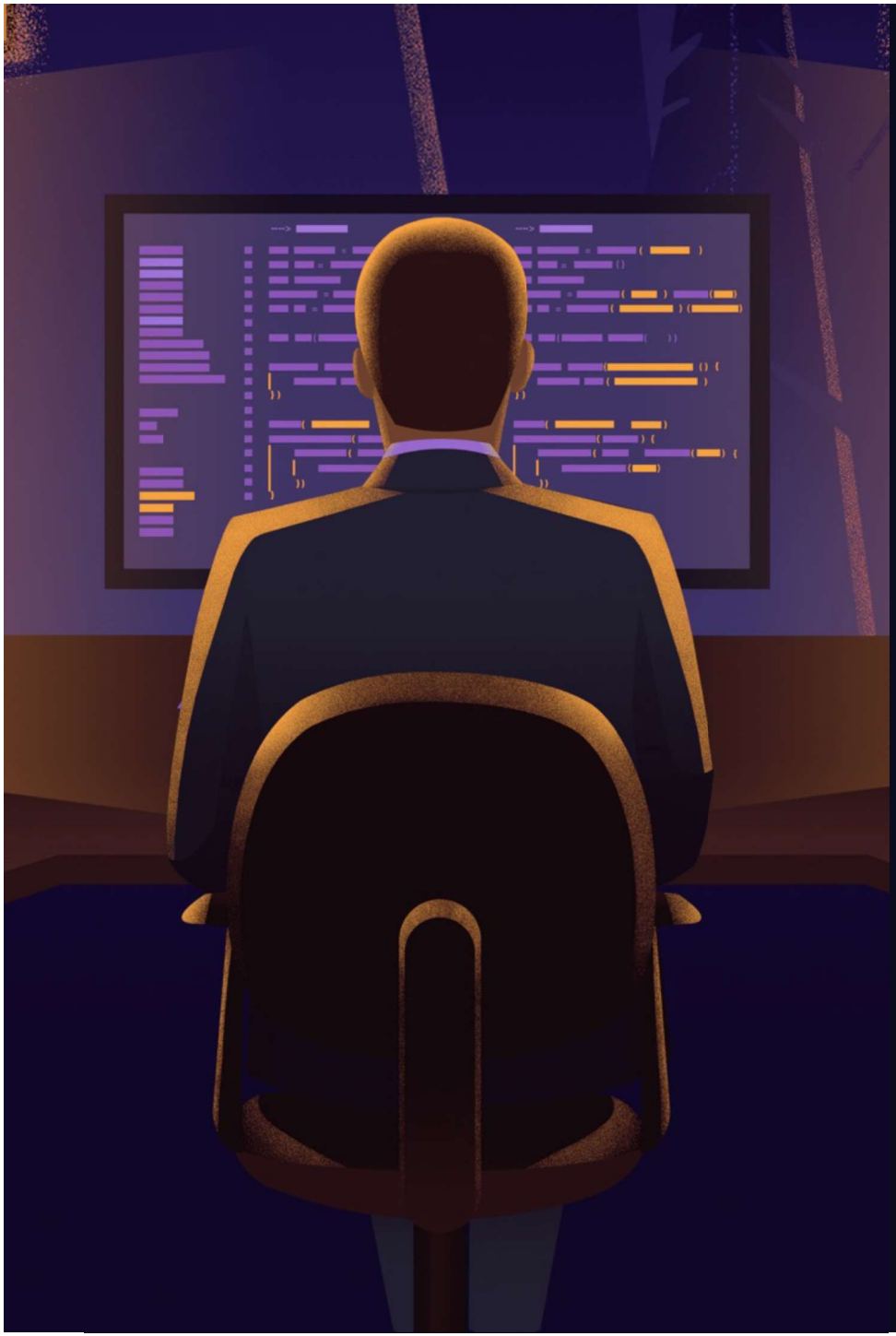
- Perspective
  - Internal
  - External
- Approach
  - Blind
  - Double-blind
- Knowledge
  - Zero (black)
  - Partial (gray)
  - Full (white)

Types of Scans

- Credentialed / Authenticated
- Uncredentialed / Unauthenticated
- Banner grabbing & Fingerprinting
- **CVE**
- **CVSS**
- Interpreting & understanding results
- SCAP
- False positive vs. False negative

Log Review & Analysis





Domain 7

Security Operations

Investigations

Secure the Scene

Collect & Control Evidence

Locard's Principle

MOM

Sources

- Oral / Written statements
- Documents
- Digital Forensics
  - Live Evidence (Volatile)
  - Secondary Storage (HD)
  - VM Instance / Virtual Disk
- E Discovery

Chain of Custody

Types of Evidence

- Real Evidence
- Direct Evidence
- Secondary Evidence
- Best Evidence Rule

Rules of Evidence

- Authentic
- Accurate
- Complete
- Convincing / Admissible

Investigative Techniques

- Media Analysis
- Software Analysis
- Network Analysis

Types of Investigations

- Criminal
- Civil
- Regulatory
- Administrative

Document & Report

Incident Response

Prep.	Triage		Action / Investigation		Recovery		
	Detection	**Response** IR Team Deployed	**Mitigation** Containment	**Reporting** Relevant Stakeholders	**Recovery** Return to normal	**Remediation** Prevention	**Lessons Learned** Improve Process
	Sources: SIEM, IDS/IPS DLP, Fire detectors Etc.	Event	Incident				

Malware

Types of Malware

- Virus
- Worm
- Companion
- Macro
- Multipartite
- Polymorphic
- Trojan
- Botnets
- Boot Sector
- Hoaxes / Pranks
- Logic Bombs
- Stealth
- Ransomware
- Rootkit
- Spyware / Adware
- Data Diddler / Salami Attack

Zero Day

Anti-Malware

- Continuous Updates

Detection

- Change Detection
- Activity Monitors
- Heuristic Scanners
- Signature Based Scanners

Prevention

- Network Segmentation
- Allow List

Policy

- Training & Awareness

Patching

Determine if Patch is available					**Implement through Change Management**		
Threat Intelligence	Vendor Notification	Pro-actively checking			Timing	Deploy	
		Agent	Agentless	Passive		Automated	Manual

Change Management

Change Request	Assess Impact	Approval		Build & Test	Notification	Implement	Validation		Version & Baseline
	Emergency Change vs. Standard process	Based on impact, severity, etc.	CCB CAB ECAB				Test New Functionality	Regression Testing	

Recovery Strategies

Backup Storage

- Types of Backups
  - Archive Bit
  - Mirror
  - Full
  - Incremental
  - Differential
- Validation
  - Checksums / CRC
- Data Storage
  - Offsite
  - Tape Rotation
- RPO
- Cold
- Warm
- Hot

Spare Parts

RAID
Redundant Array of Independent Disks

- **RAID 0**
  Striping
- **RAID 1**
  Mirroring
- **RAID 5**
  Parity
- **RAID 6**
  Double Parity

High Availability System

- Clustering
- Redundancy

Recovery Sites

- Types of Sites
  - Geographically remote
  - Mirror / Redundant
  - Mobile
  - Hot
  - Warm
  - Cold

Business Continuity Management (BCM)

Focuses on critical and essential functions of business

Goals of BCM

1. Safety of people
2. Minimize damage
3. Survival of business

Business Impact Assessment

- Identify Critical Processes & Systems
- Measurements of Time
  - RPO
  - RTO
  - WRT
  - MTD
- Owner approval of #s and associated costs

Types of Plans

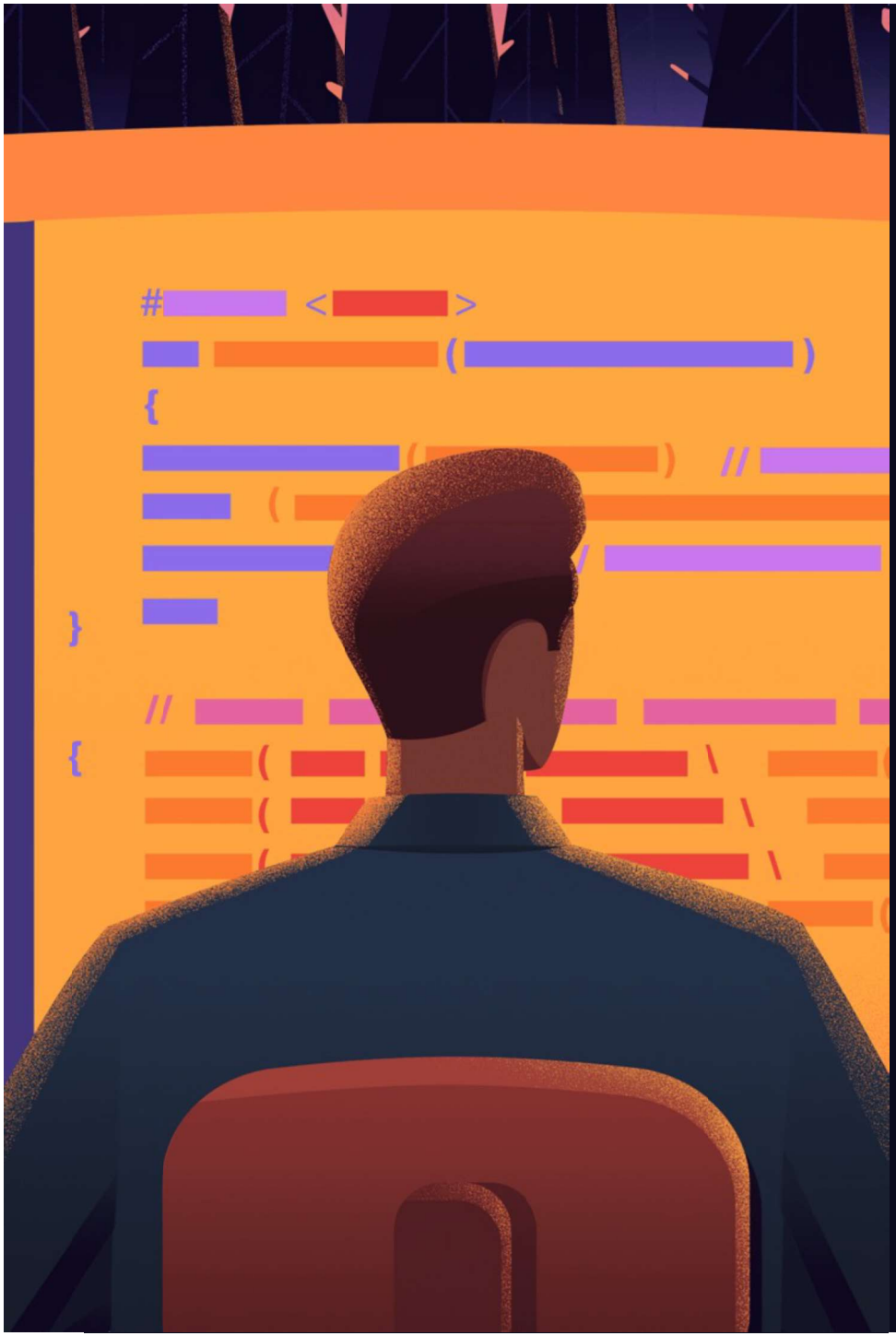
- Business Continuity Plan (**BCP**)
- Disaster Recovery Plan (**DRP**)

Testing Plans

- Read-through / Checklist
- Walkthrough
- Simulation
- Parallel
- Full-interruption / Full-scale

Restoration order

- Most critical first
- Dependency charts



Domain 8

Software Development Security

Secure Software Development

- Bake In Security
- System Life Cycle (SLC)
  - Software Development Life Cycle (SDLC)
    - Plan + Mgmt. Approval
    - Requirements
    - Architecture & Design
    - Development
    - Testing
    - Deployment
    - Operation
    - Disposal
  - Maturity Models
  - APIs
    - REST
    - SOAP
  - Obfuscation
    - Lexical, Data, Control flow
  - Acquire Software
    - Assess vendors
    - Contracts, / SLAs
  - Software Security Weaknesses & Vulnerabilities
    - Buffer Overflows
    - SQL Injection
    - XSS / CSRF
    - Covert Channels
    - Backdoors / Trapdoors
    - Memory / Object Reuse
    - TOCTOU
    - Citizen Developers
  - Secure Programming
    - Input Validation
    - Session Management
    - Polyinstantiation
  - Maintain Software
    - SCM
    - SOAR

- Waterfall
- Agile
- DevOps
- Canary
- Certification
- Accreditation

- Cannot go back
- Sprints
- Scrum Master
- Combine Dev, QA & Ops
- SecDevOps

Databases

- **Components**
  - Hardware
  - **Software**
    - Language (SQL)
    - Users
    - Data
- **Maintaining Integrity of Data**
  - Concurrency
  - Locks
  - A — Atomicity
  - C — Consistency
  - I — Isolation
  - D — Durability
- SQL Injection

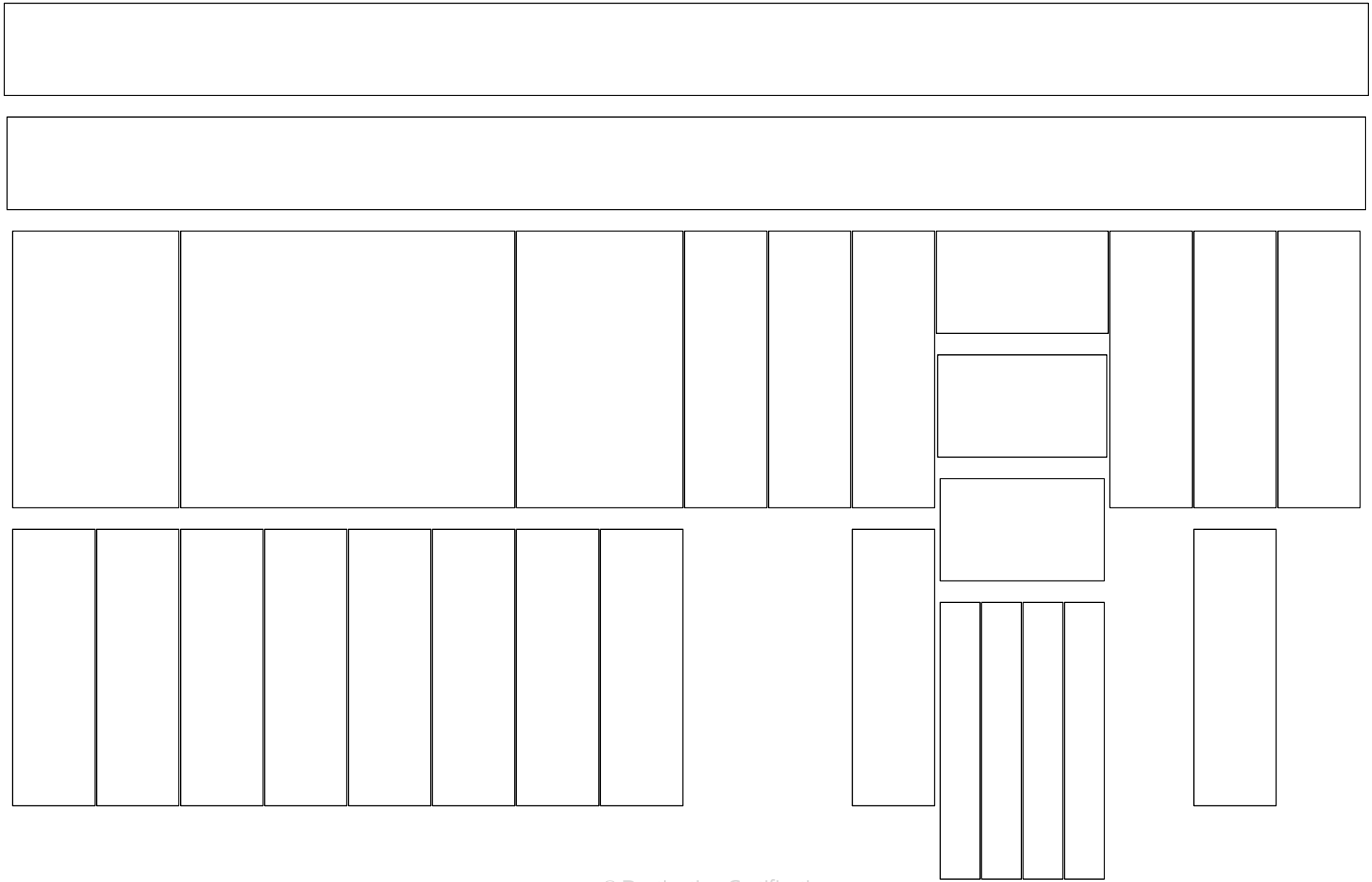
- **Database**
- **Tables**
  - Rows = Tuples / Records
  - Columns = Attributes
  - Fields
  - Primary & Foreign Keys

Printable Blank MindMaps

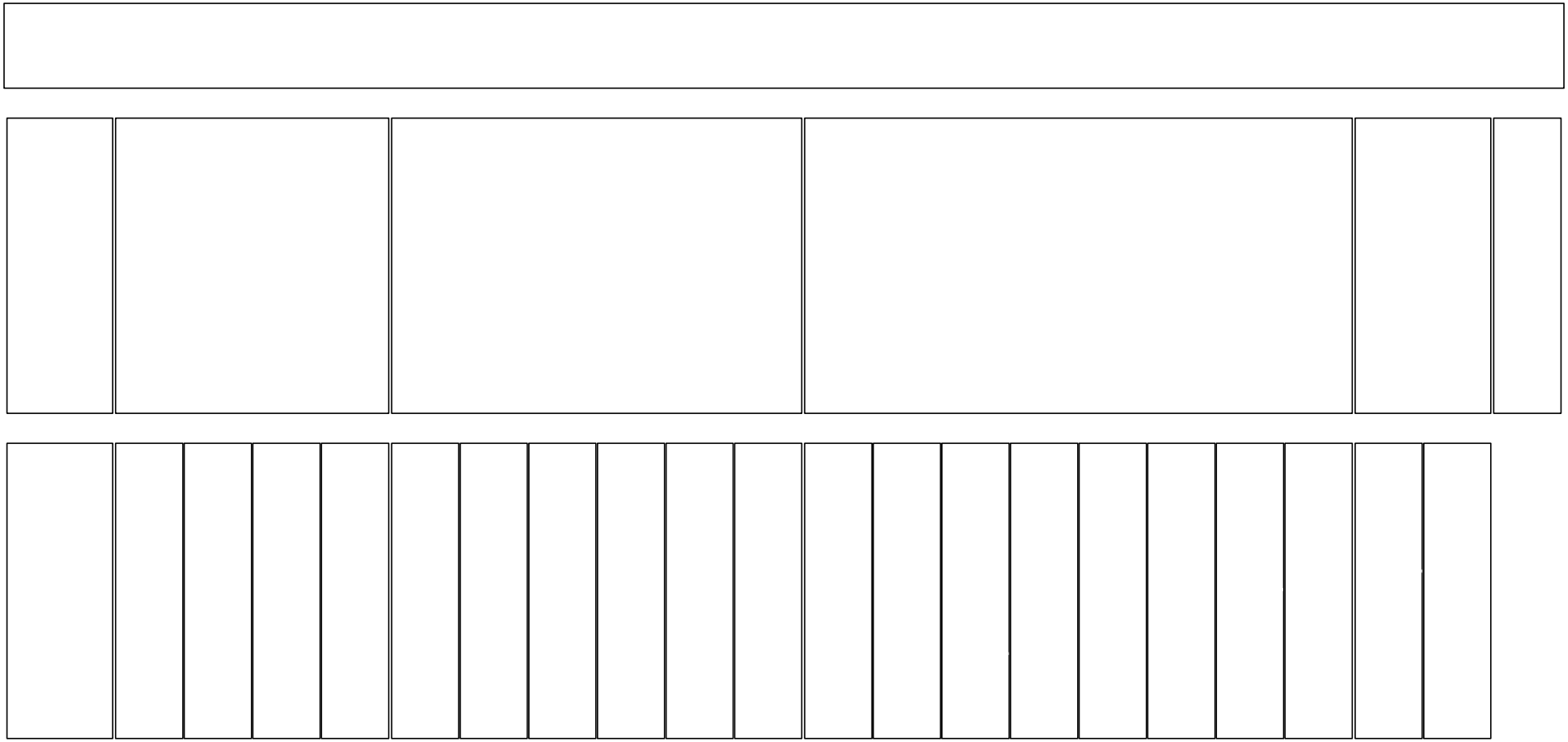
Print out the following blank MindMaps and fill them in as your watch our MindMap videos!

Print pages 41 to 70

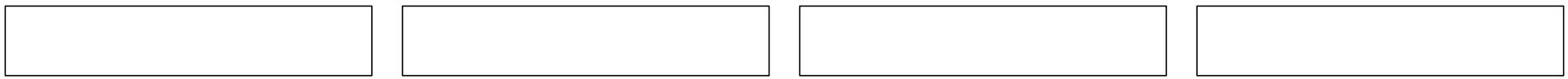
Alignment of Security Function to Business Strategy



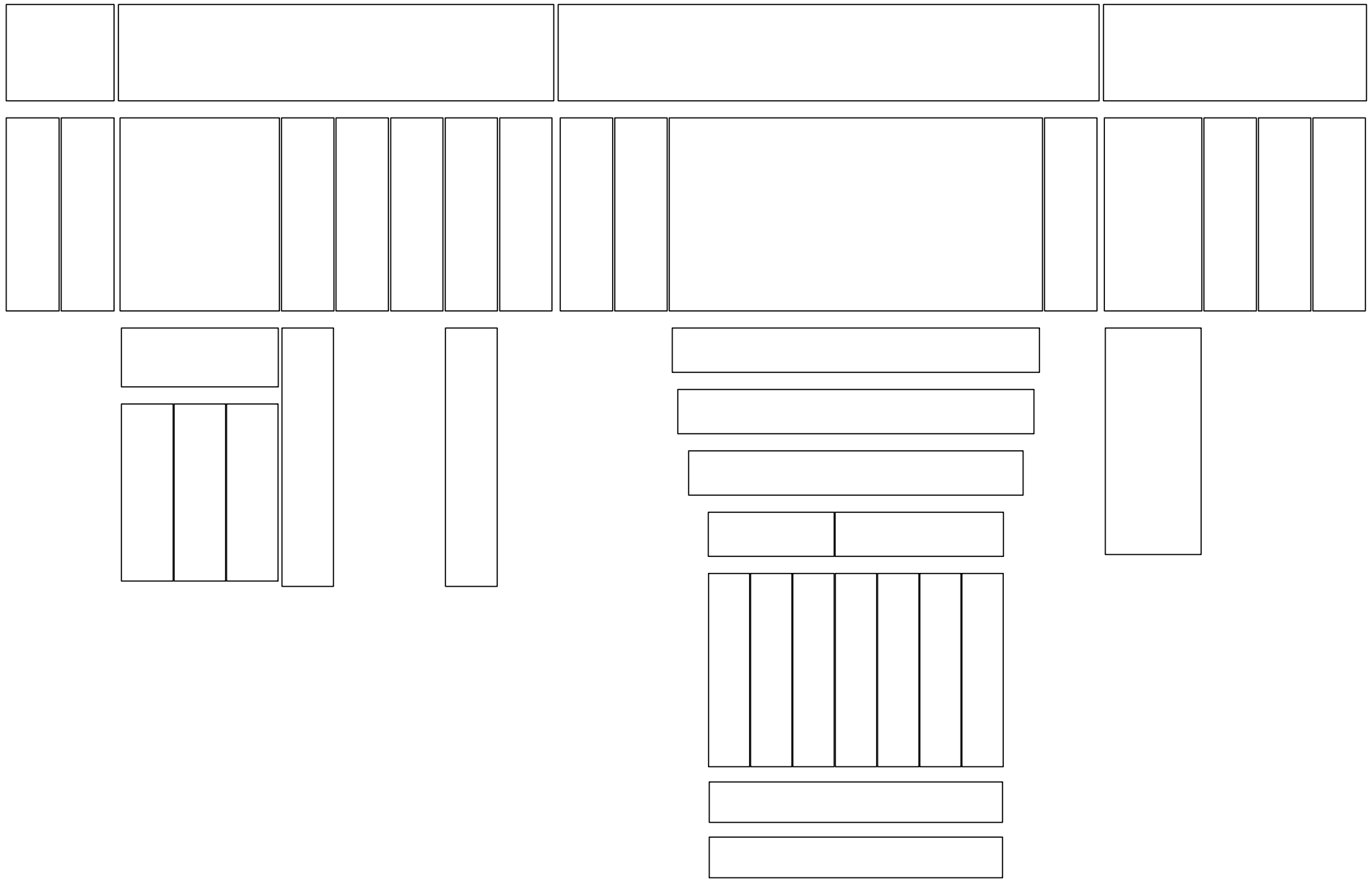
Privacy



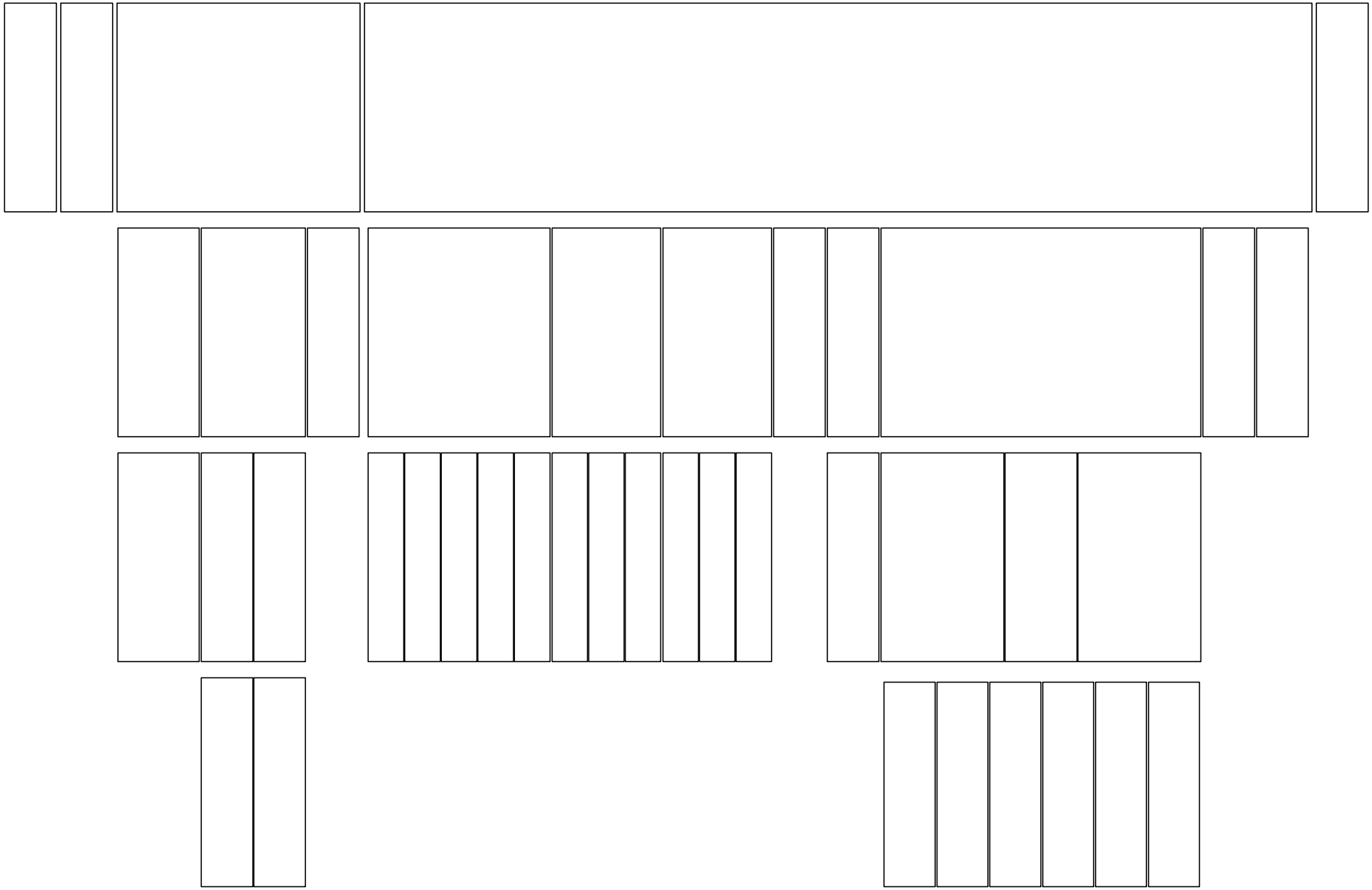
Intellectual Property



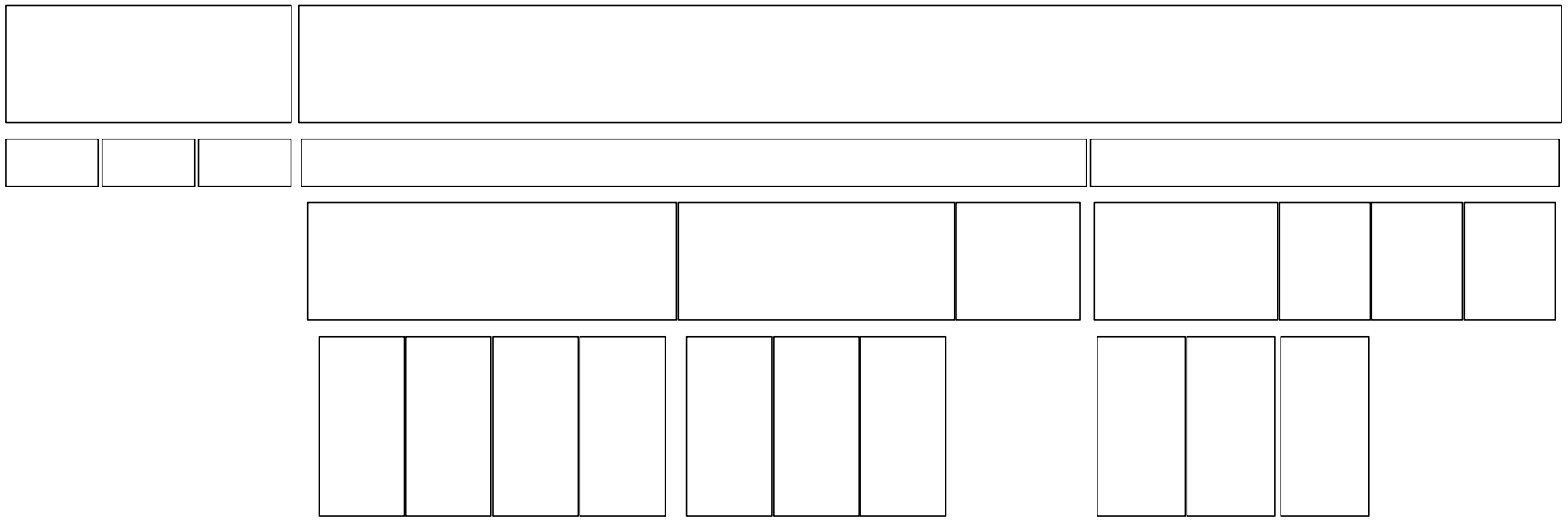
Risk Management



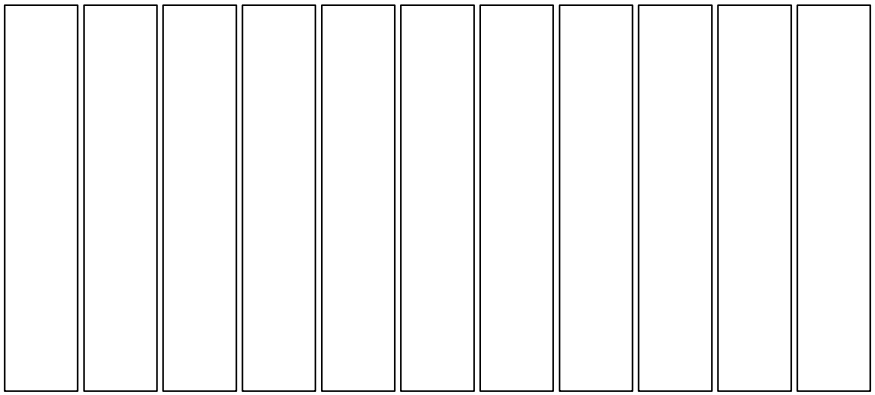
Asset Classification



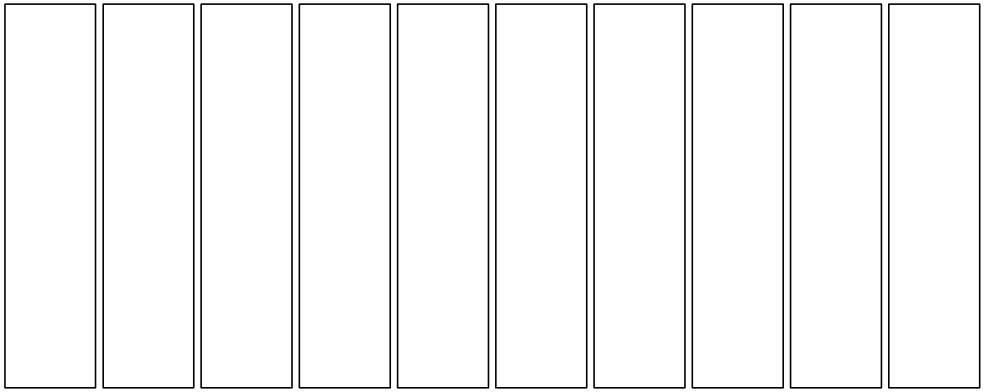
Models



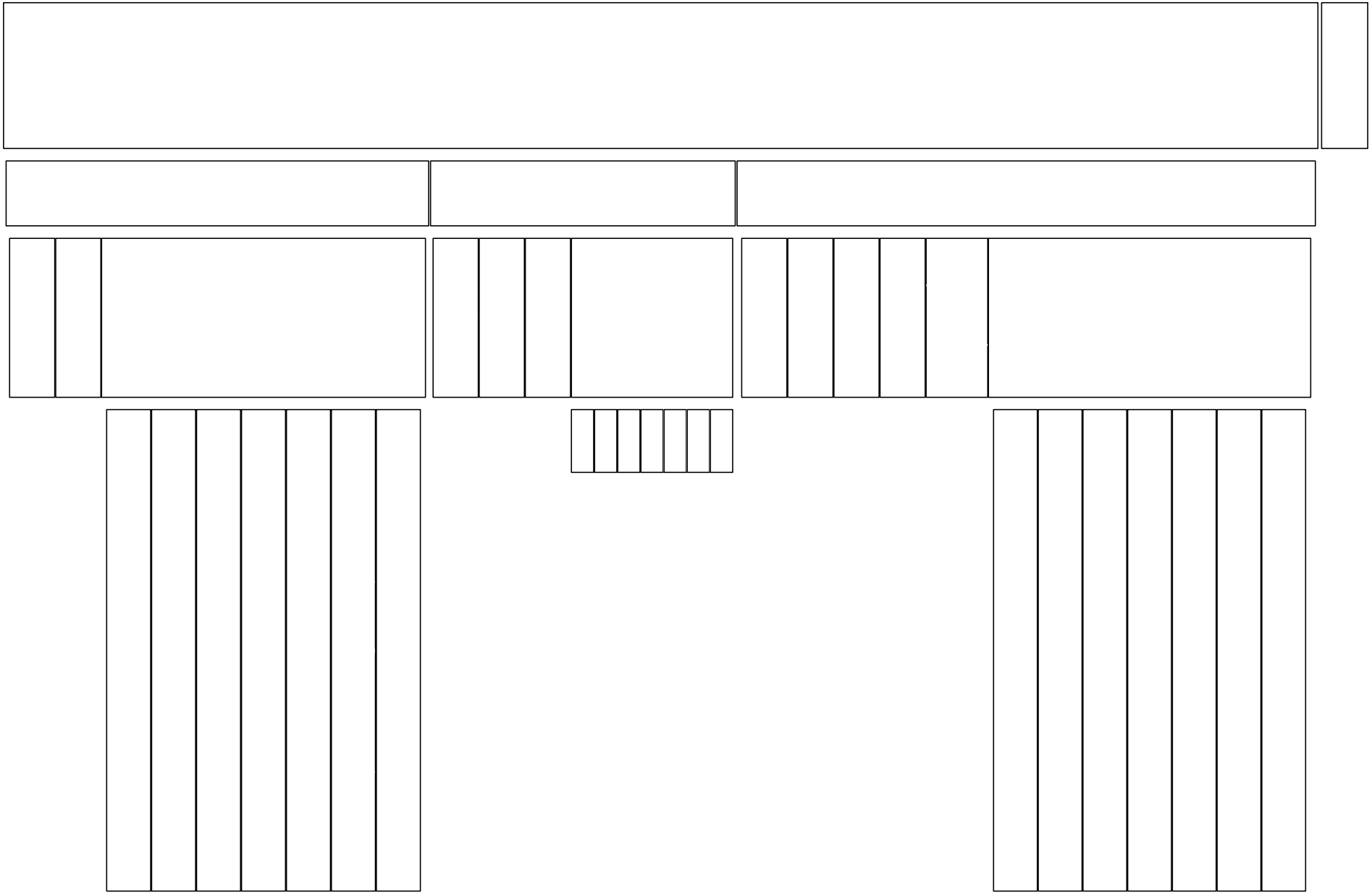
Secure Design Principles



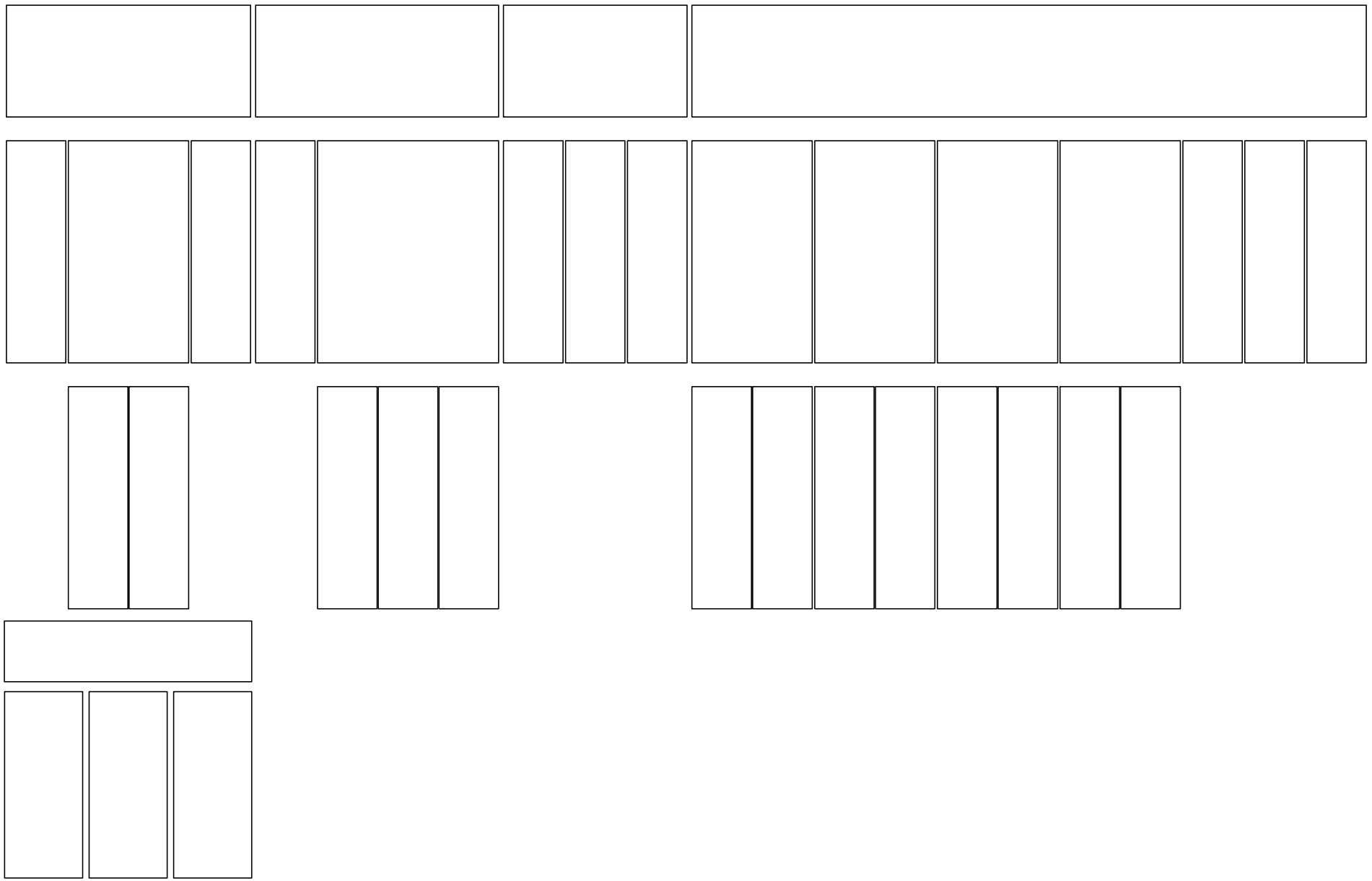
Security Frameworks



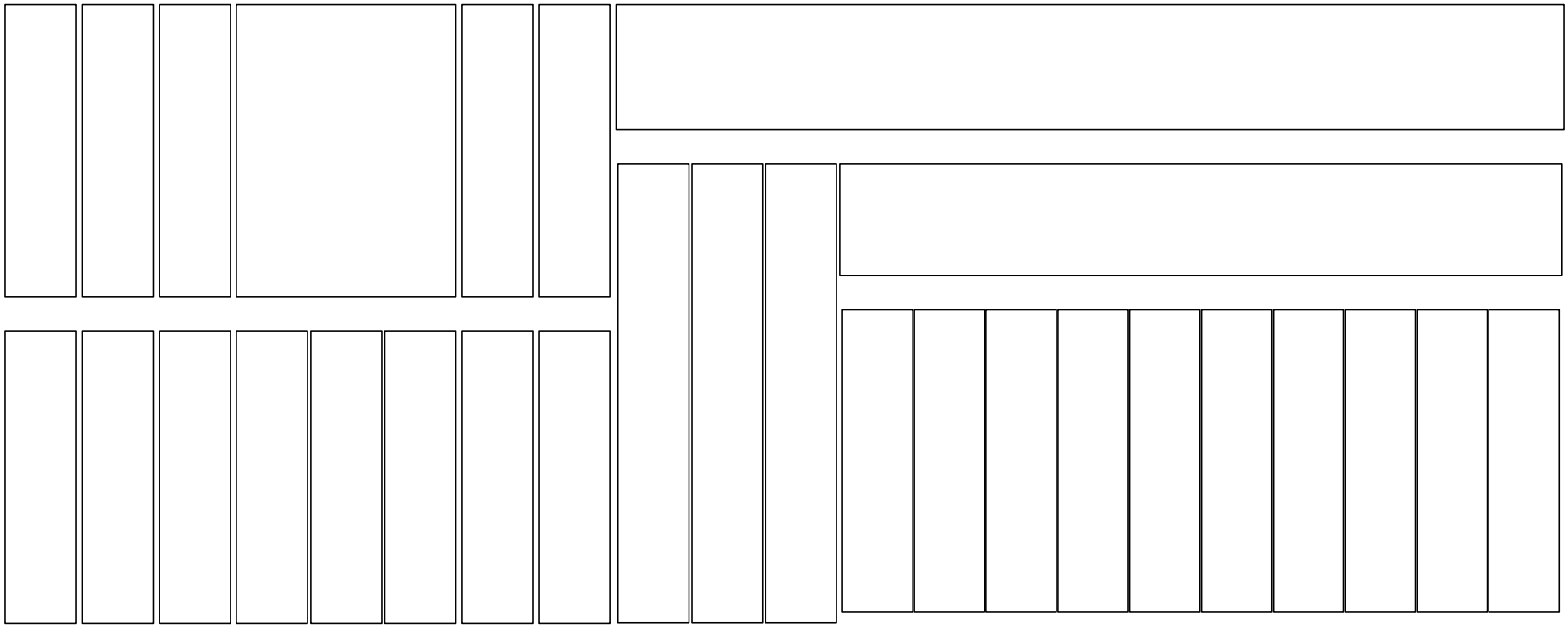
Evaluation Criteria



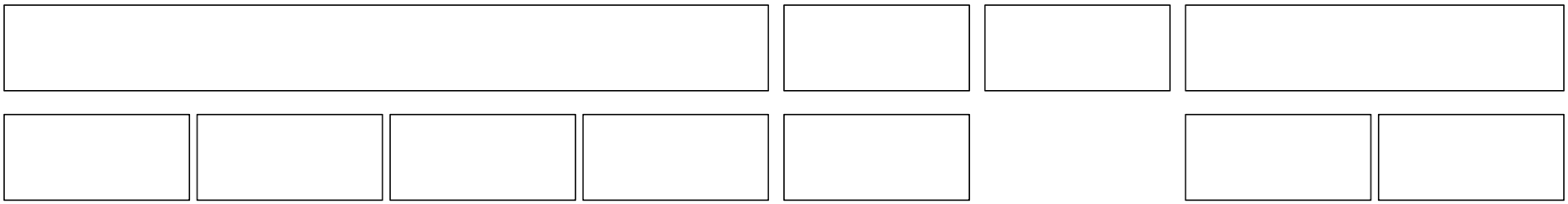
Trusted Computing Base (TCB)



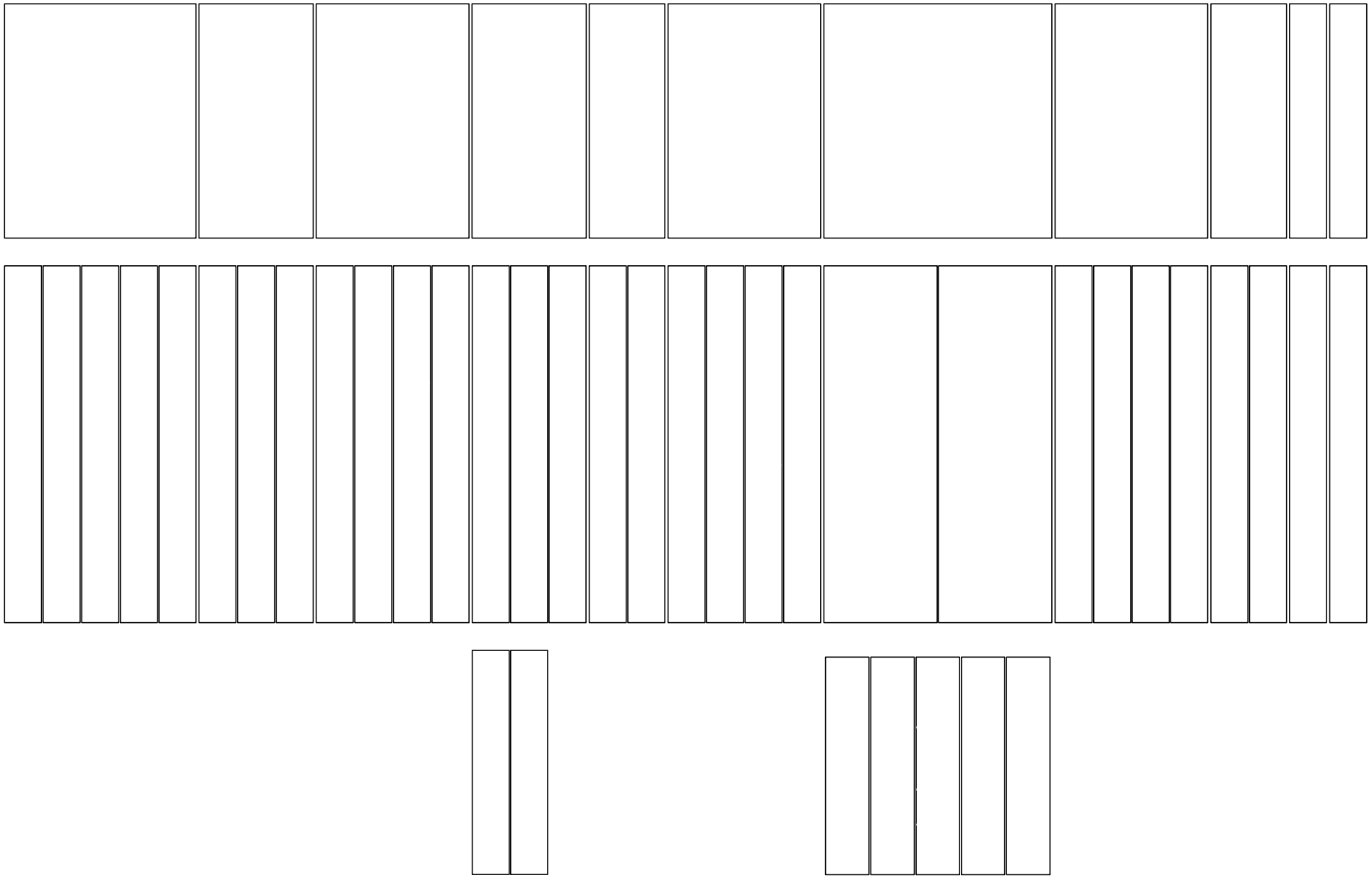
Vulnerabilities in Systems



Web-based Vulnerabilities



Cloud Computing



Cryptographic Services

Cryptographic terminology

Secret Writing

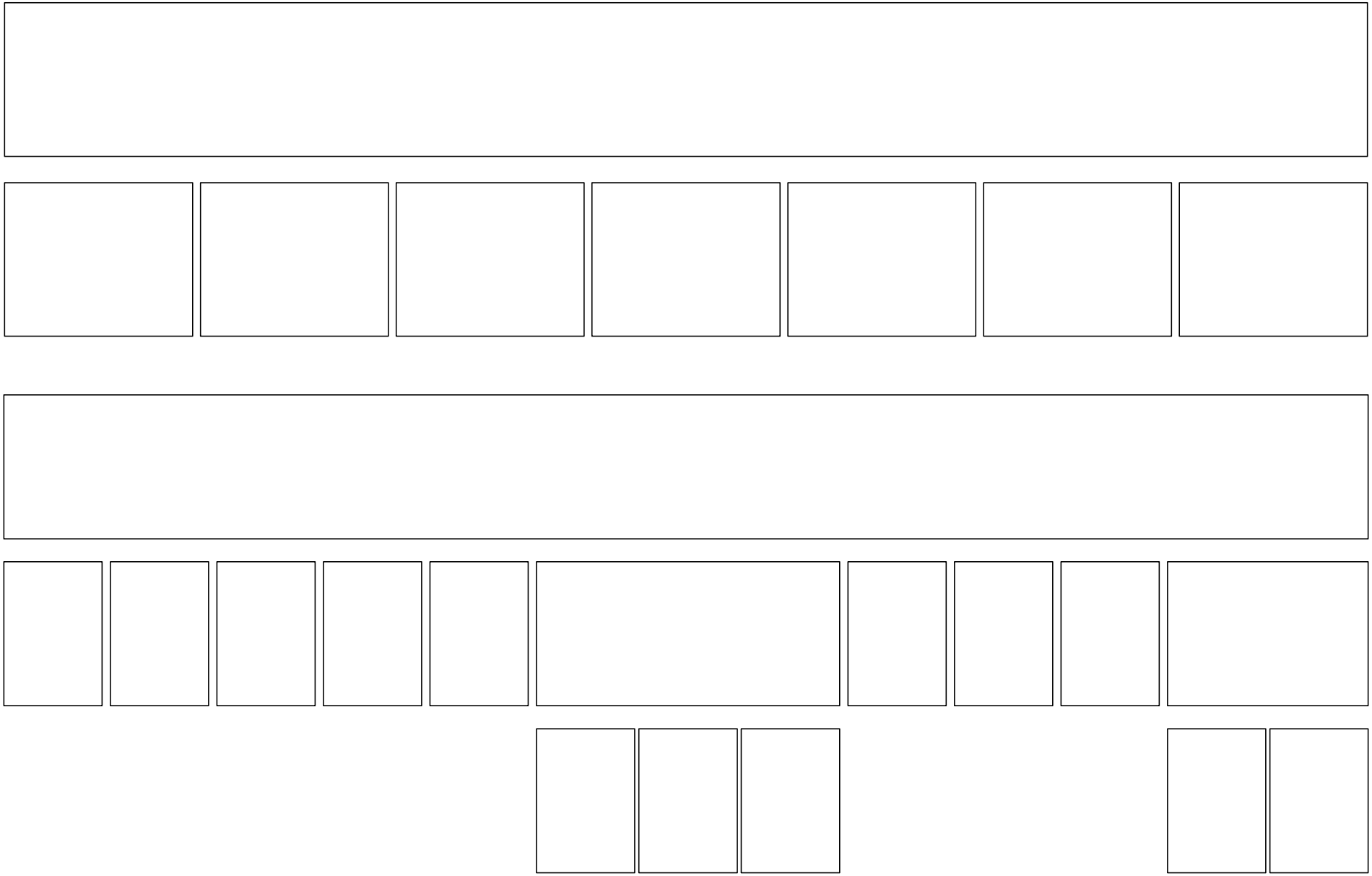
Digital Signatures

Digital Certificates

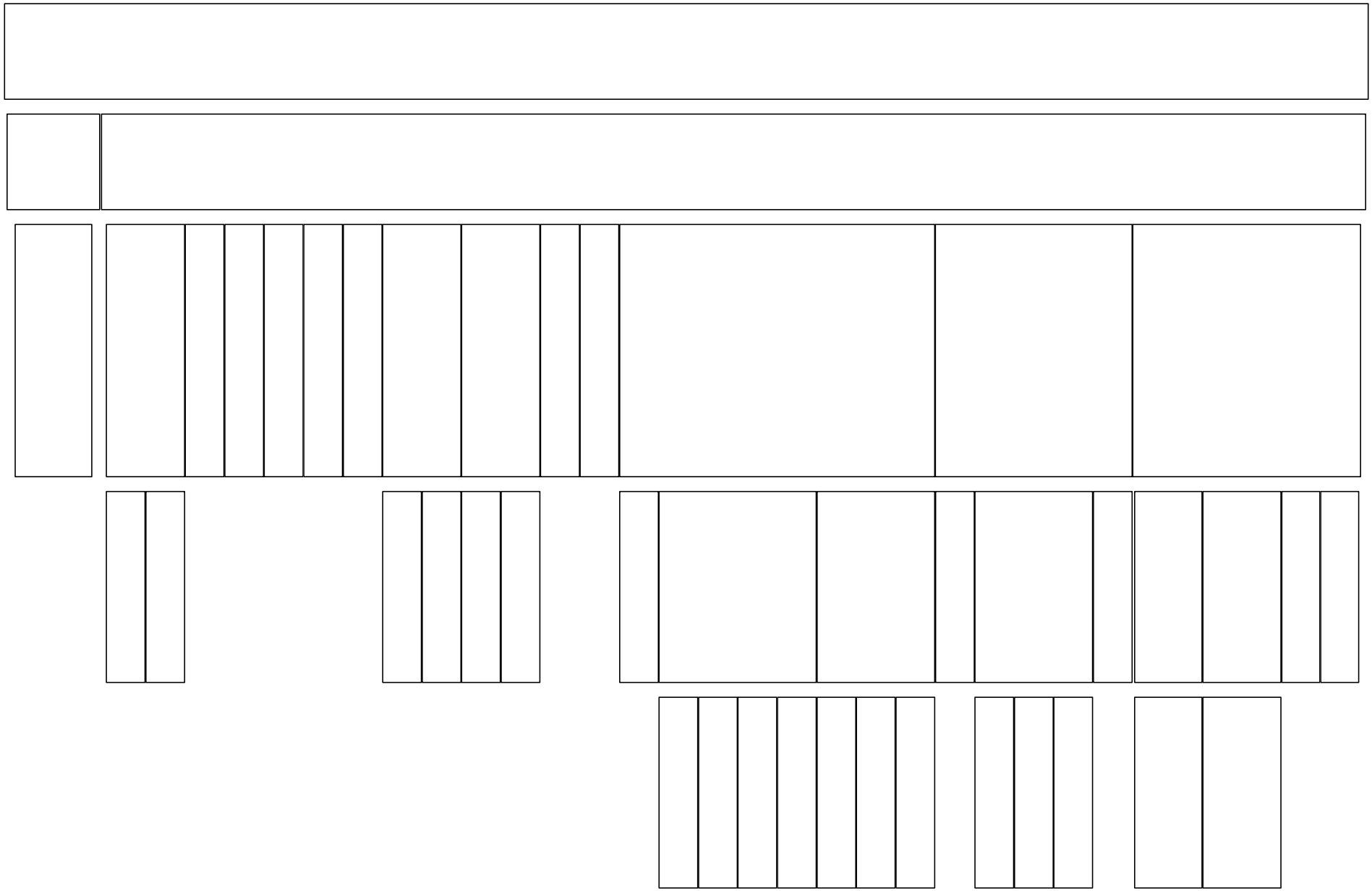
PKI

Key Management

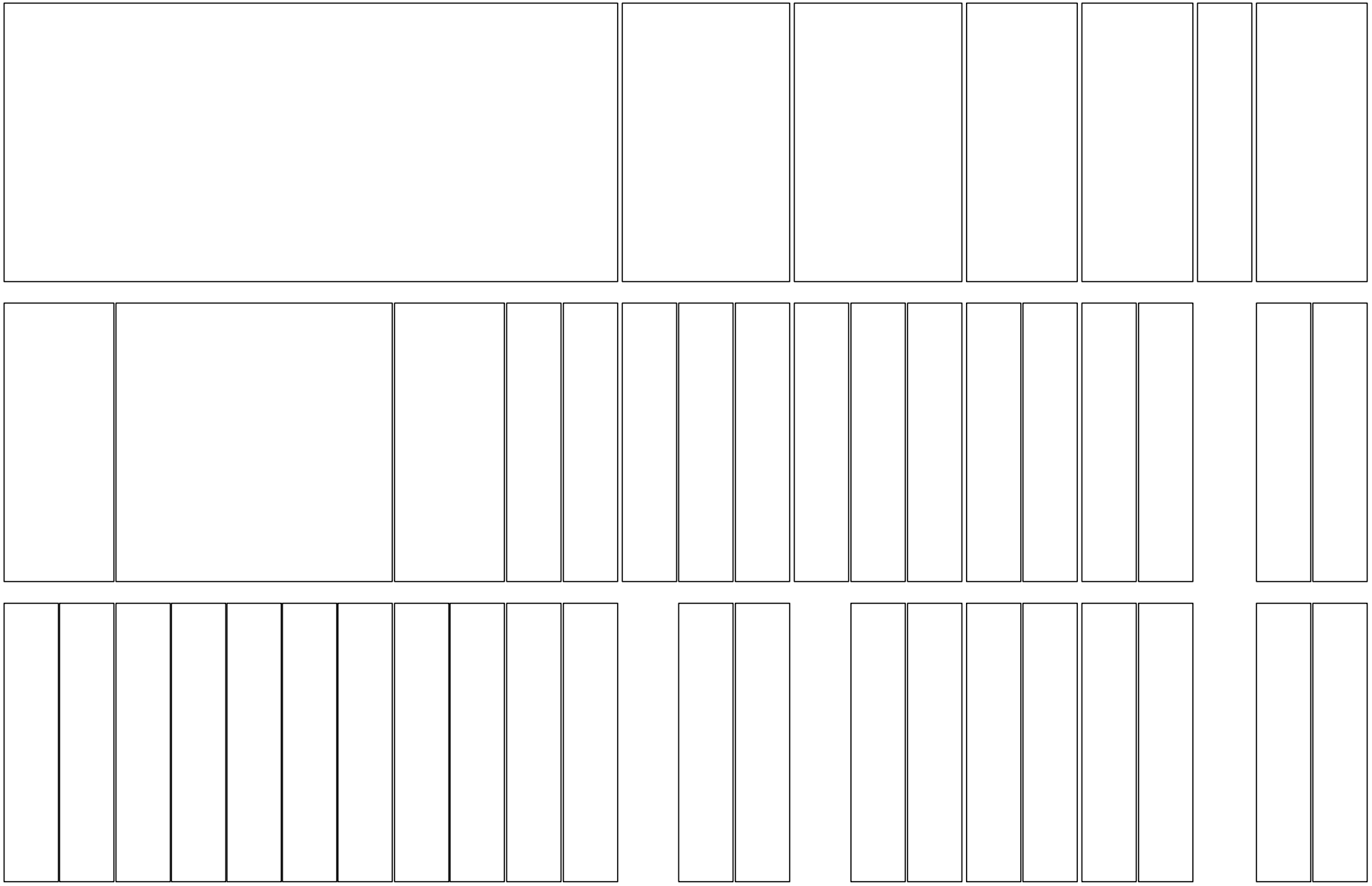
Cryptanalysis



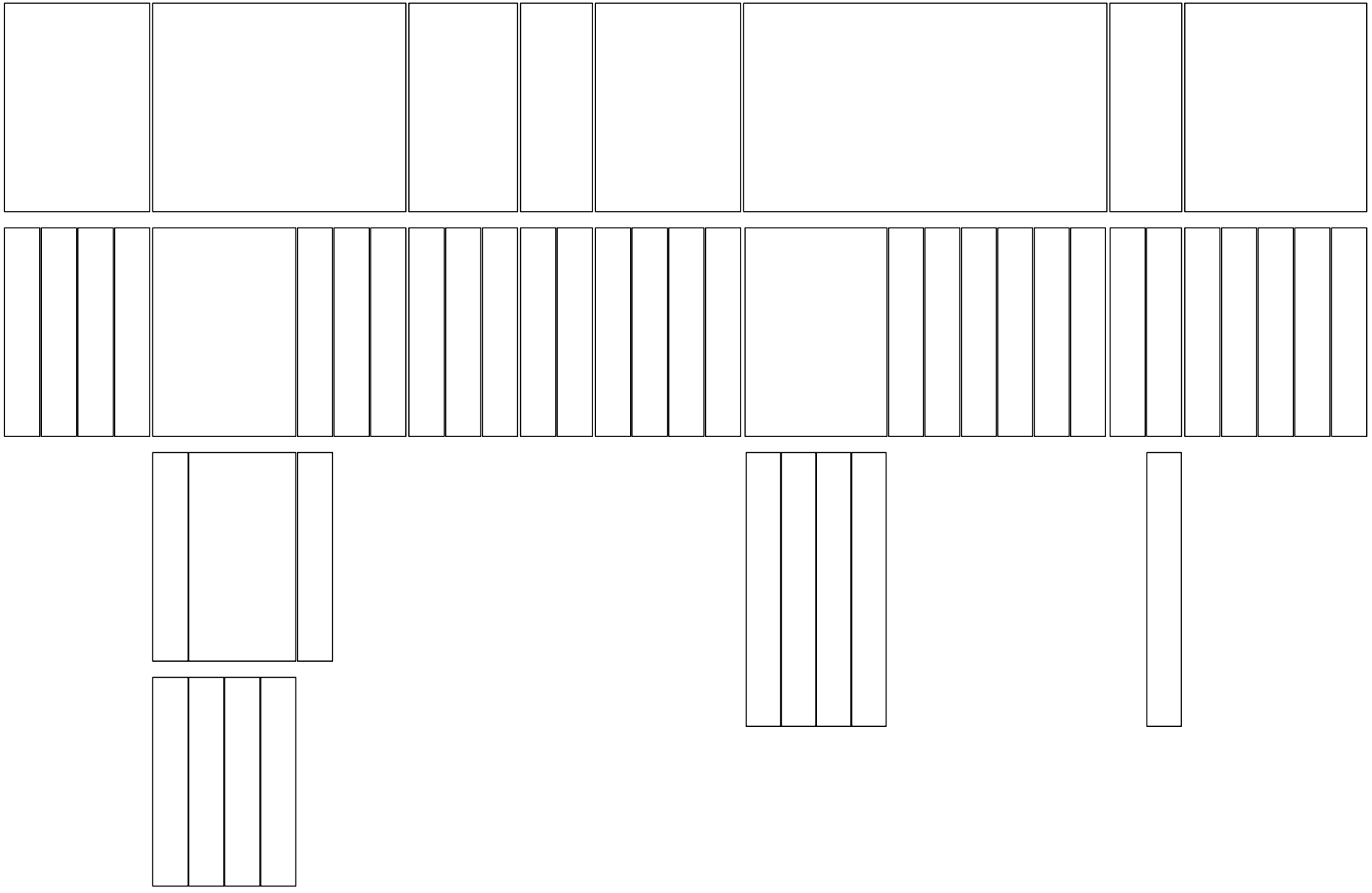
Physical Security



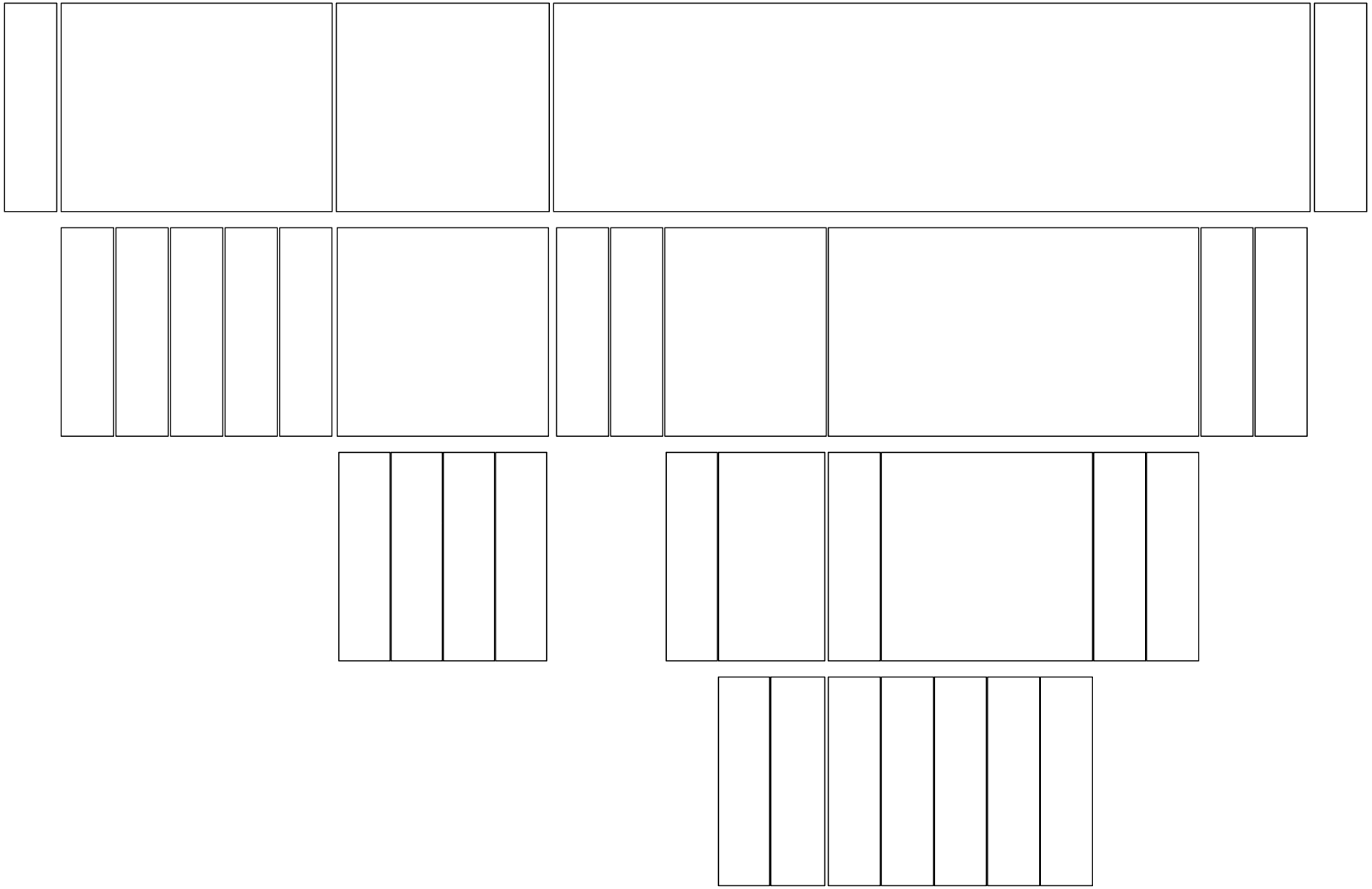
Open Systems Interconnection (OSI) Model



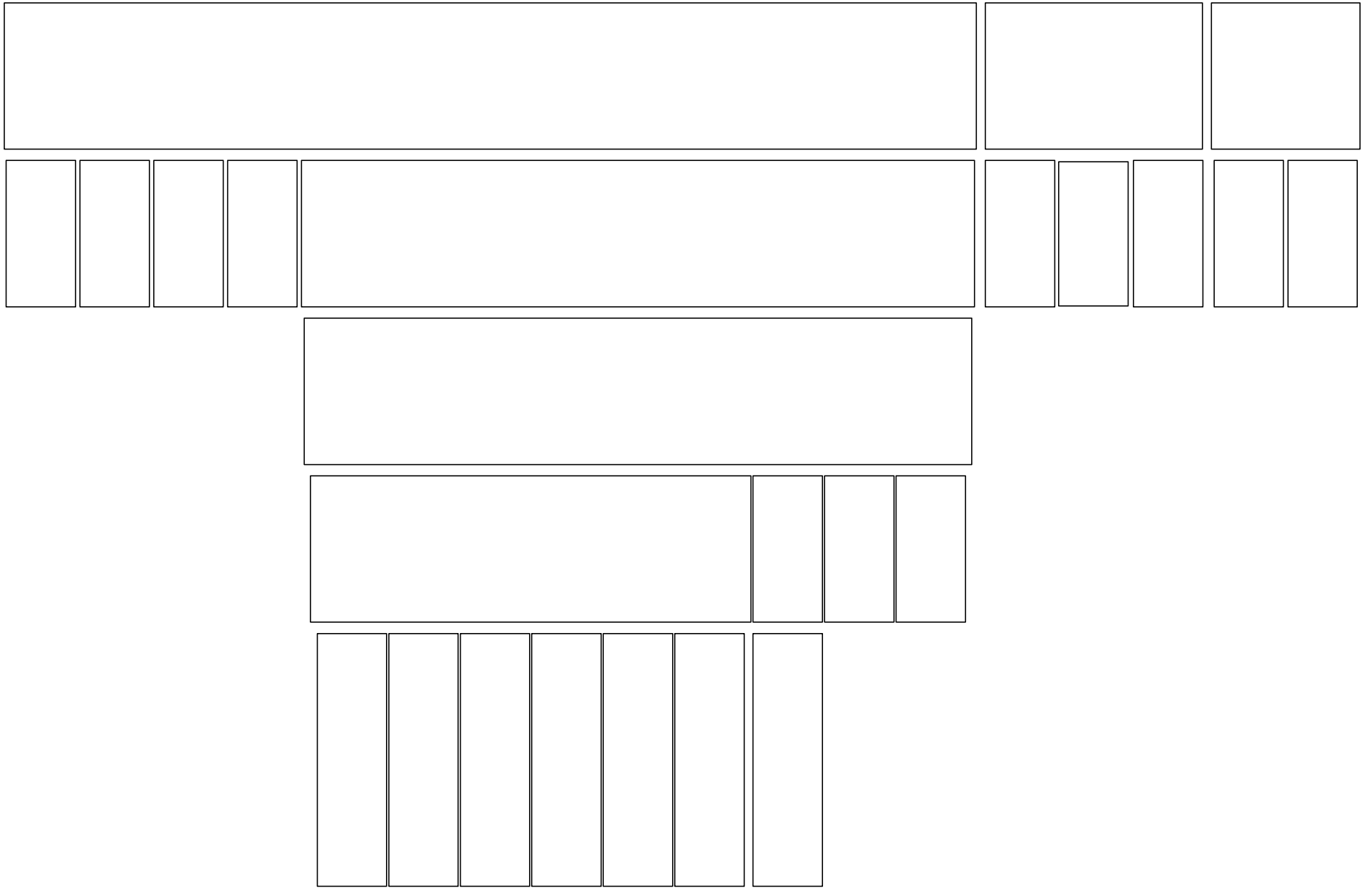
Networking



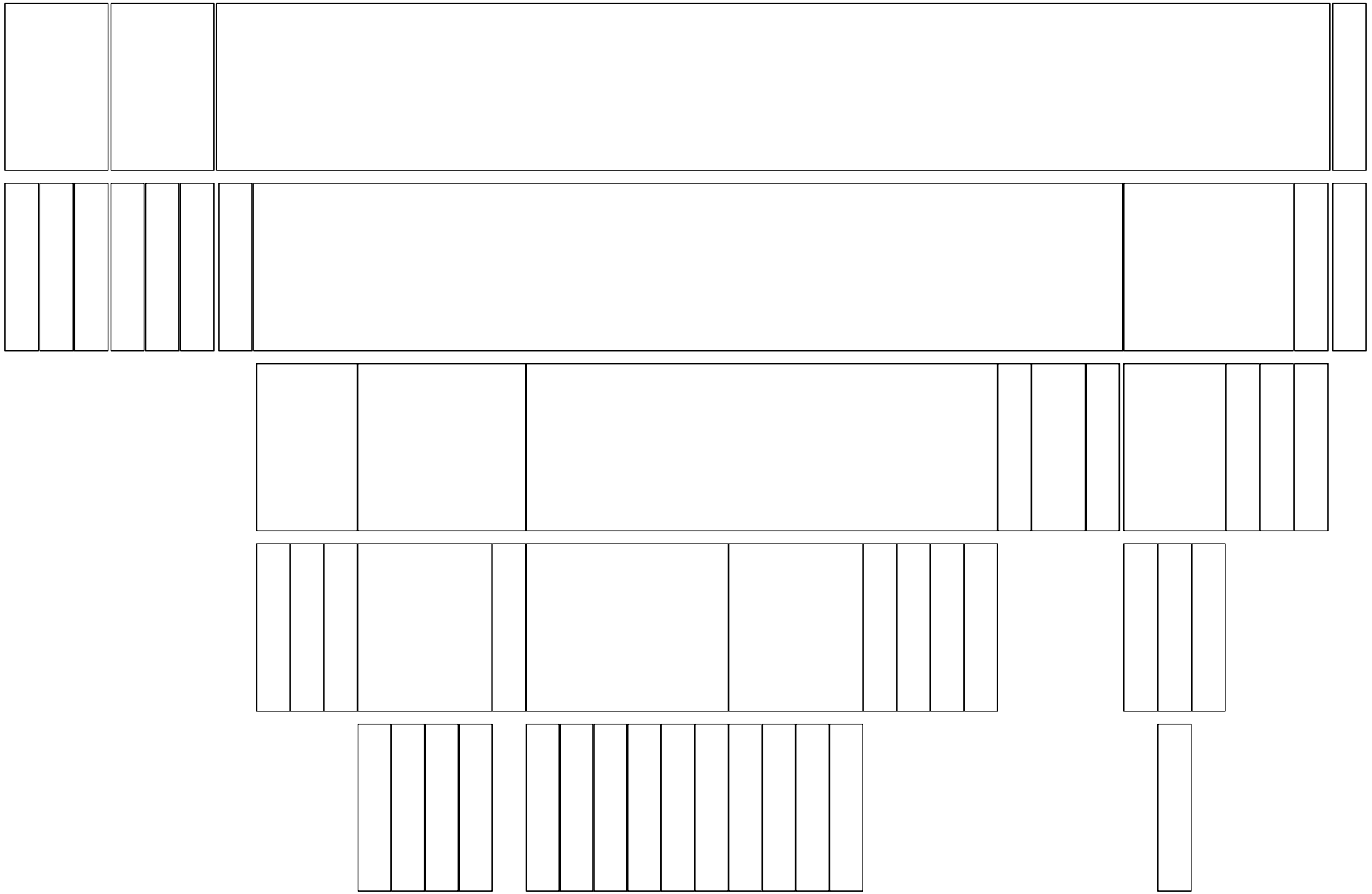
Network Defense



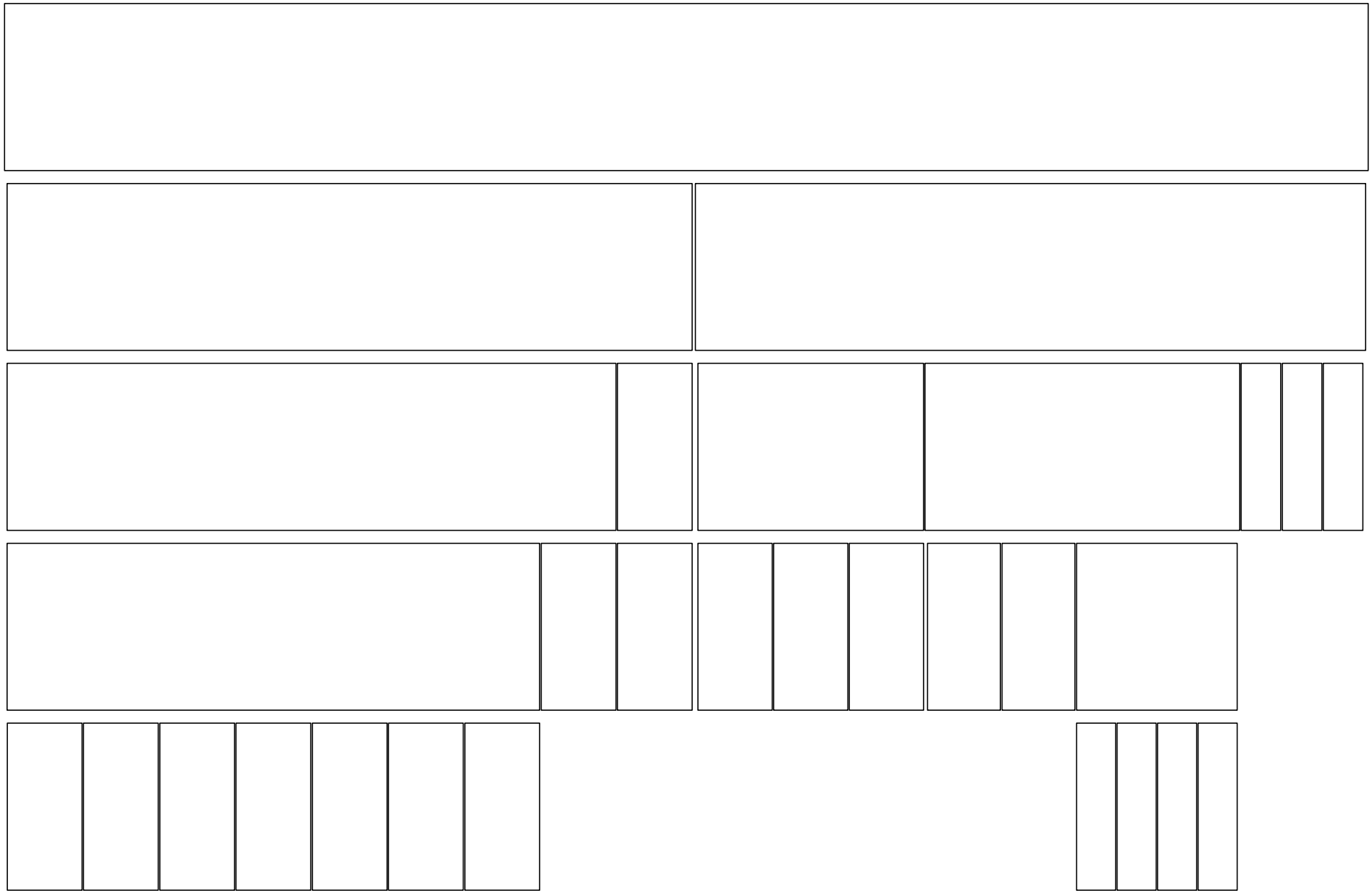
Remote Access



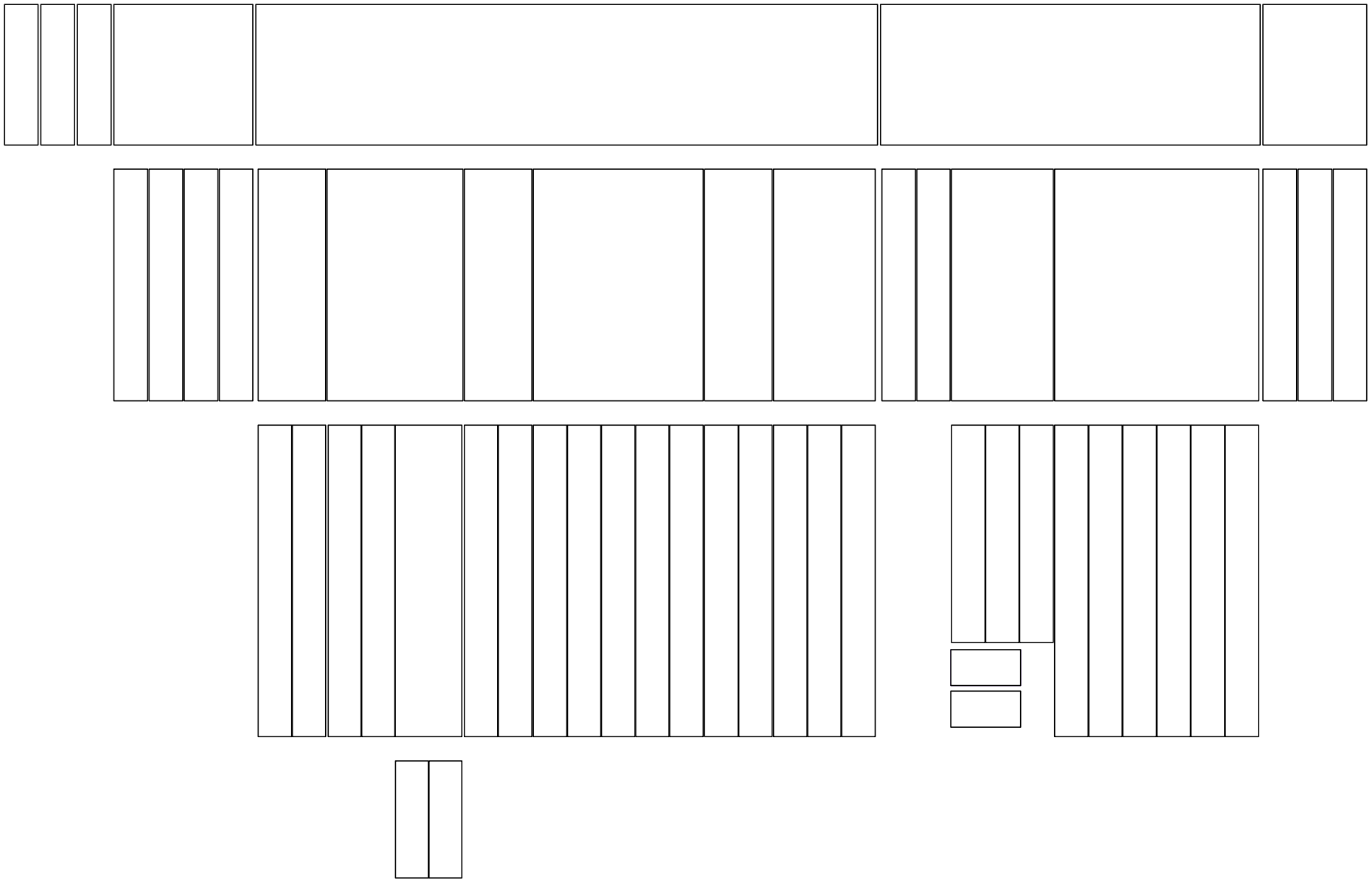
Access Control



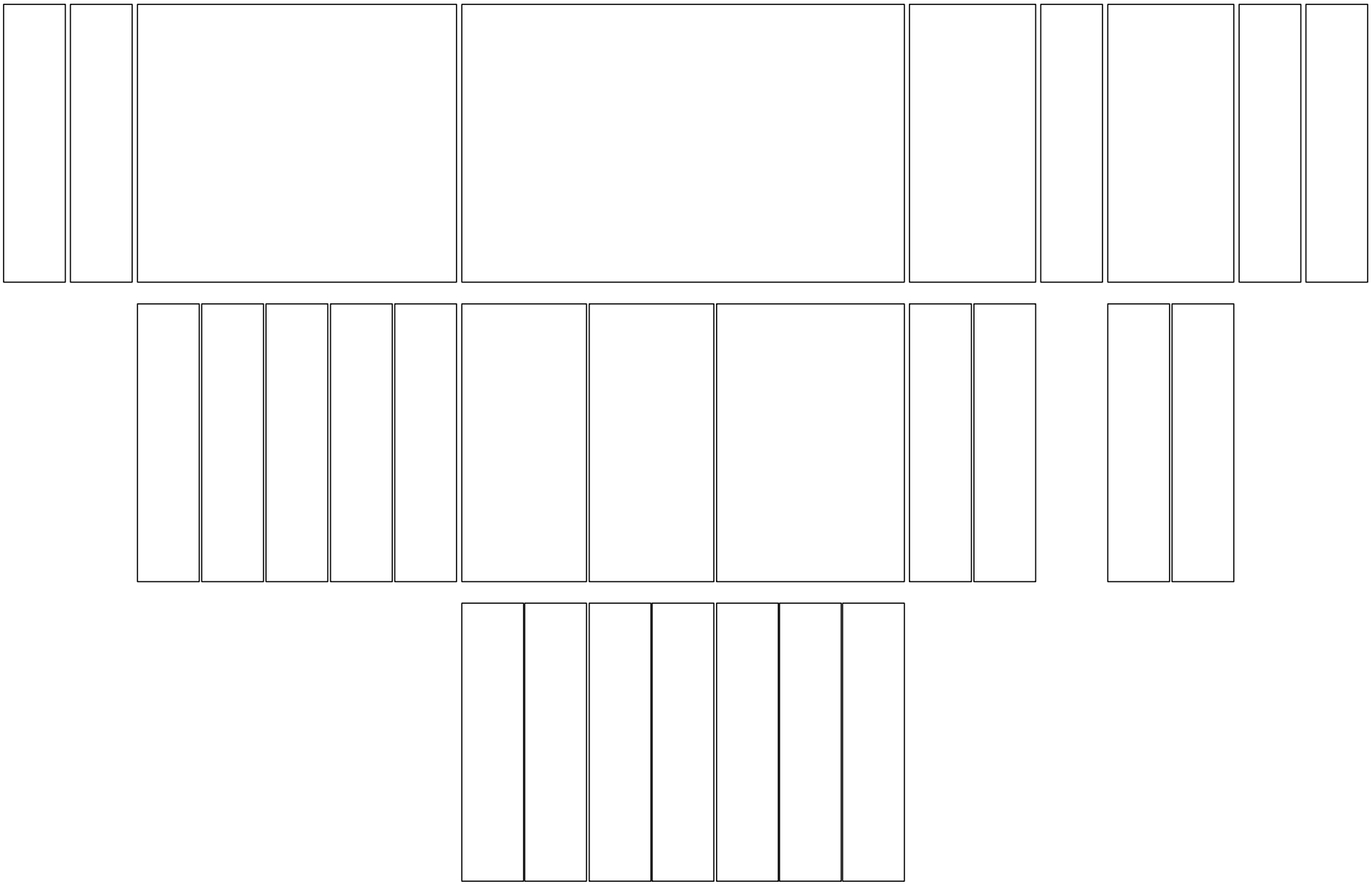
Single Sign-on / Federated Access



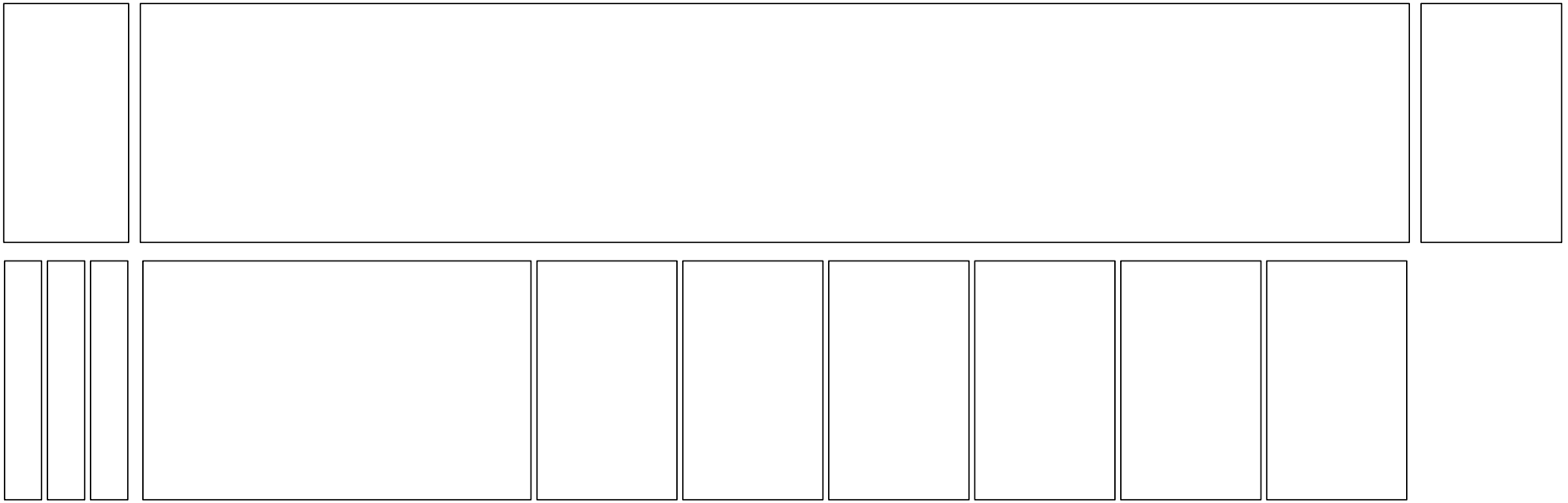
Security Assessment and Testing



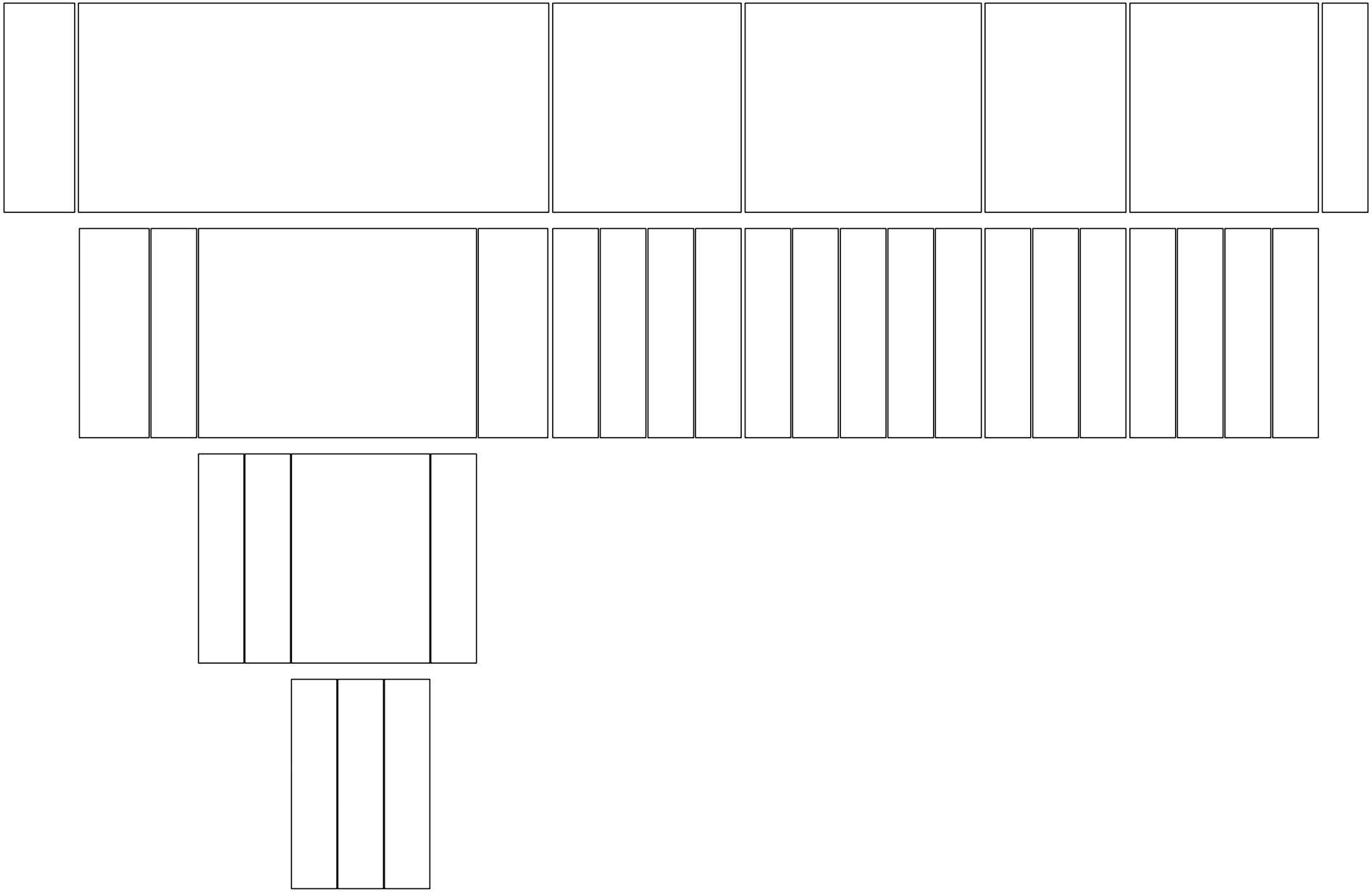
Identifying Vulnerabilities



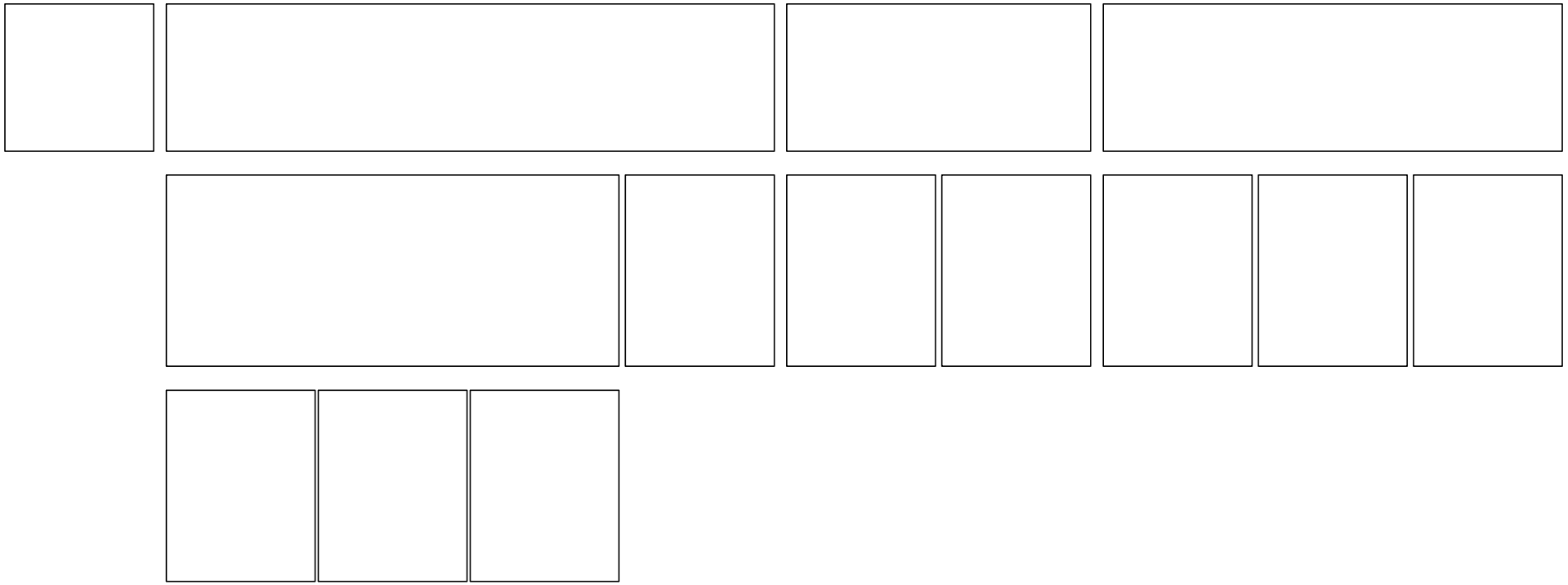
Log Review & Analysis



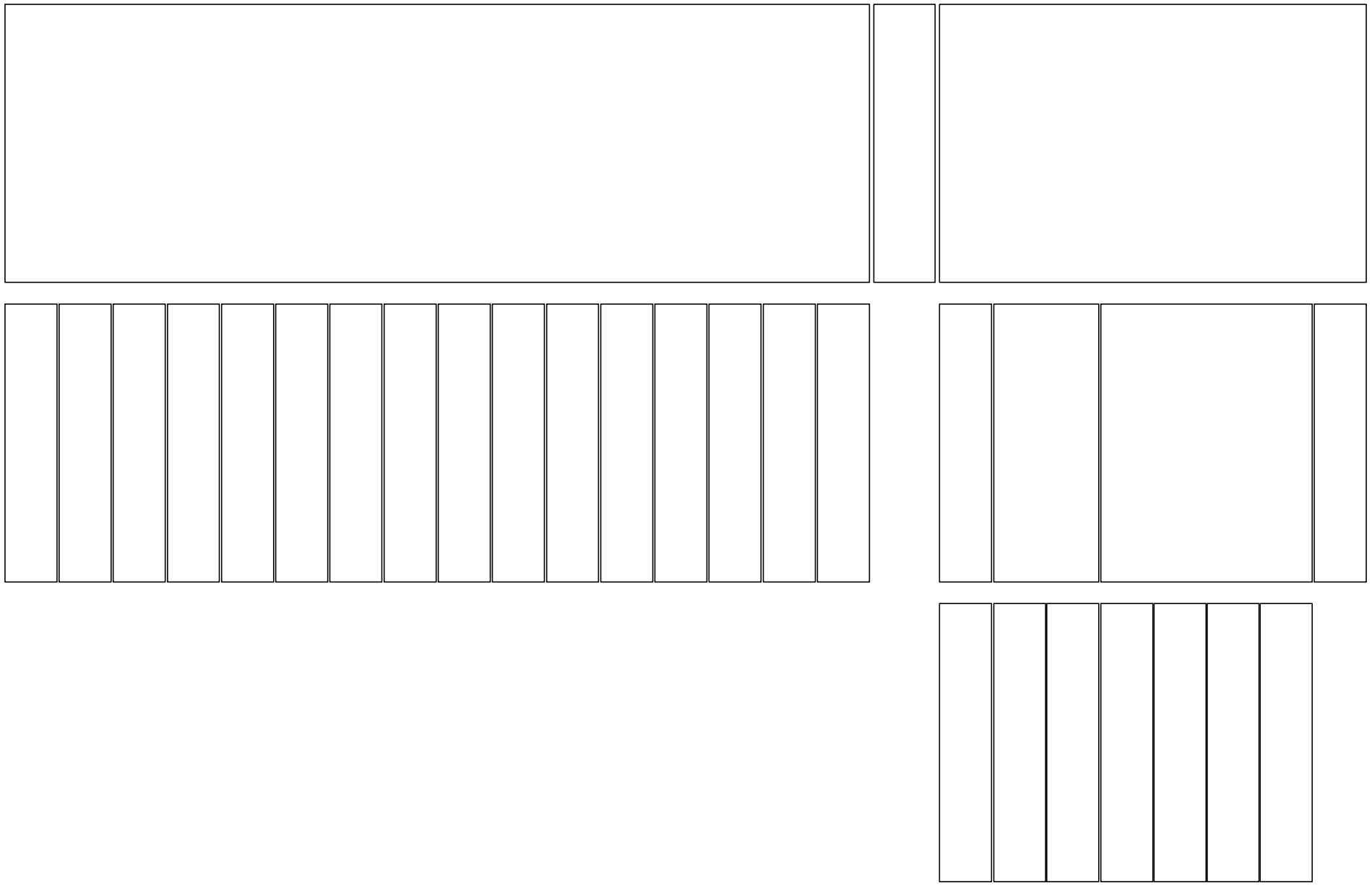
Investigations



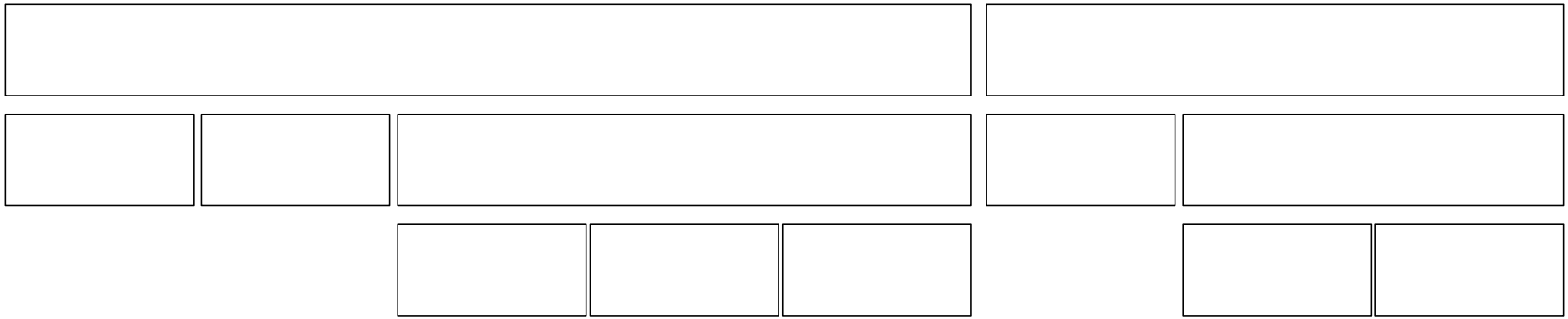
Incident Response



Malware

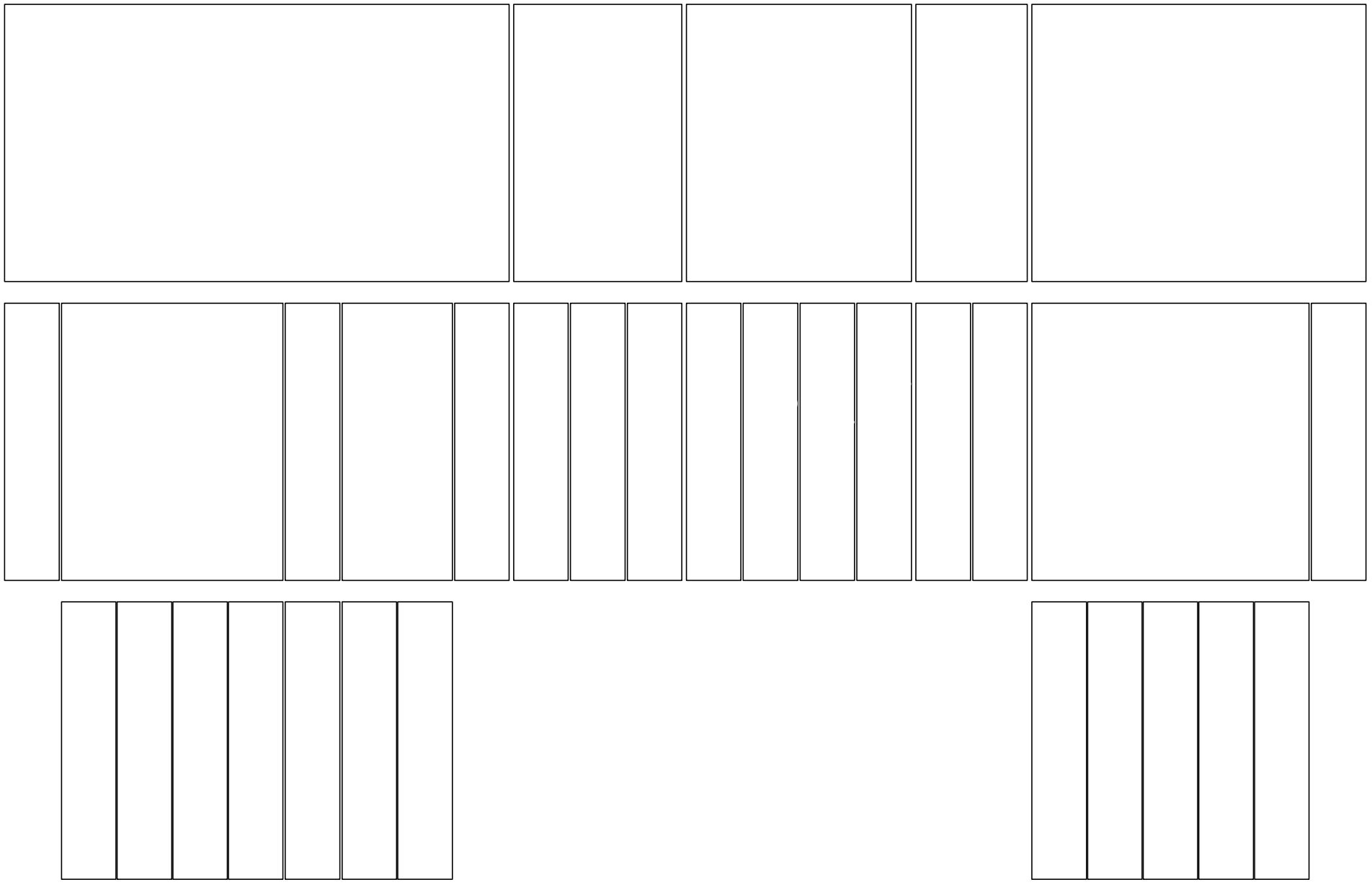


Patching

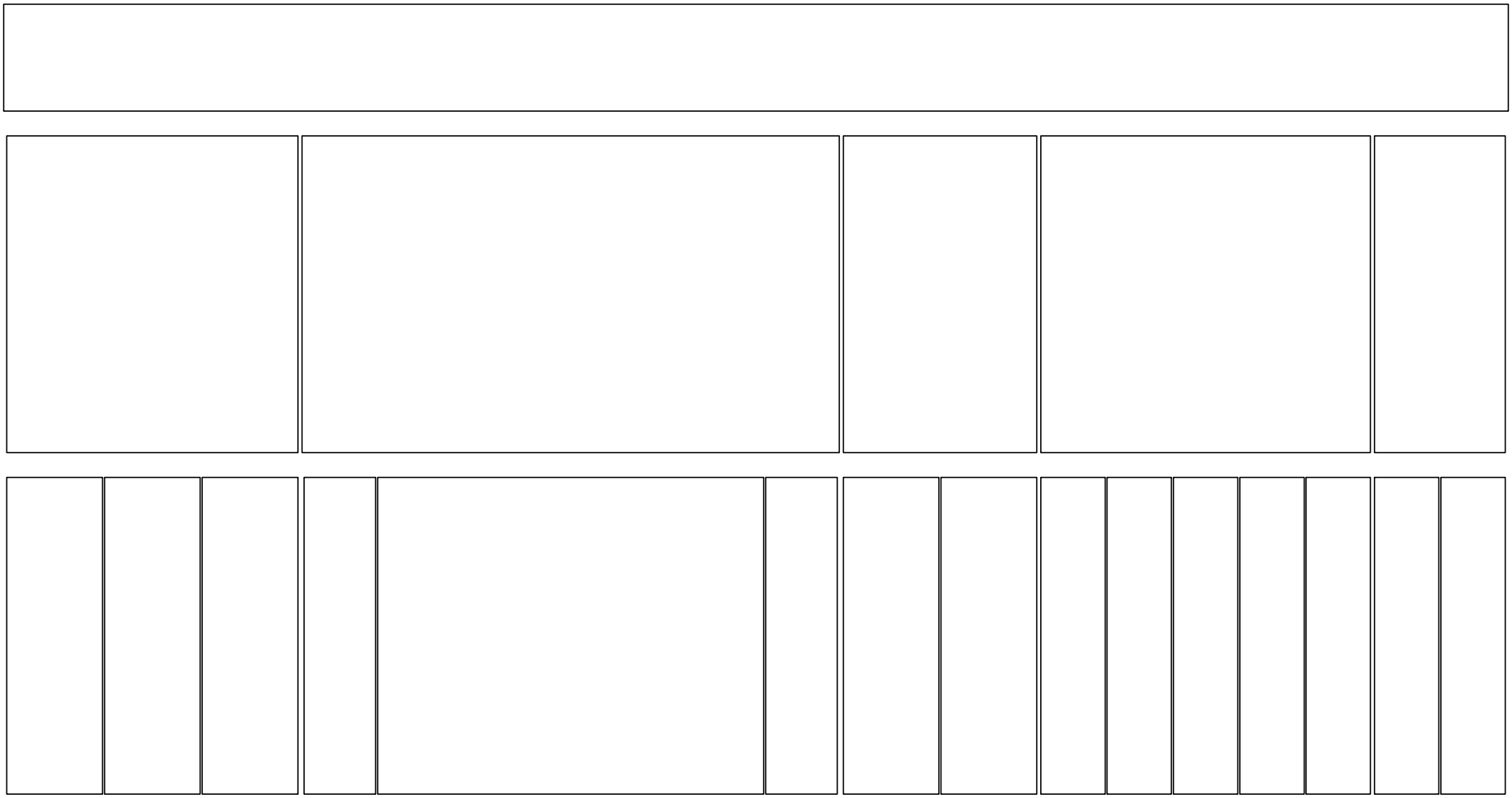


Change Management

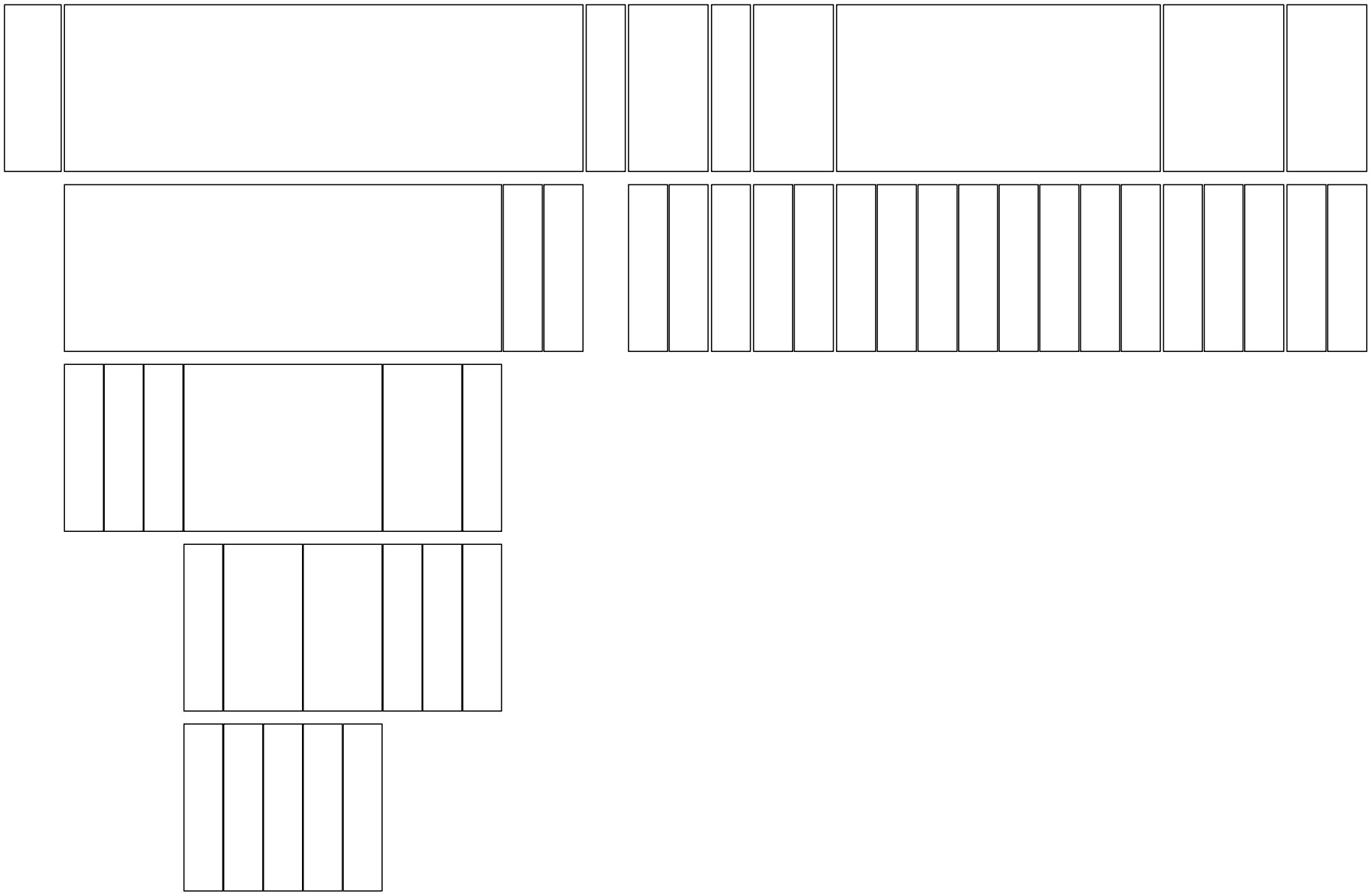
Recovery Strategies



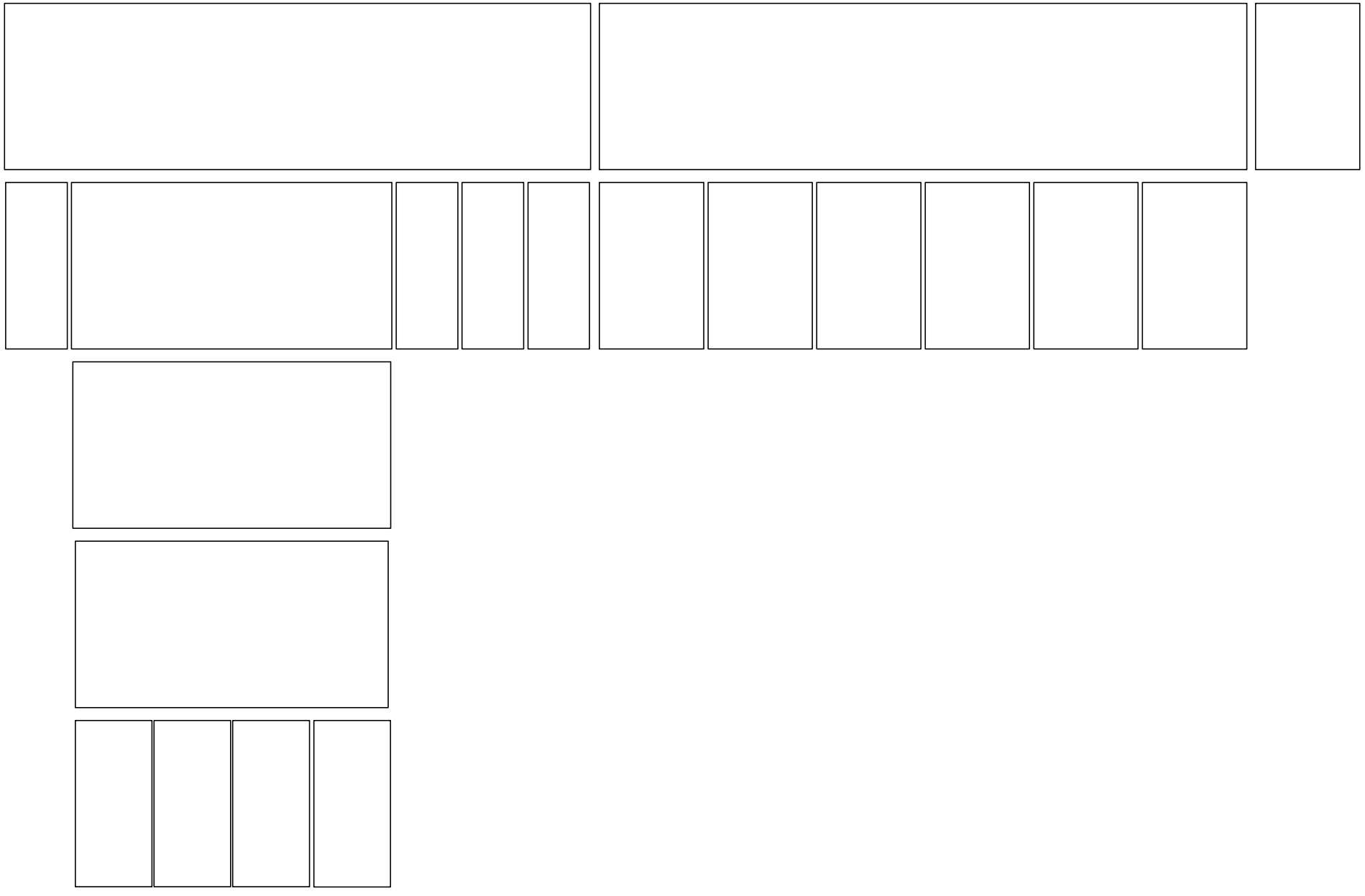
Business Continuity Management (BCM)



Secure Software Development



Databases



Hi there!

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

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

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

We have guided thousands of folks to confidently pass the CISSP exam over the last 20+ years. We provide expert instruction and an integrated intelligent system of study resources and tools.

All the best in your studies!

Rob Witcher

Co-founder & Master Instructor