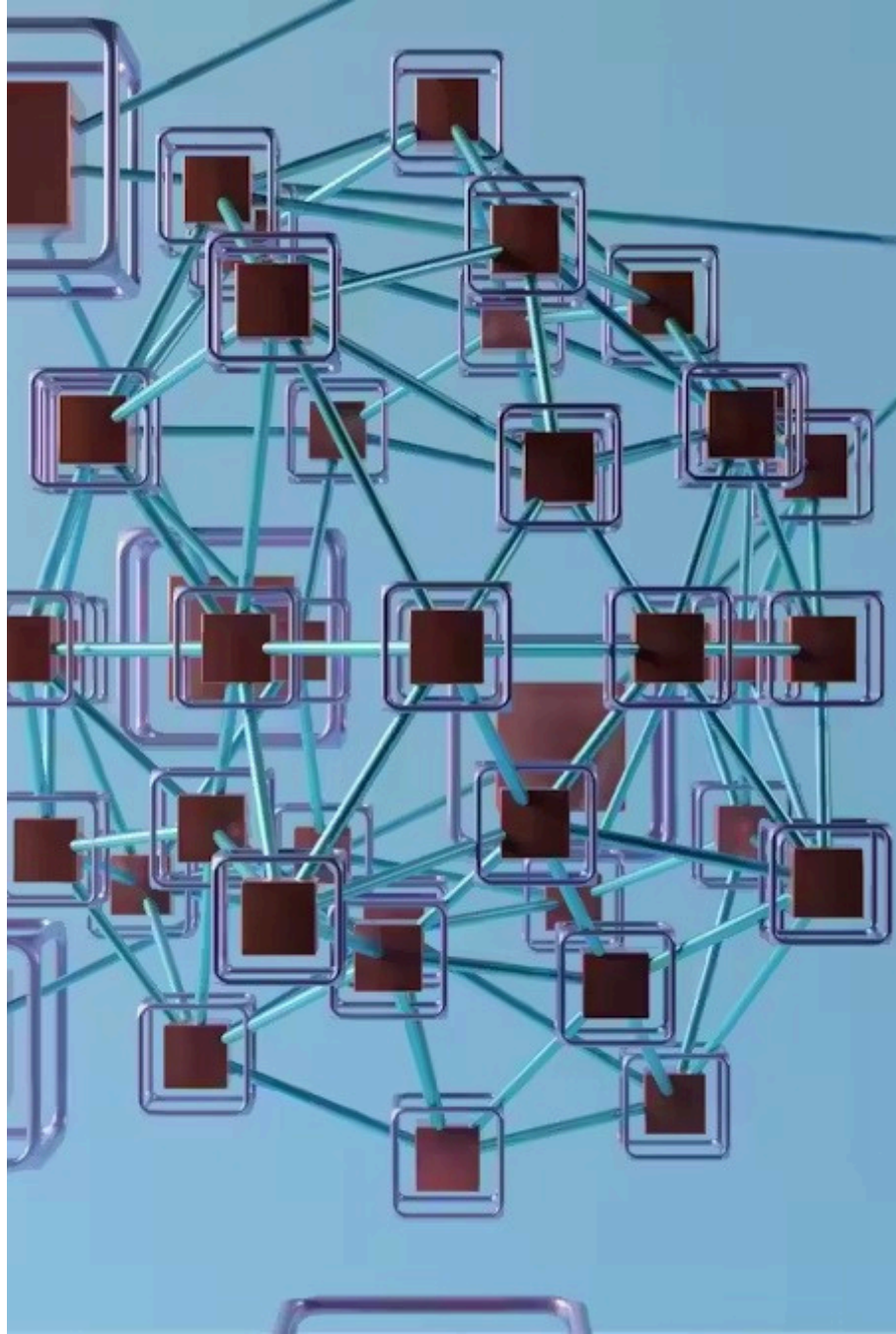
Lecture 4: Organization Security Policy Framework

Establishing Rules, Roles, and Responsibilities



Agenda

01

The3Components of a Policy Framework

02

Core Policy Documents

03

Defining the Basic Security Policy

04

Specialized Policies vs. Security Procedures

05

Example: The Event Response Procedure

The Security Policy Framework

Establishestheorganization'sattitudetowardsecurityanddefinesactions to protect assets.

Basic Security Policy

Definesorganization'ssecurity stance and principles

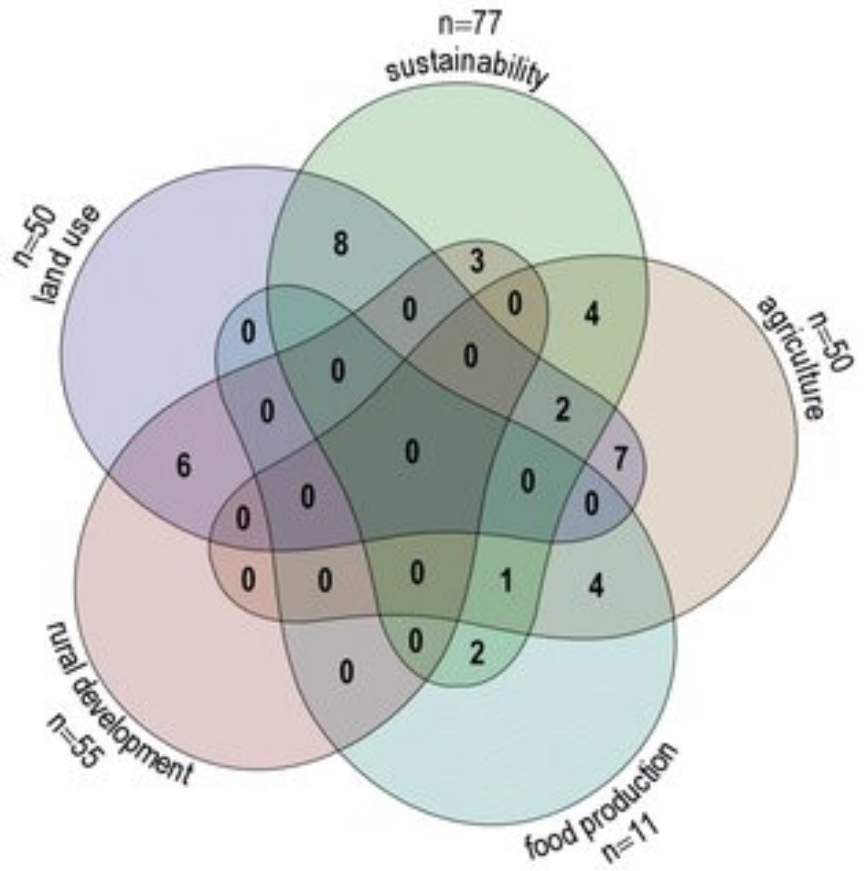
Specialized Policies

Sector-specificrulesand role-based requirements

Security Procedures

Operationalstepstoimplement and enforce policies

Core Policy Documents



Security Policy Review

Definespurpose, structure, responsibilities, and timeframe for changes.

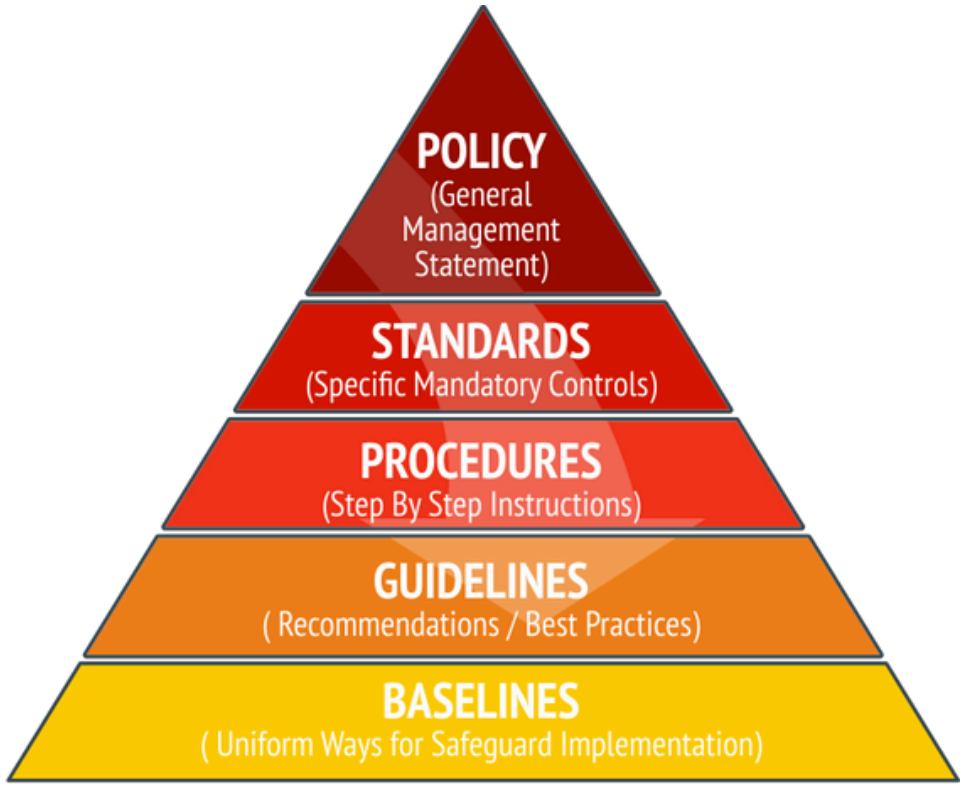
BasicSecurityPolicy Description

Determines resolved/prohibited activities and necessary controls.

Security Architecture Guide

Describes security mechanisms' relation in the organization's network architecture.

The Basic Security Policy



Role

Defines fundamental rules for processing, storing, and exchanging information.

Approach

Uses a "top-down" method to guide gradual security system development.

Function

Servesasthe foundation for all other security policies and procedures.

Specialized Security Policies

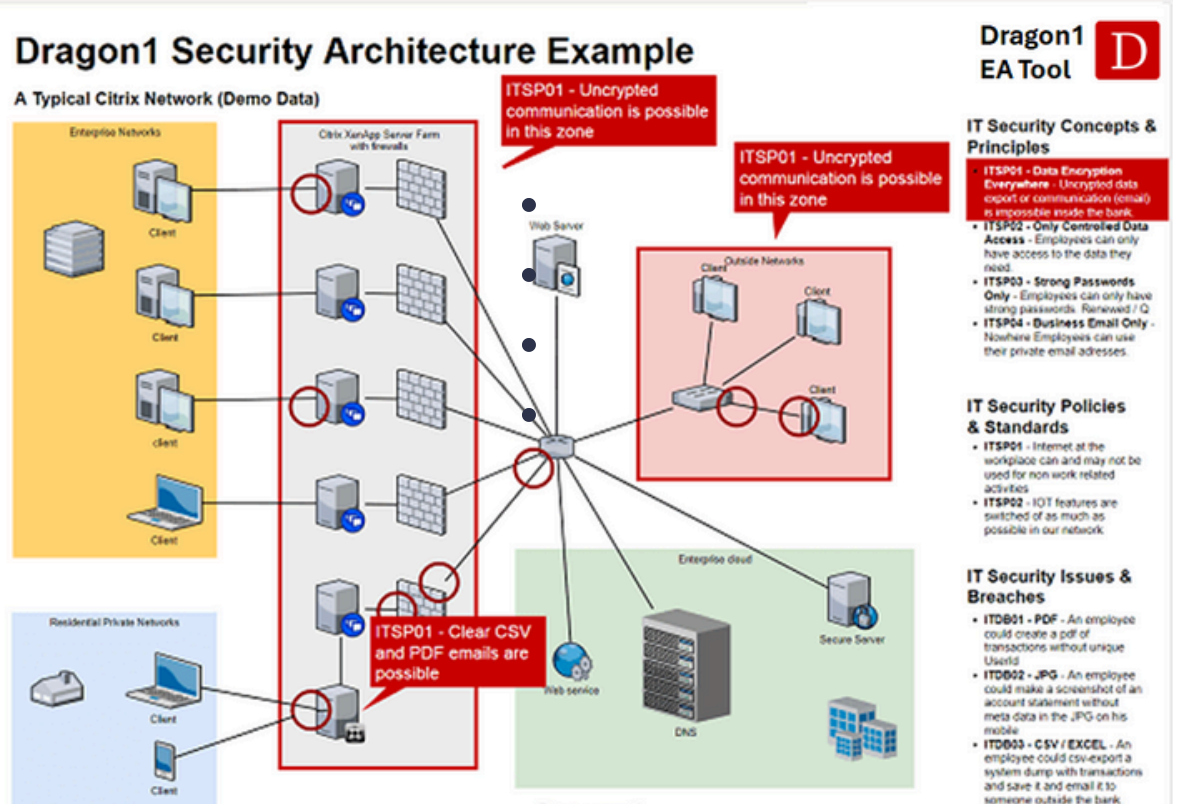
Detailed policies tailored for specific areas within an organization.

User-Affecting Policies

- Acceptable Use Policy
- Remote Access Policy
- Information Security Policy
- Password Protection Policy

Technical Area Policies

- Firewall Configuration Policy
- Encryption & Key Management Policy
- VPN Security Policy



Security Procedures: The "How-To"

Security procedures complement policies by detailing how to protect resources and enforce policies.

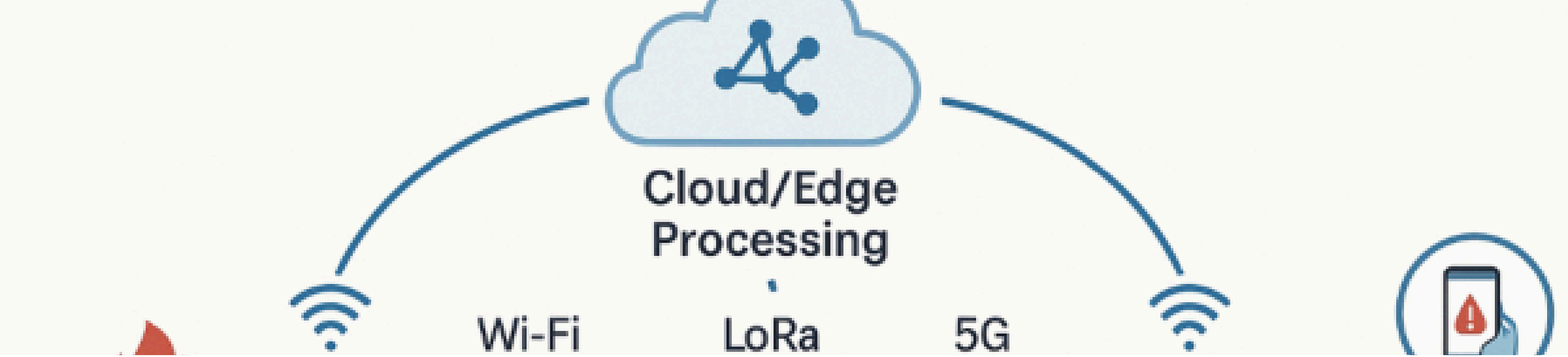
Policy

Describes what to protect and basic protection rules.

Procedure

Determines how to protect and mechanisms for enforcement.

They are step-by-step instructions transforming policy into real action.



Example: Event Response Procedure

A critical security tool for managing network intrusions or natural disasters.

1

Responsibilities

Defines roles of response team members.

2

InformationHandling

What to record, track, and how to study abnormalities.

3

Notification & Communication

Whom and when to notify, and how to release information.

4

Post-Event Analysis

How subsequent analysis should be carried out and participants.

Key Takeaways

Policy Foundation

Securitypoliciesareessential for defining an organization's security posture.

Layered Approach

Aframeworkincludesbasic, specialized policies, and detailed procedures.

Actionable Steps

Procedurestranslatepolicies into practical, actionable steps for employees.

Continuous Improvement

Regular reviewandupdatesensure policies remain effective and relevant.

Further Reading

- Landoll, D. (2021).Information Security Policies, Procedures, and Standards: A Practitioner's Reference. CRC Press.
- Straub, D. W., Goodman, S. E., &Baskerville, R. (2008). Information Security: Policy, Processes, and Practices. M.E. Sharpe.
- Paananen, H., & Siponen, M. (2019). Information security policy: An organizational-level process model. Proceedings of the 52nd Hawaii International Conference on System Sciences.

Review questions:

- What is the main purpose of an organization's security policy?
- What are the three typical components of an organization's security policy framework?
- What is the difference between a "basic security policy" and a "specialized security policy"?
- Explain the relationship between security policies and security procedures. Why are both necessary?
- What key elements should an event response procedure define?