GESTIÓN DE RIESGOS II

Ciclo 2025 - 1
SI904V (ST215V) - Seguridad de Sistemas
Jesús Huapaya Ciriaco, MBA

Content

Title: "Risk Control Strategies in Cybersecurity"

Subtitle: "Avoidance, Transfer, Mitigation & Response Planning"

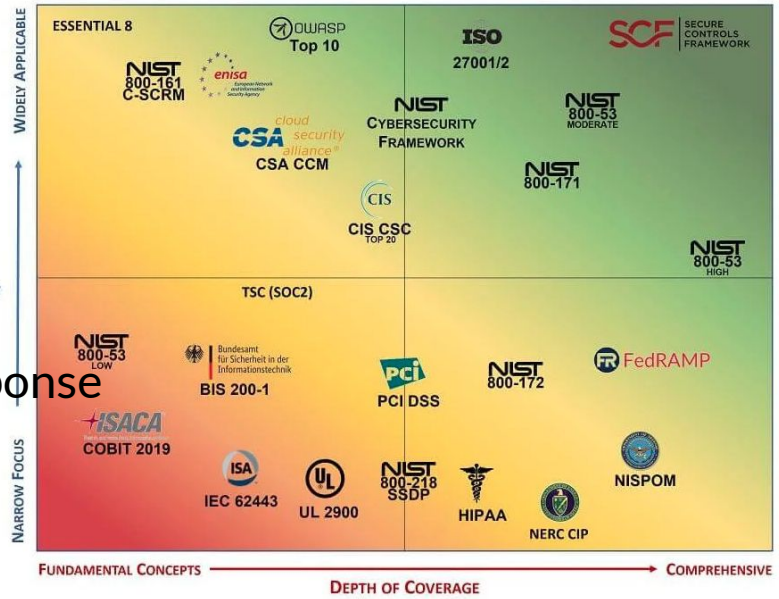
Sources:

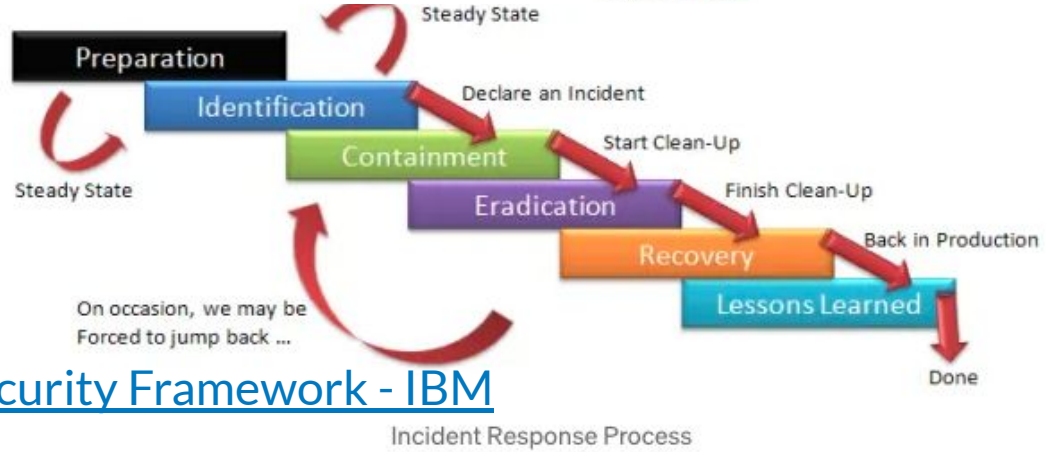
[NIST Cybersecurity Framework]

[ISO 27005 Risk Assessment]

[SANS Incident Handling]

YouTube Video: [Building a Cybersecurity Framework - IBM]





Incident Response Process

Risk Avoidance Strategies

Eliminating high-risk activities (e.g., blocking shadow IT).

Example: Prohibiting USB drives after NotPetya.

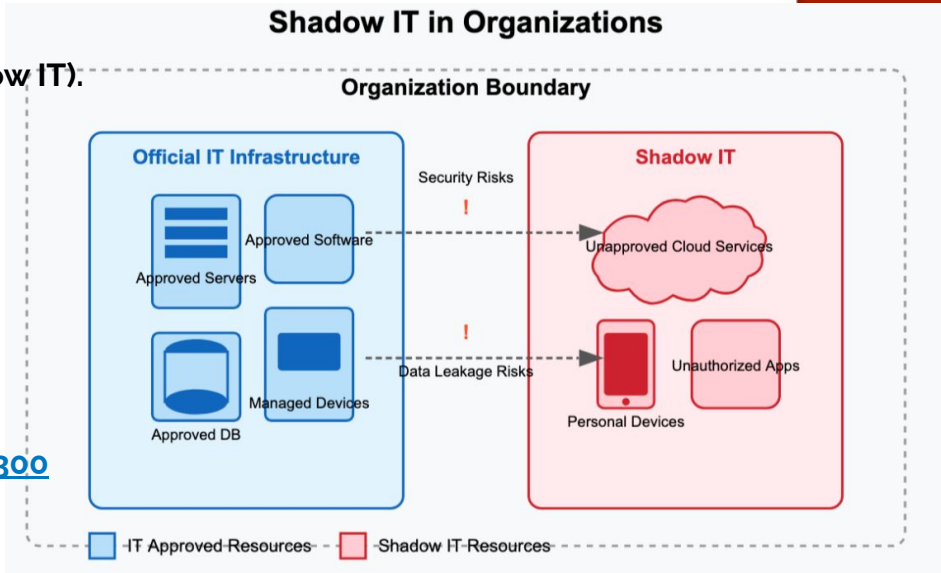
Sources:

[Integrating Cybersecurity and Enterprise Risk Management (ERM)]

[Maersk says June cyberattack could cost it up to $300 million]

[Don't Let Shadow IT Put Your Business at Risk]

YouTube Video: The Dangers of the USB Drive



Risk Transfer Methods

Cyber insurance (e.g., AIG's $90M payout for Mondelez).

Third-party contracts (SLA penalties).

Sources

Insurance giant settles NotPetya lawsuit, signaling cyber insurance shakeup

Cyber Insurance Guide (FTC)

Cloud SLAs (AWS)

YouTube Video: How Would Cyber Insurance Companies Cover Catastrophic Hacks? | WSJ Tech News Briefing

Incident Response Plan (IRP)

NIST's 4 phases: Preparation → Detection → Containment → Recovery.

Case: Equifax's failed IRP execution.

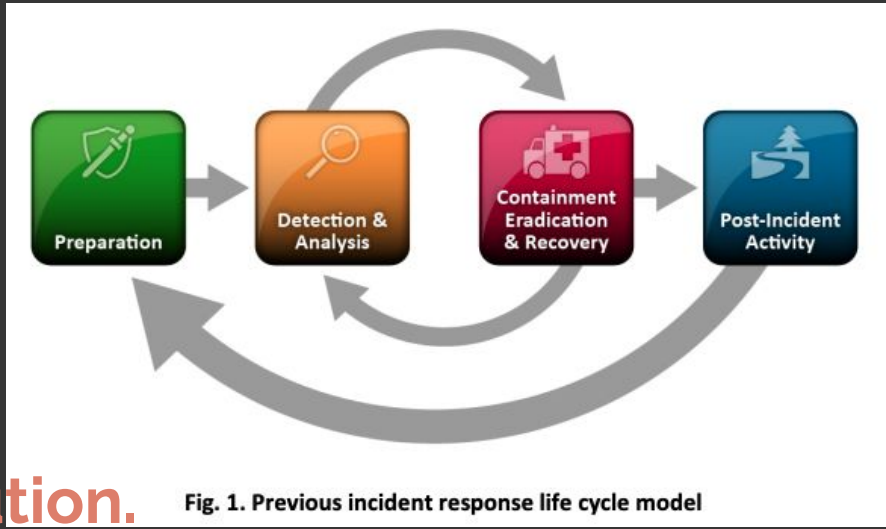


Fig. 1. Previous incident response life cycle model

Sources

Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile

Equifax IRP Failures (US Senate)

SANS 504-B Incident Response Cycle: Cheat-Sheet

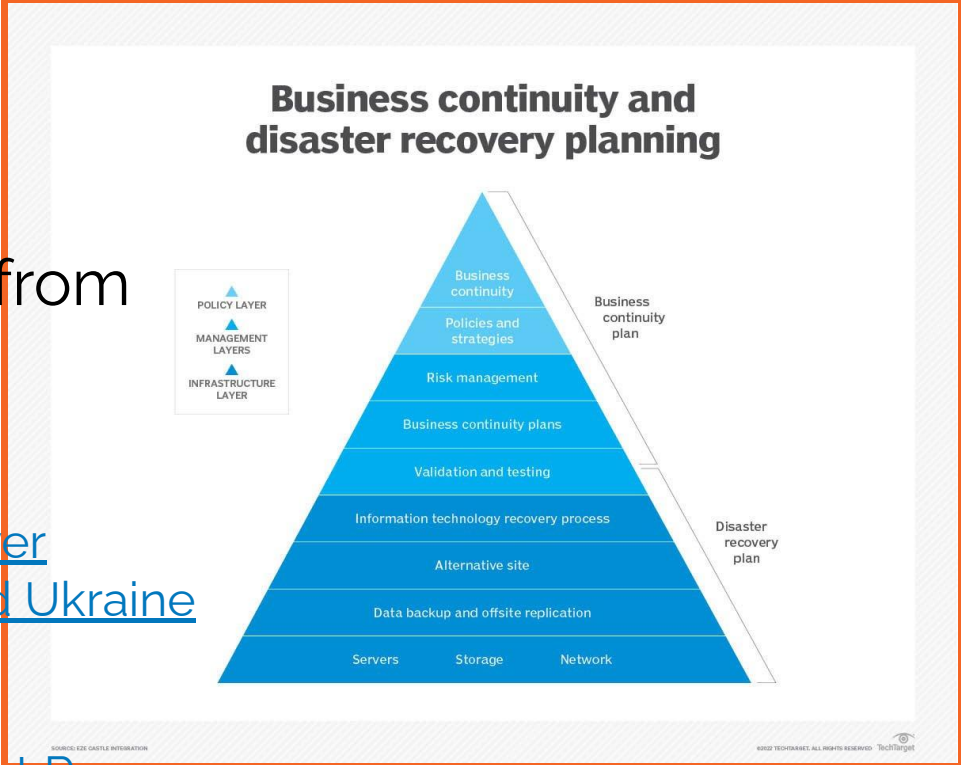
YouTube Video: Mastering Your Incident Response Plan (IRP): Are you prepared, Guide to plan Ahead?

Disaster Recovery Plan (DRP)

RTO/RPO metrics.
Case: Maersk's 10-day recovery from NotPetya.

Sources:
[The NIST CyberSecurity Framework: Recover]
[The day a mysterious cyber-attack crippled Ukraine]
[DRP Best Practices (DisasterRecovery.org)]

YouTube Video: [Difference Between Incident Response Plan (IRP) and Disaster Recovery Plan (DRP)]



Business Continuity Plan (BCP)

Critical function prioritization.

Case: Zoom's BCP during COVID-19 surge.

Sources:

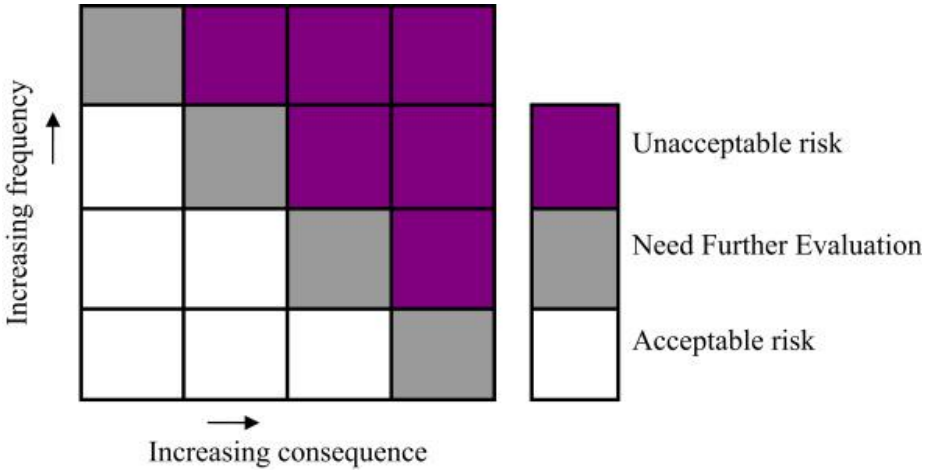
[ISO 22301:2019 (Draft): Security and resilience — Business continuity management systems — Requirements]

[Zoom chalks up 300 million daily participants despite security issues]

["Business Continuity Management" - Federal Financial Institutions Examination Council (FFIEC)]

YouTube Video: [More Companies Advise Against Using Zoom During Covid-19 Crisis]

Risk Acceptance Criteria



Risk appetite frameworks.

Example: Banks accepting fraud risks with cost-benefit analysis.

Sources:
COSO Risk Appetite Framework

How Much Does Fraud Prevention and Compliance Cost Banks?

FAIR Risk Model

YouTube Video: Risk Appetite & Tolerance (ISACA)

Risk Control Cycles

PDCA (Plan-Do-Check-Act) in controls.

Case: Toyota's continuous security improvement.

Sources:
- Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- Toyota Leaked Vehicle Data of 2 Million Customers
- ISO 27001 Series: The PCDA Approach

YouTube Video: PDCA Cycle: Plan Do Check Act (What is PDCA and how is it used in Information Security?)

Figure D-1. Security Automation Domains

Control Categories & Functions

Type	Example
Preventive	Firewalls, MFA
Detective	SIEM, IDS
Corrective	Backups, Patches

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

TABLE 1: Security and Privacy Control Families

Sources

NIST (SP 800-53) - Security and Privacy Controls for Information Systems and Organizations

Open Web Application Security Project (OWASP) Controls

CIS Critical Security Controls

YouTube Video: Unify Your Security Operations with Splunk Mission Control

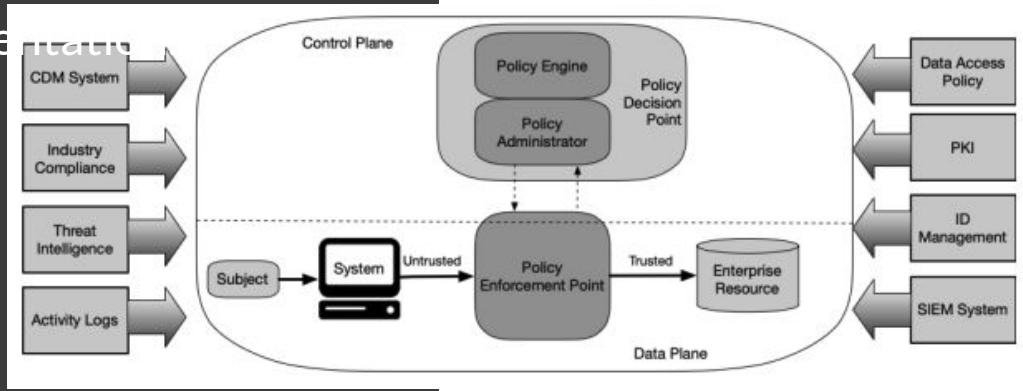
Layered Defense Strategy

Defense in depth: Network → Host → App → Data layers.

Case: Microsoft's Zero Trust implementation

Sources:
- NIST Zero Trust Architecture
- Microsoft Zero Trust Case
- CISA Cyber Essentials Starter Kit

YouTube Video: Zero Trust Explained (Microsoft)



Case 1: Cambridge Analytica & Data Privacy Violations (2018)

What happened: Harvested 87M Facebook profiles without consent for political targeting

Legal consequences: $5B FTC fine (largest in Facebook's history)

Ethical issues: Consent, data misuse, and democratic integrity

Sources:

FTC Settlement Document

YouTube Video: What is the Cambridge Analytica scandal?

Case 2: Uber Data Breach Cover-up (2016)

What happened: Paid hackers $100k to hide breach of 57M user records

Legal fallout: $148M settlement across US states

Professional ethics: CSO fired for concealment

Sources:

What can the Uber breach teach us about information security?

YouTube Video: Uber Paid Hackers $100K To Delete Data And Stay Quiet | CNBC

Case 3: Sony Pictures Hack (2014)

What happened: North Korean hackers leaked emails and unreleased films

Legal issues: First cyberattack declared act of terrorism by US

Intellectual property implications: Pirated films cost millions

Sources:

The Sony Pictures Breach: A Deep Dive into a Landmark Cyber Attack

YouTube Video: The Perfect Weapon (2020): Sony Hack (Clip) | HBO

Case 4: Microsoft vs. US Government (2013-2018)

Legal battle: Refusal to hand over emails stored in Irish data center

Outcome: CLOUD Act resolution (clarifying cross-border data access)

Privacy vs. law enforcement debate

Sources:

United States vs Microsoft

YouTube Video: Defending the cloud: Microsoft argues landmark data storage case

Case 5: Google Right to Be Forgotten (2014-Present)

EU ruling: Individuals can request removal of personal search results

Implementation challenges: Over 5 million URLs processed

Balance between privacy and free speech

Sources:

Google wins landmark right to be forgotten case

YouTube Video: Privacy Law and the right to be forgotten: Three Minute Lectures