Information Security CS 3002

Dr. Haroon Mahmood

Assistant Professor

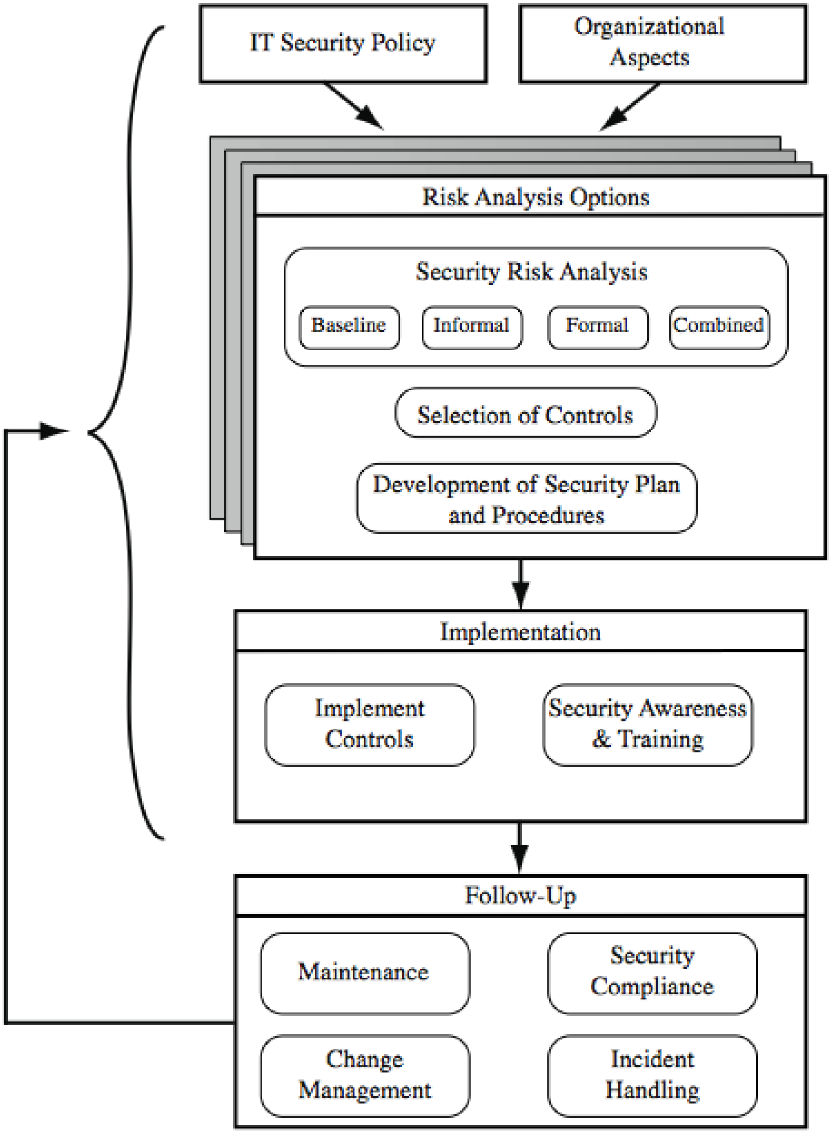
NUCES Lahore

Disclaimer: The contents of these slides have been taken from the book of Computer Security by William Stallings.

IT Security Management

- **IT Security Management:** a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability. IT security management functions include:
  - organizational IT security objectives, strategies and policies
  - determining organizational IT security requirements
  - identifying and analyzing security threats to IT assets
  - identifying and analyzing risks
  - specifying appropriate safeguards
  - monitoring the implementation and operation of safeguards
  - developing and implement a security awareness program
  - detecting and reacting to incidents

IT Security Management Process



IT Security Policy

Organizational Aspects

Risk Analysis Options

Security Risk Analysis

Baseline

Informal

Formal

Combined

Selection of Controls

Development of Security Plan and Procedures

Implementation

Implement Controls

Security Awareness & Training

Follow-Up

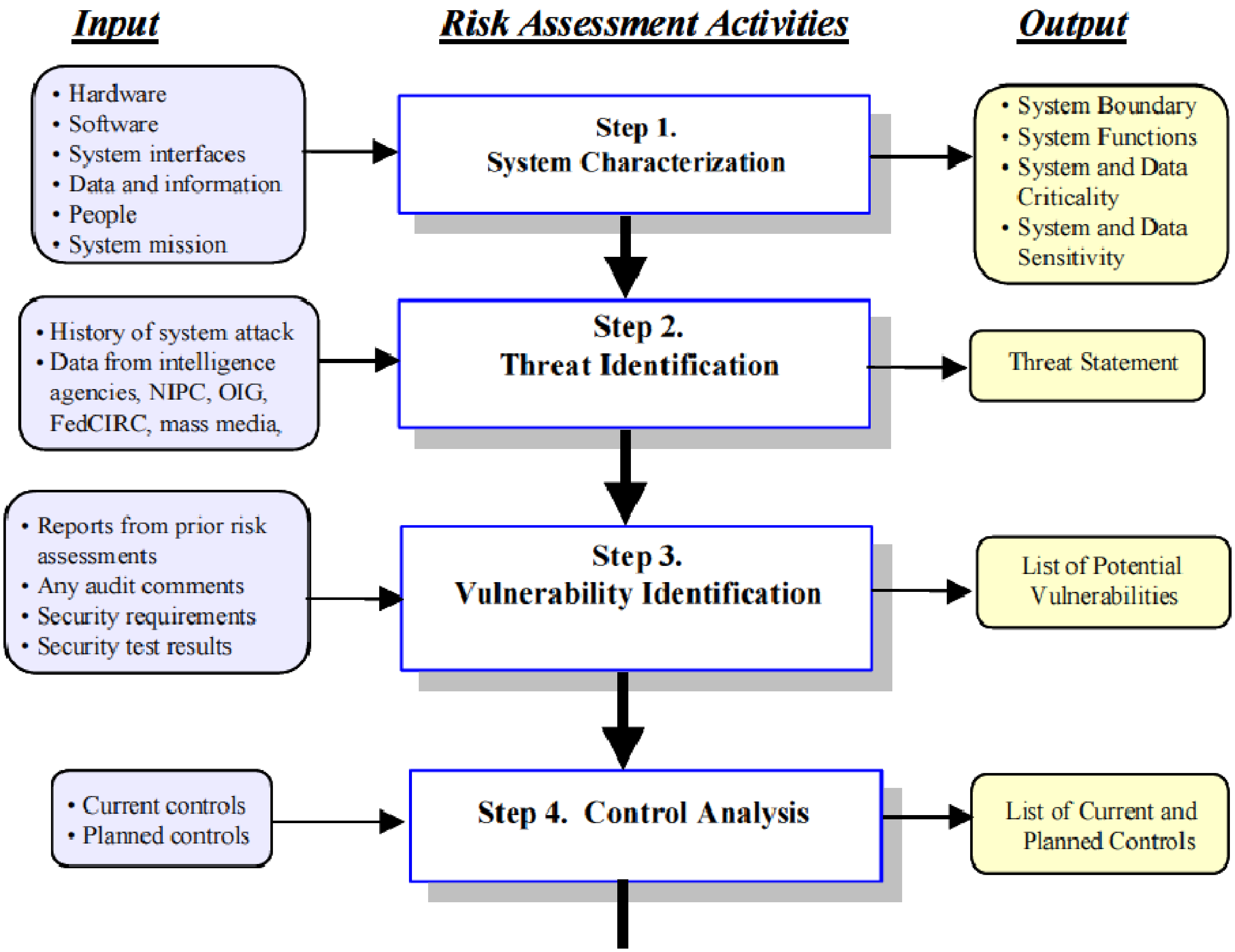
Maintenance

Security Compliance

Change Management

Incident Handling

Security Risk Analysis



Input

Risk Assessment Activities

Output

- Hardware
- Software
- System interfaces
- Data and information
- People
- System mission

Step 1.
System Characterization

- System Boundary
- System Functions
- System and Data Criticality
- System and Data Sensitivity

- History of system attack
- Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media,

Step 2.
Threat Identification

Threat Statement

- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test results

Step 3.
Vulnerability Identification

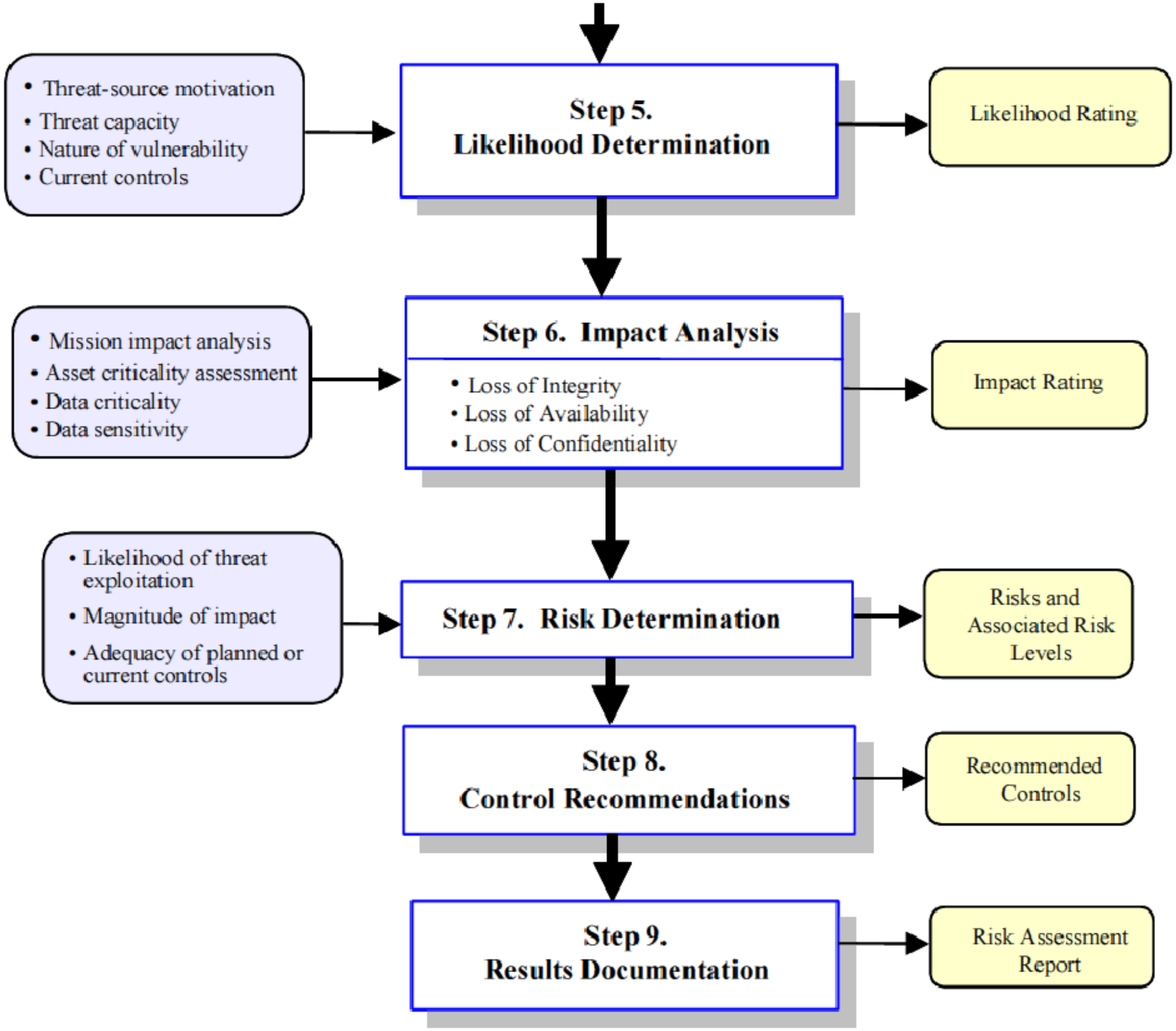
List of Potential Vulnerabilities

- Current controls
- Planned controls

Step 4. Control Analysis

List of Current and Planned Controls

Security Risk Analysis



- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls

Step 5.
Likelihood Determination

Likelihood Rating

- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity

Step 6. Impact Analysis

- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

Impact Rating

- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

Step 7. Risk Determination

Risks and Associated Risk Levels

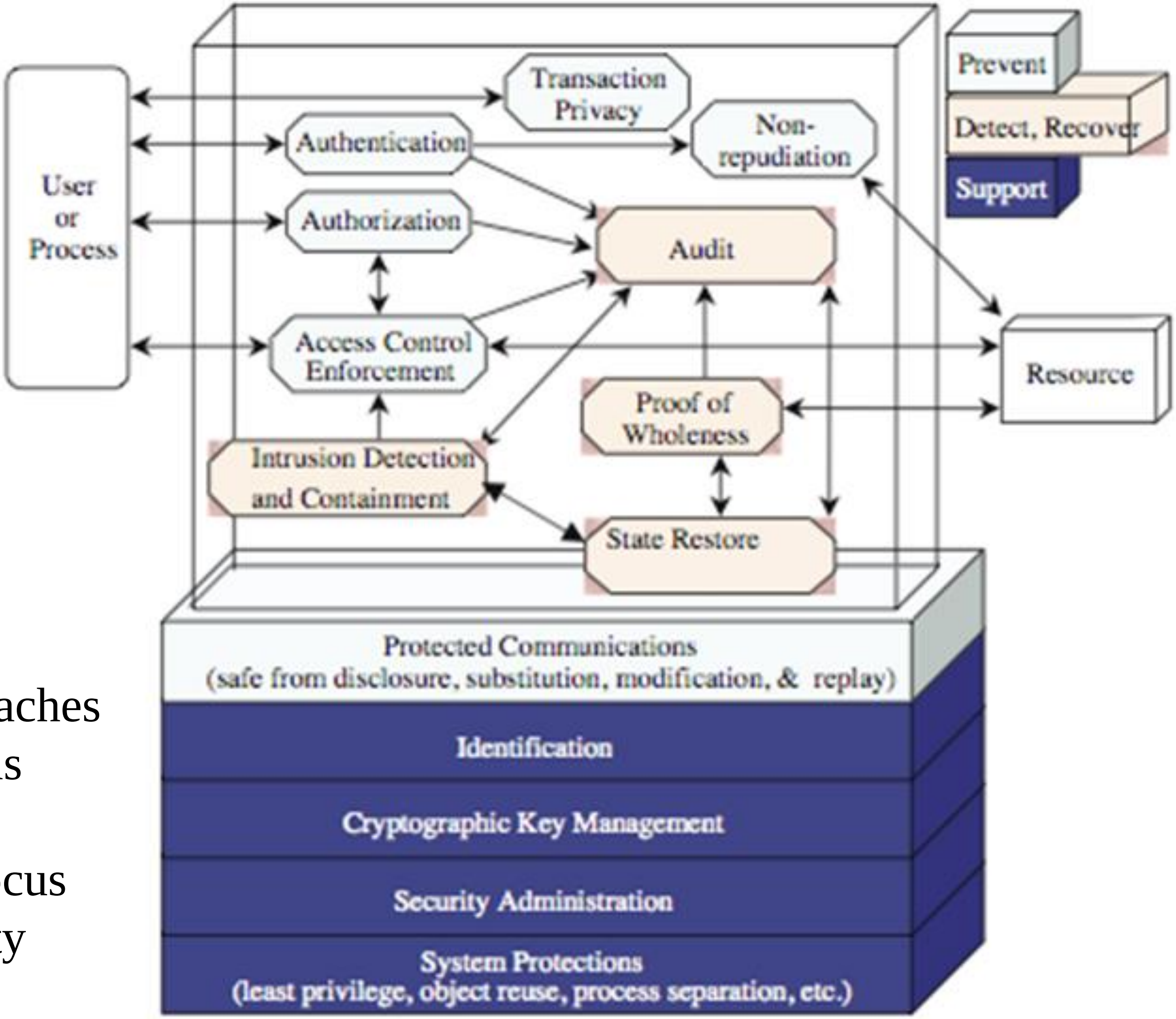
Step 8.
Control Recommendations

Recommended Controls

Step 9.
Results Documentation

Risk Assessment Report

Technical Controls



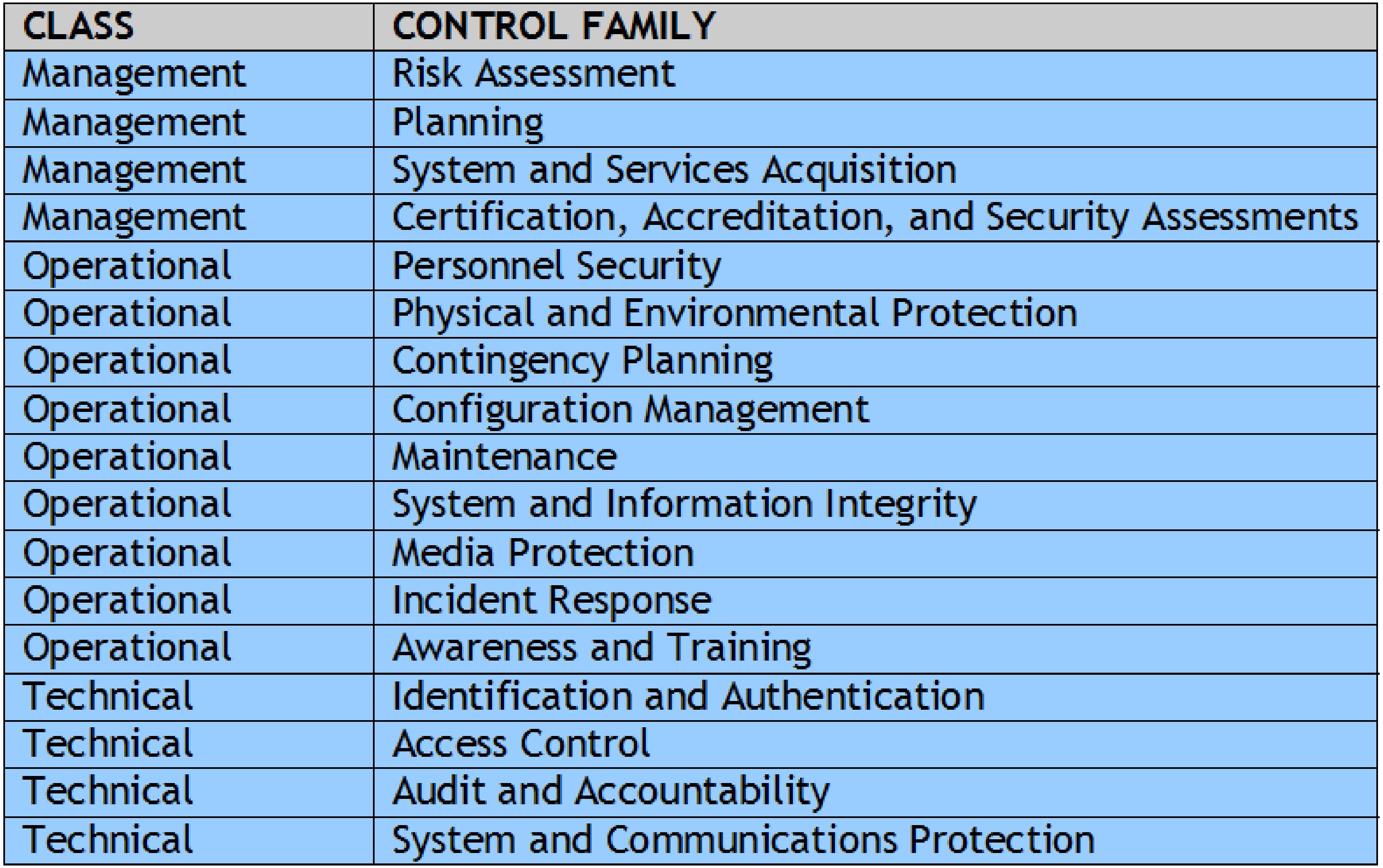
Prevent
Detect, Recover
Support
User or Process
Transaction Privacy
Authentication
Non-repudiation
Authorization
Audit
Access Control Enforcement
Resource
Proof of Wholeness
Intrusion Detection and Containment
State Restore
Protected Communications (safe from disclosure, substitution, modification, & replay)
Identification
Cryptographic Key Management
Security Administration
System Protections (least privilege, object reuse, process separation, etc.)

Supportive: generic, underlying technical IT capabilities

Preventative: focus on preventing security breaches by warning of violations

Detection/recovery: focus on response to a security breach

Lists of Controls (NIST, ISO; choose a combination)



CLASS	CONTROL FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection

IT Security Plan

- provides details of
  - what will be done
  - what resources are needed
  - who is responsible

- should include
  - risks, recommended controls, action priority
  - selected controls, resources needed
  - responsible personnel, implementation dates

Implementation Plan

Risk (Asset/ Threat)	Level of Risk	Recommended Controls	Priority	Selected Controls	Required Resources	Responsible Persons	Start - End Date	Other Comments
Hacker attack on Internet Router	High	1. disable external telnet access 2. use detailed auditing of privileged command use 3. set policy for strong admin passwords 4. set backup strategy for router config file 5. set change control policy for the router configuration	1	1. 2. 3. 4. 5.	1. 3 days IT net admin time to change & verify router config, write policies; 2. 1 day of training for net admin staff	Sohail Naeem, Lead Network Sys Admin, Corporate IT Support Team	1-Feb-2021 to 4-Feb-2021	1. need periodic test & review of config & policy use

Case Study: Silver Star Mines

- fictional operation of global mining company
- large IT infrastructure
  - a variety of servers executing both common and specific software
  - some directly relates to health & safety
  - formerly isolated systems now networked with internet

- An initial review of company’s risk profile and security recommendations are required

Assets and security requirements

- reliability and integrity of SCADA nodes and net
- integrity of stored file and database information
- availability, integrity of financial system
- availability, integrity of procurement system
- availability, integrity of maintenance/production system
- availability, integrity and confidentiality of mail services

Threats & Vulnerabilities

- unauthorized modification of control system
- corruption, theft, loss of info
- attacks/errors affecting procurement system
- attacks/errors affecting financial system
- attacks/errors affecting mail system
- attacks/errors maintenance/production affecting system

Risk Analysis

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	layered firewalls & servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	firewall, policies	Possible	Major	Extreme	2
Availability and integrity of Financial System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	3
Availability and integrity of Procurement System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	4
Availability and integrity of Maintenance/ Production System	Attacks/errors affecting system	firewall, policies	Possible	Minor	Medium	5
Availability, integrity and confidentiality of mail services	Attacks/errors affecting system	firewall, ext mail gateway	Almost Certain	Minor	High	6

Security Compliance (Audit/Verify)

- audit process to review security processes
- to verify compliance with security plan
- using internal or external personnel
- usually based on checklists to check
  - suitable policies and plans were created
  - suitable selection of controls were chosen
  - that they are maintained and used correctly
- often as part of wider general audit

Human-Caused Threats

- Less predictable, may be targeted, harder to deal with

- Include:
  - Unauthorized physical access
    - leading to other threats
  - Theft of equipment / data
  - Vandalism of equipment/data
  - Misuse of resources

Mitigation Measures: Human-Caused Threats

- improving employee behavior
- increasing employee accountability
- mitigating liability for employee behavior
- complying with regulations and contractual obligations
- Physical access control
  - IT equipment, wiring, power, communications, media
- Have a spectrum of approaches
  - Restrict building access, locked area, secured, power switch secured, tracking device
- Also need intruder sensors/alarms
- hiring, training, monitoring behavior, and handling departure

Security in Hiring Process

- **Objective:**
  - **“to ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities”**
- **need appropriate background checks, screening, and employment agreements**

Background Checks & Screening

- issues:
  - inflated resumes
  - reticence of former employers to give good or bad references due to fear of lawsuits
- employers do need to make significant effort to do background checks / screening
  - get detailed employment / education history
  - reasonable checks on accuracy of details
  - have experienced staff members interview
- for some sensitive positions, additional intensive investigation is warranted

Employment Agreements

- employees should agree to and sign the terms and conditions of their employment contract, which should include:
  - information on their and the organization’s security responsibilities
  - confidentiality and non-disclosure agreement
  - agreement to abide by organization's security policy

During Employment

- current employee security objectives:
  - ensure employees, contractors, third party users are aware of info security threats & concerns
  - know their responsibilities and liabilities
  - are equipped to support organizational security policy in their work, and reduce human error risks
- need security policy and training
- security principles:
  - least privilege
  - separation of duties
  - limited reliance on key personnel

Termination of Employment

- termination security objectives:
  - ensure employees, contractors, third party users exit organization or change employment in an orderly manner
  - that the return of all equipment and the removal of all access rights are completed

- critical actions:
  - remove name from authorized access list
  - inform guards that general access not allowed
  - remove personal access codes, change lock combinations, reprogram access card systems, etc
  - recover all assets

Email & Internet Use Policies

- E-mail & Internet access for employees is common in office and some factories
- increasingly have e-mail and Internet use policies in organization's security policy
- due to concerns regarding
  - work time lost
  - computer / comms resources consumed
  - risk of importing malware
  - possibility of harm, harassment, bad conduct