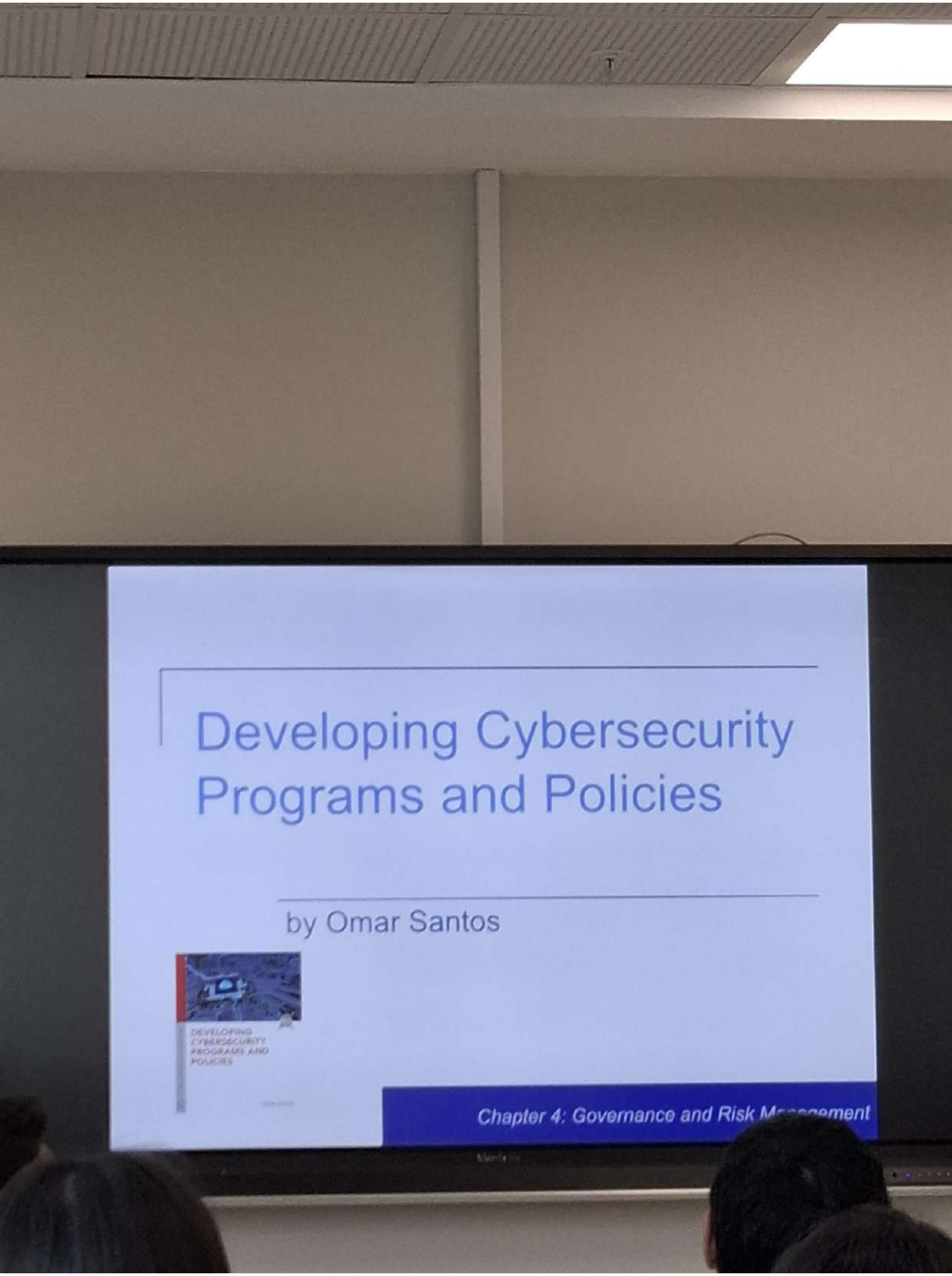
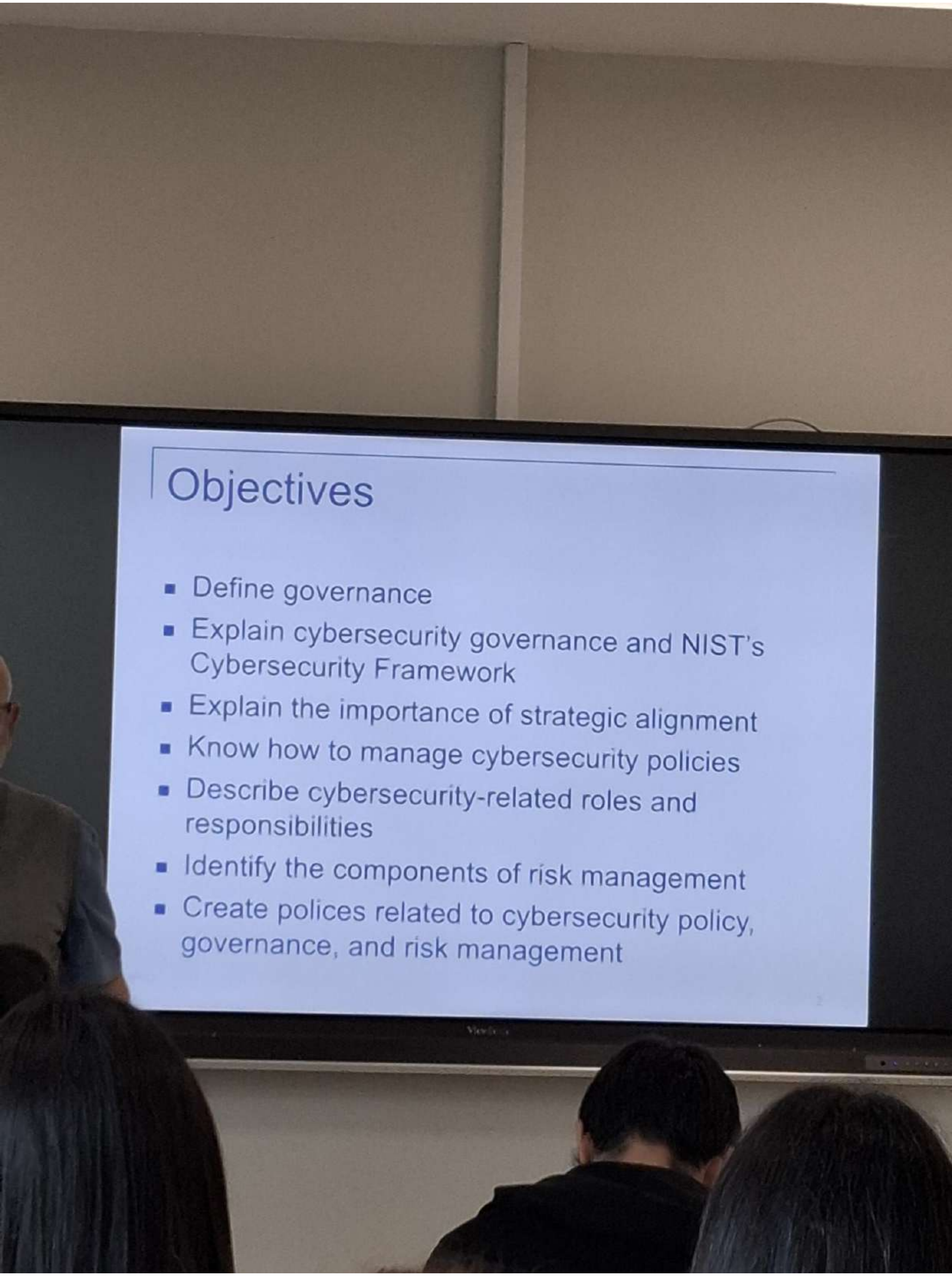


Developing Cybersecurity Programs and Policies

by Omar Santos

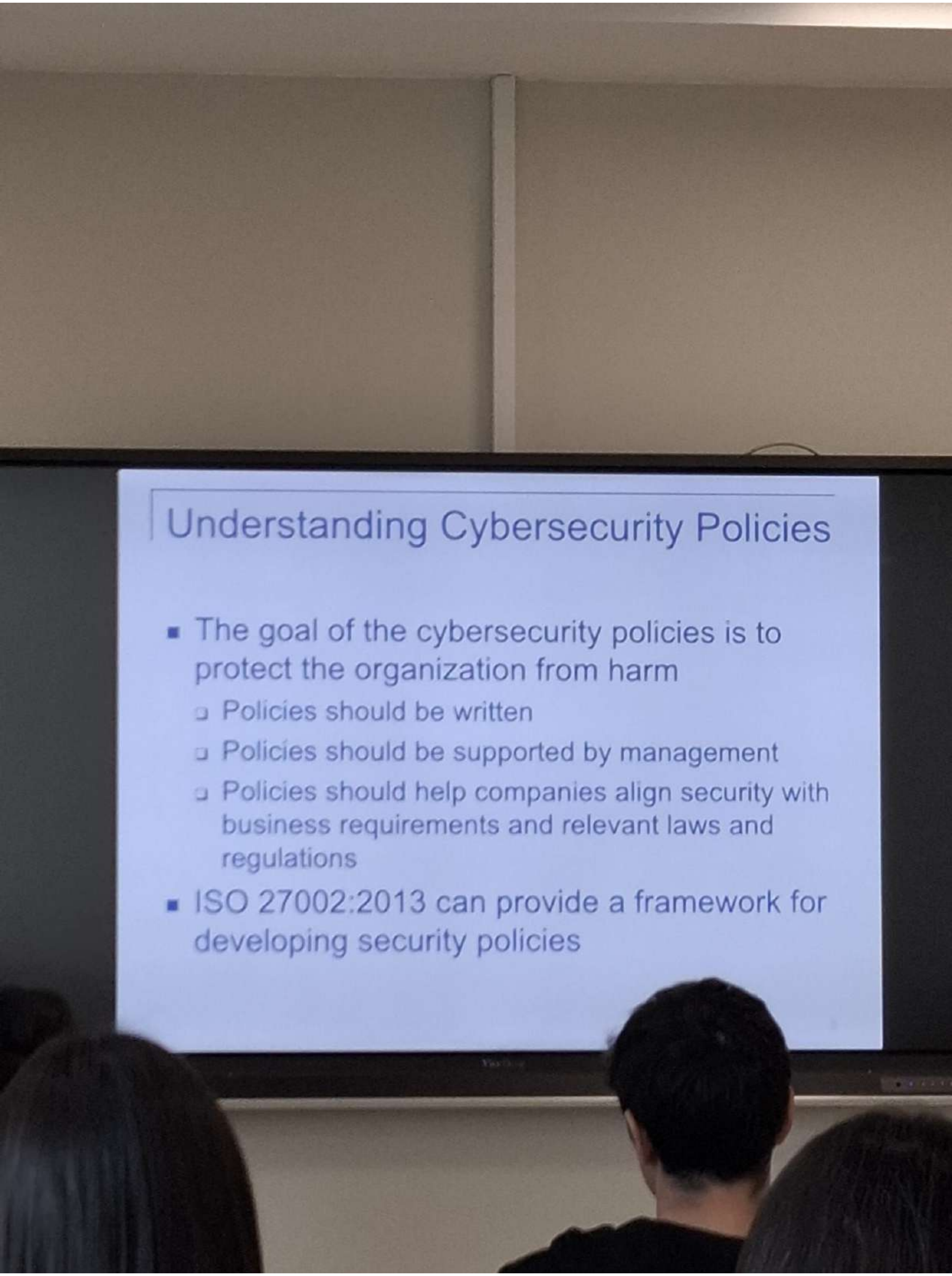
DEVELOPING
CYBERSECURITY
PROGRAMS AND
POLICIES

Chapter 4: Governance and Risk Management



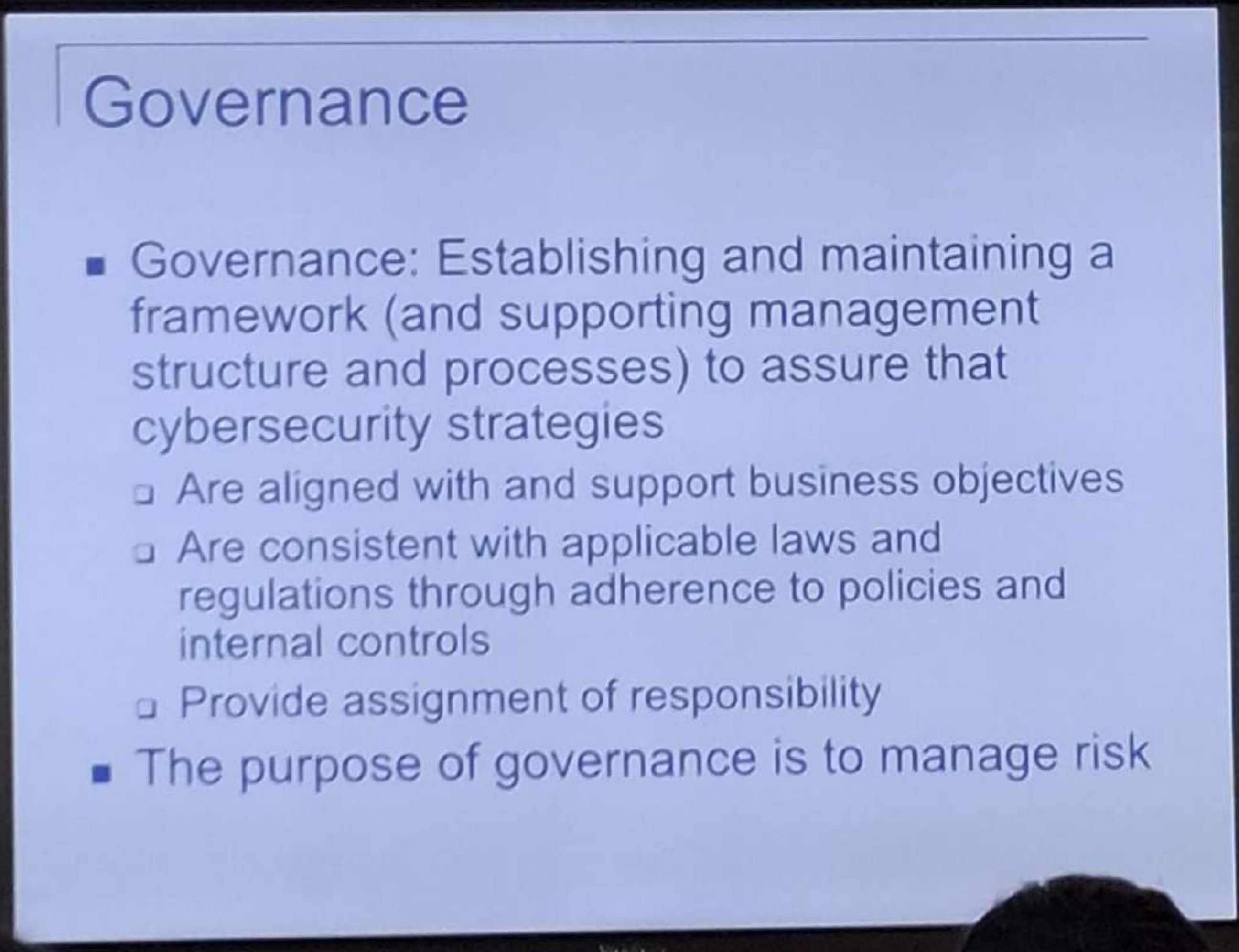
Objectives

- Define governance
- Explain cybersecurity governance and NIST's Cybersecurity Framework
- Explain the importance of strategic alignment
- Know how to manage cybersecurity policies
- Describe cybersecurity-related roles and responsibilities
- Identify the components of risk management
- Create polices related to cybersecurity policy, governance, and risk management



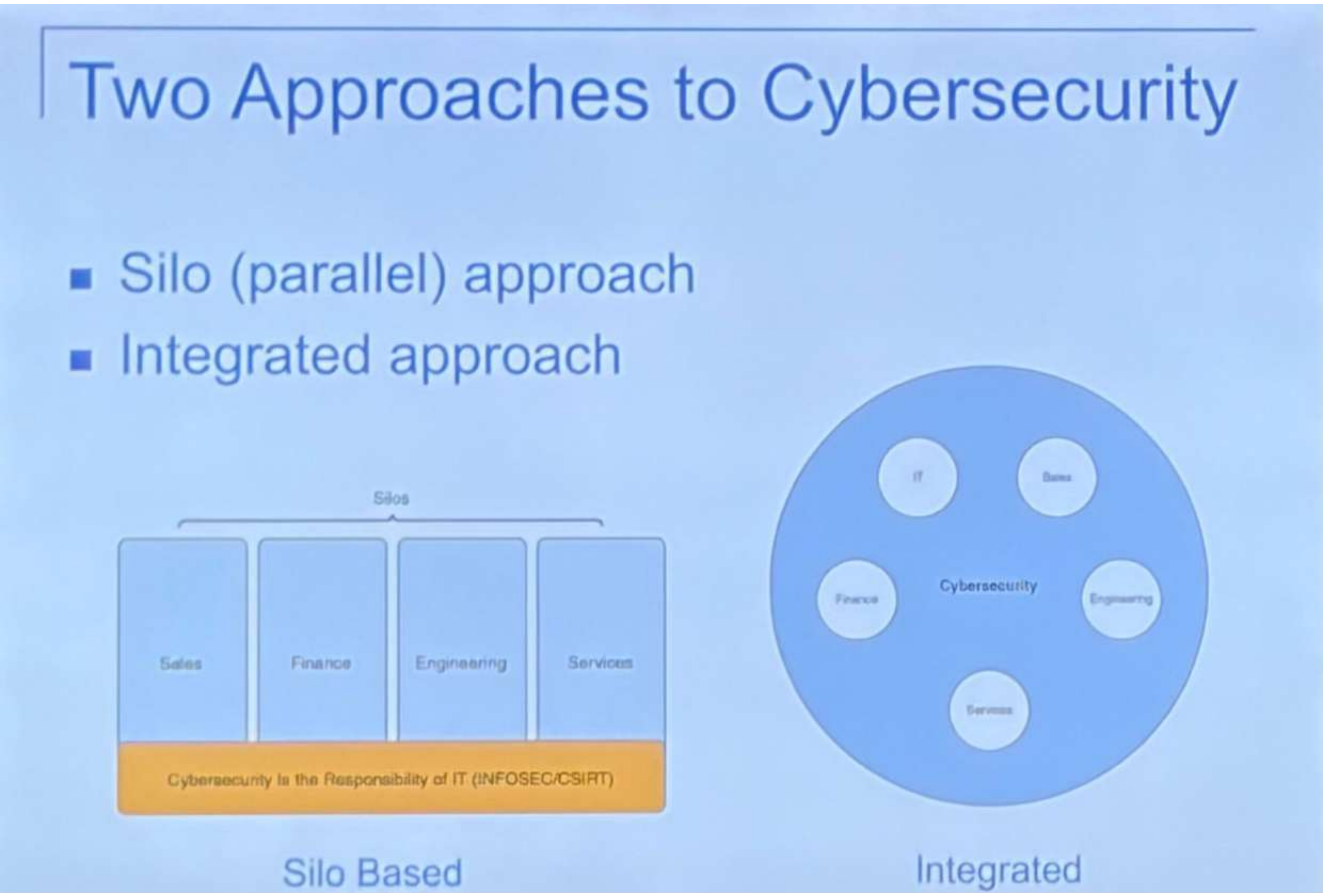
Understanding Cybersecurity Policies

- The goal of the cybersecurity policies is to protect the organization from harm
  - Policies should be written
  - Policies should be supported by management
  - Policies should help companies align security with business requirements and relevant laws and regulations
- ISO 27002:2013 can provide a framework for developing security policies



Governance

- Governance: Establishing and maintaining a framework (and supporting management structure and processes) to assure that cybersecurity strategies
  - Are aligned with and support business objectives
  - Are consistent with applicable laws and regulations through adherence to policies and internal controls
  - Provide assignment of responsibility
- The purpose of governance is to manage risk



Two Approaches to Cybersecurity

- Silo (parallel) approach
- Integrated approach

Silos

Sales

Finance

Engineering

Services

Cybersecurity Is the Responsibility of IT (INFOSEC/CSIRT)

Silo Based

IT

Sales

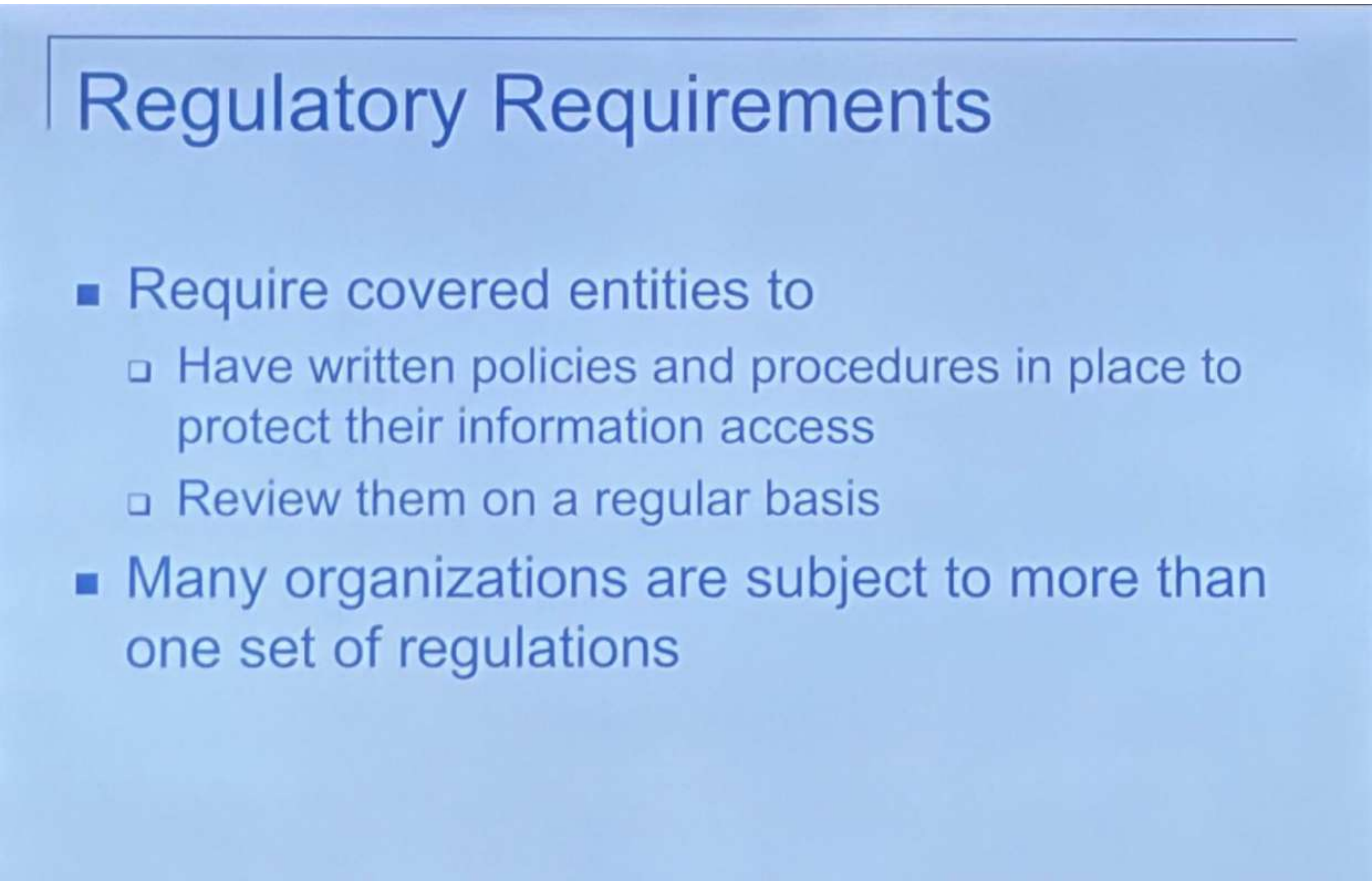
Finance

Cybersecurity

Engineering

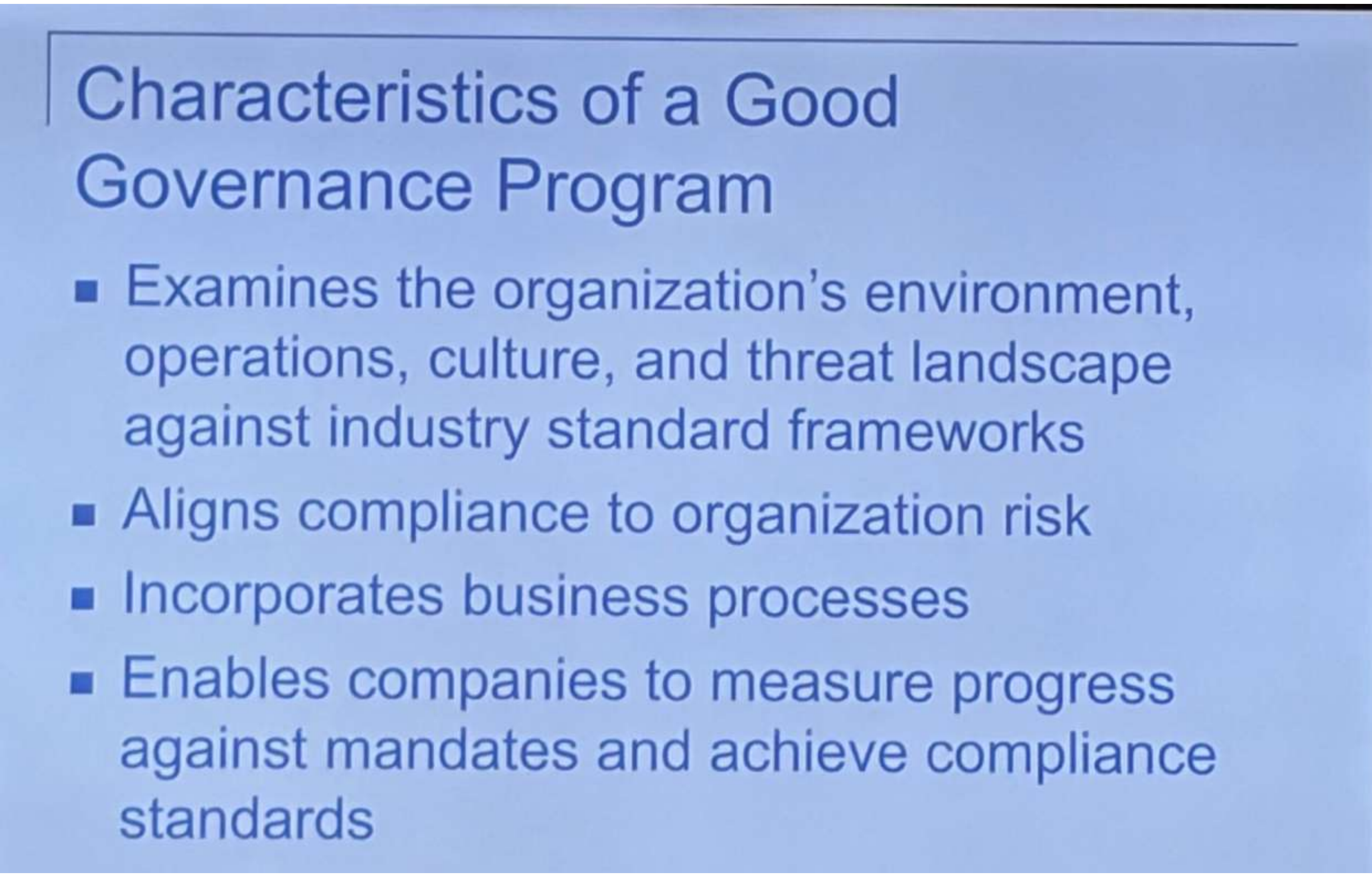
Services

Integrated



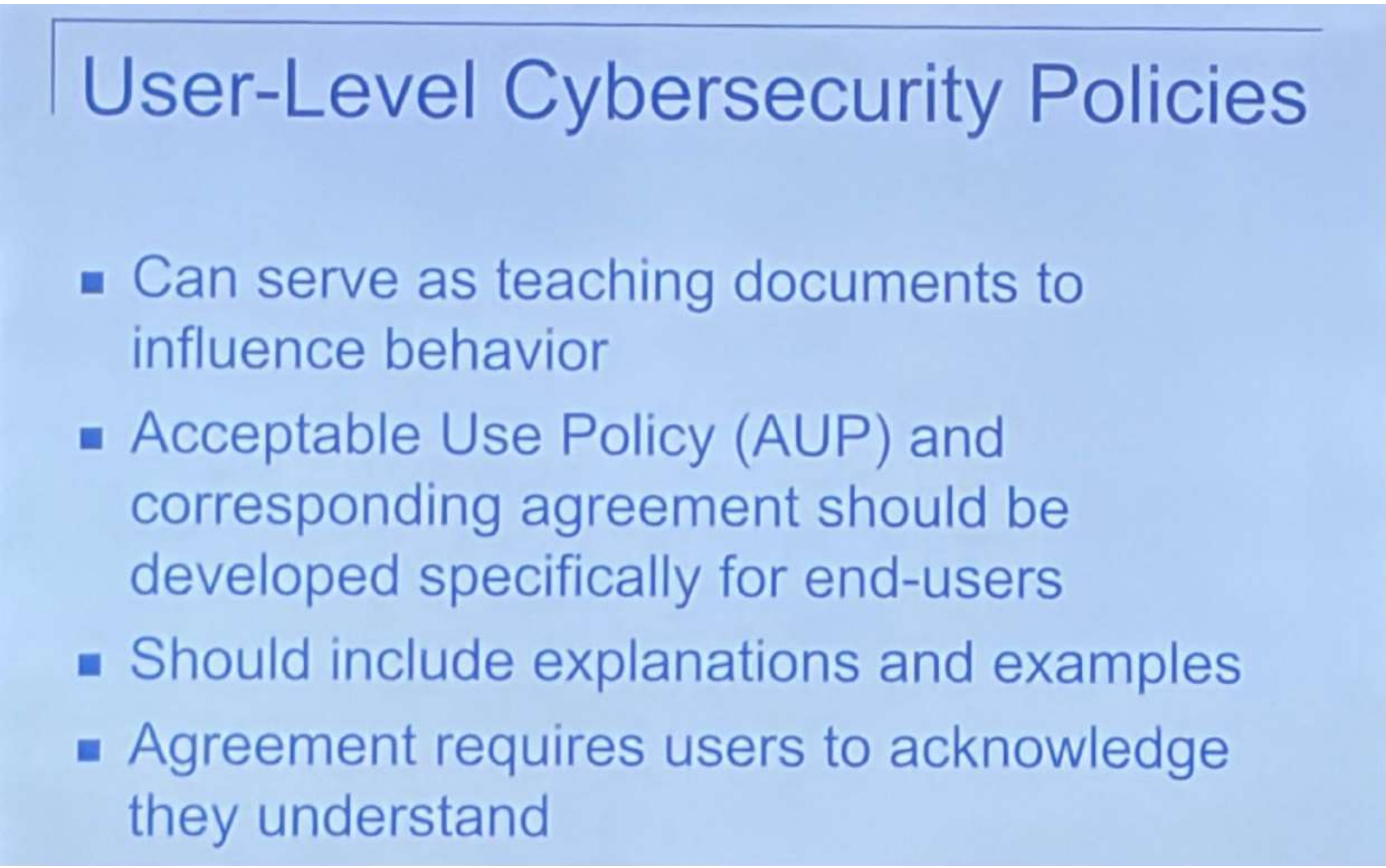
Regulatory Requirements

- Require covered entities to
  - Have written policies and procedures in place to protect their information access
  - Review them on a regular basis
- Many organizations are subject to more than one set of regulations



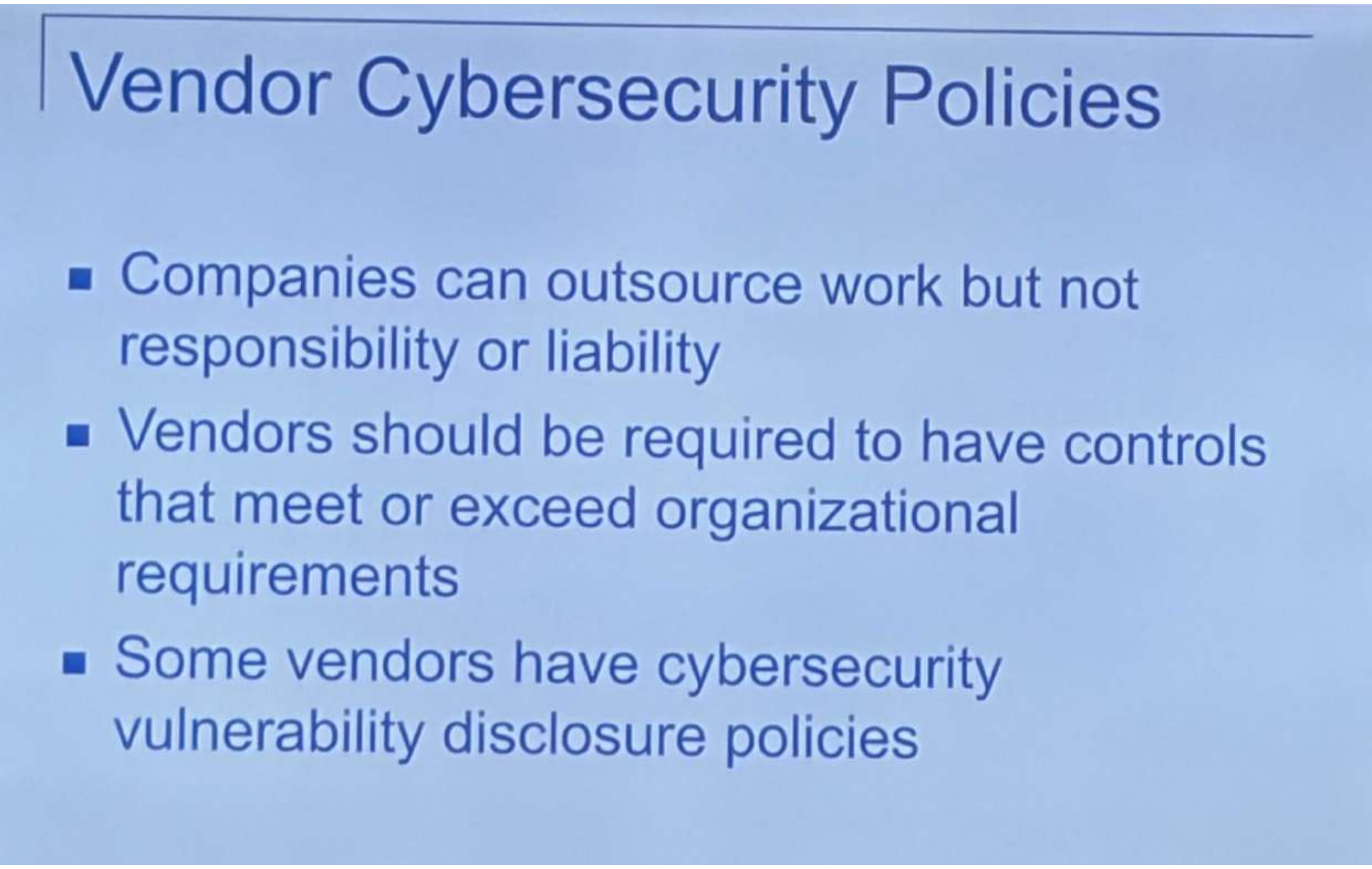
Characteristics of a Good Governance Program

- Examines the organization’s environment, operations, culture, and threat landscape against industry standard frameworks
- Aligns compliance to organization risk
- Incorporates business processes
- Enables companies to measure progress against mandates and achieve compliance standards



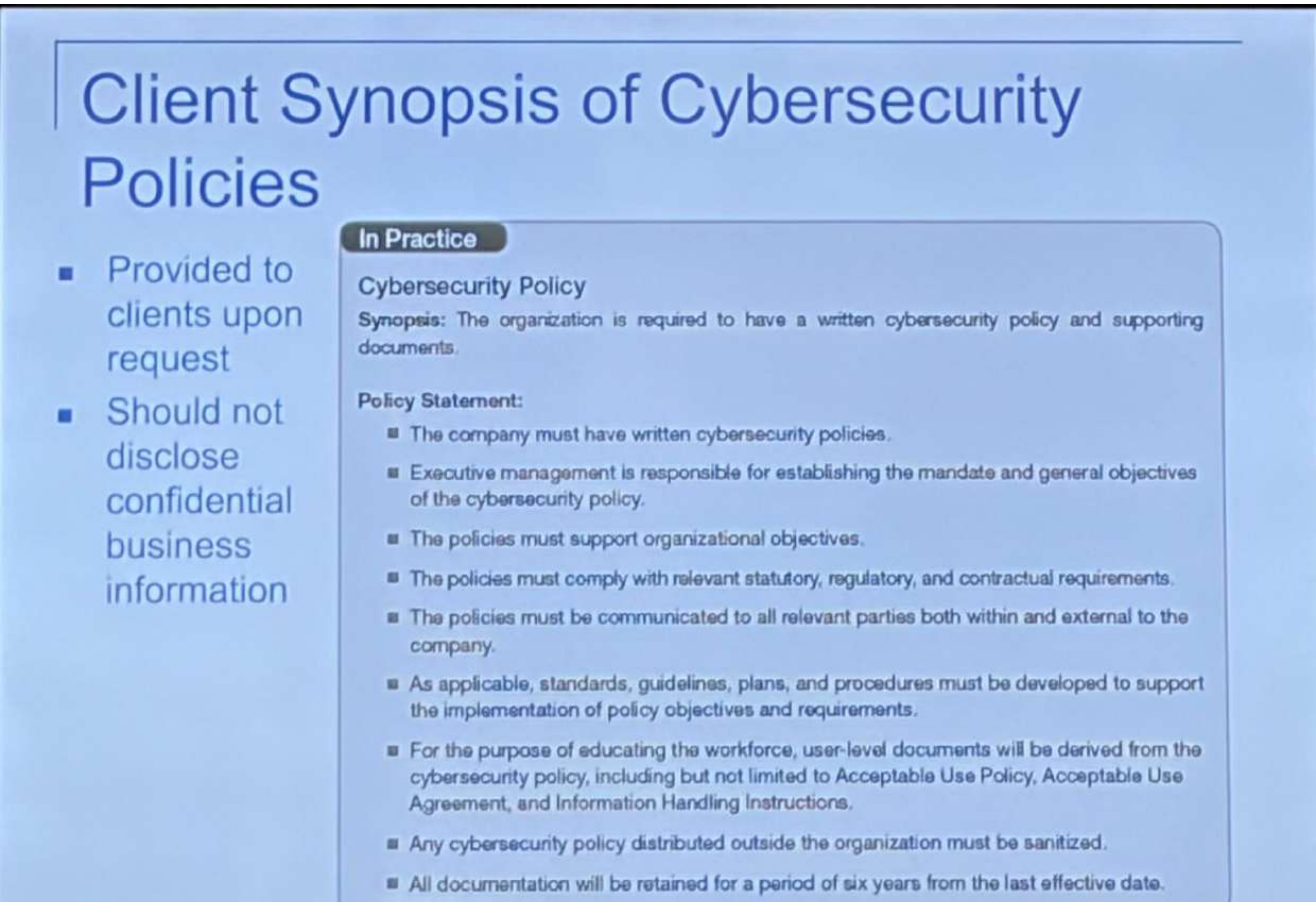
User-Level Cybersecurity Policies

- Can serve as teaching documents to influence behavior
- Acceptable Use Policy (AUP) and corresponding agreement should be developed specifically for end-users
- Should include explanations and examples
- Agreement requires users to acknowledge they understand



Vendor Cybersecurity Policies

- Companies can outsource work but not responsibility or liability
- Vendors should be required to have controls that meet or exceed organizational requirements
- Some vendors have cybersecurity vulnerability disclosure policies



Client Synopsis of Cybersecurity Policies

- Provided to clients upon request
- Should not disclose confidential business information

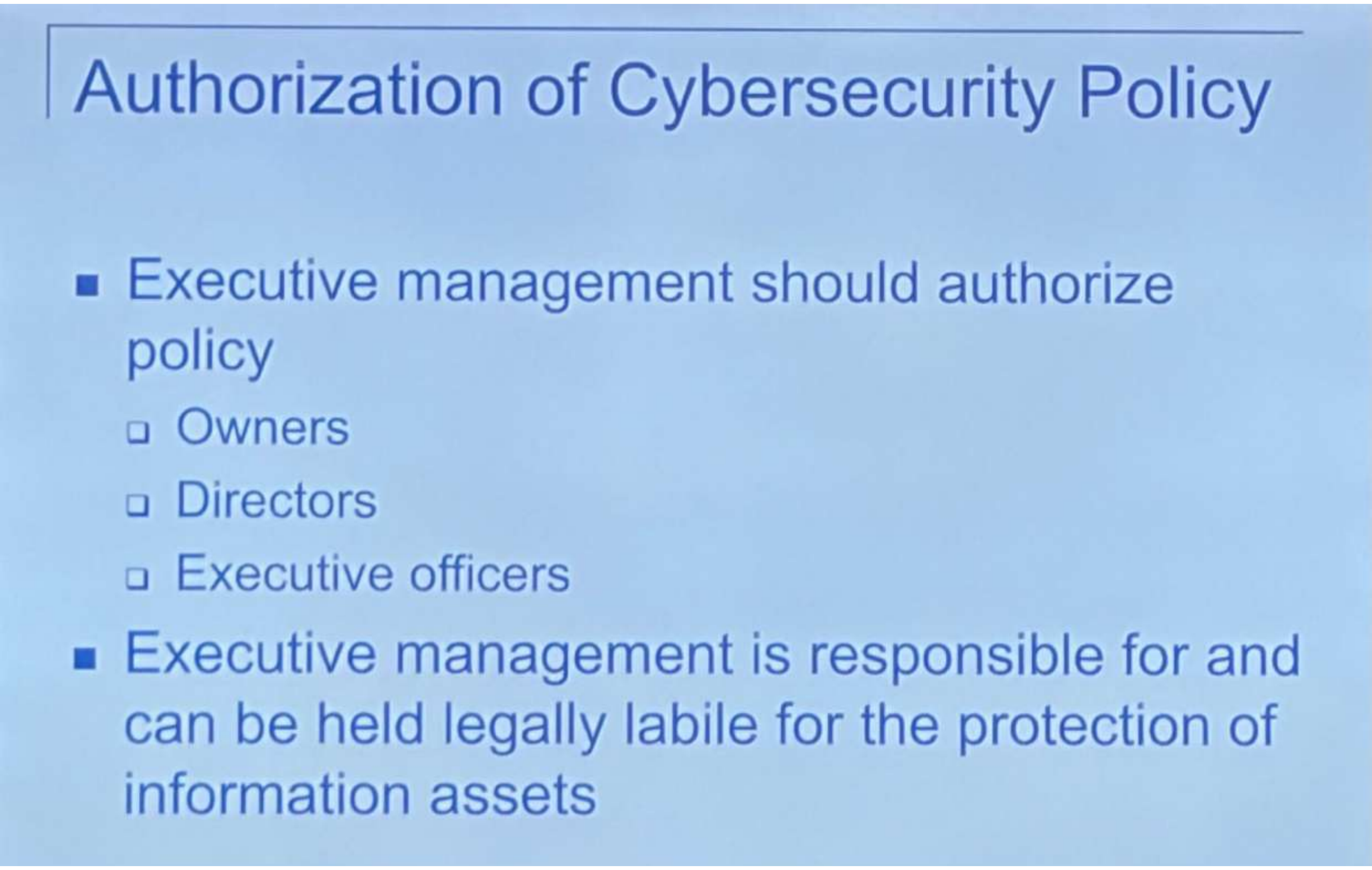
In Practice

Cybersecurity Policy

Synopsis: The organization is required to have a written cybersecurity policy and supporting documents.

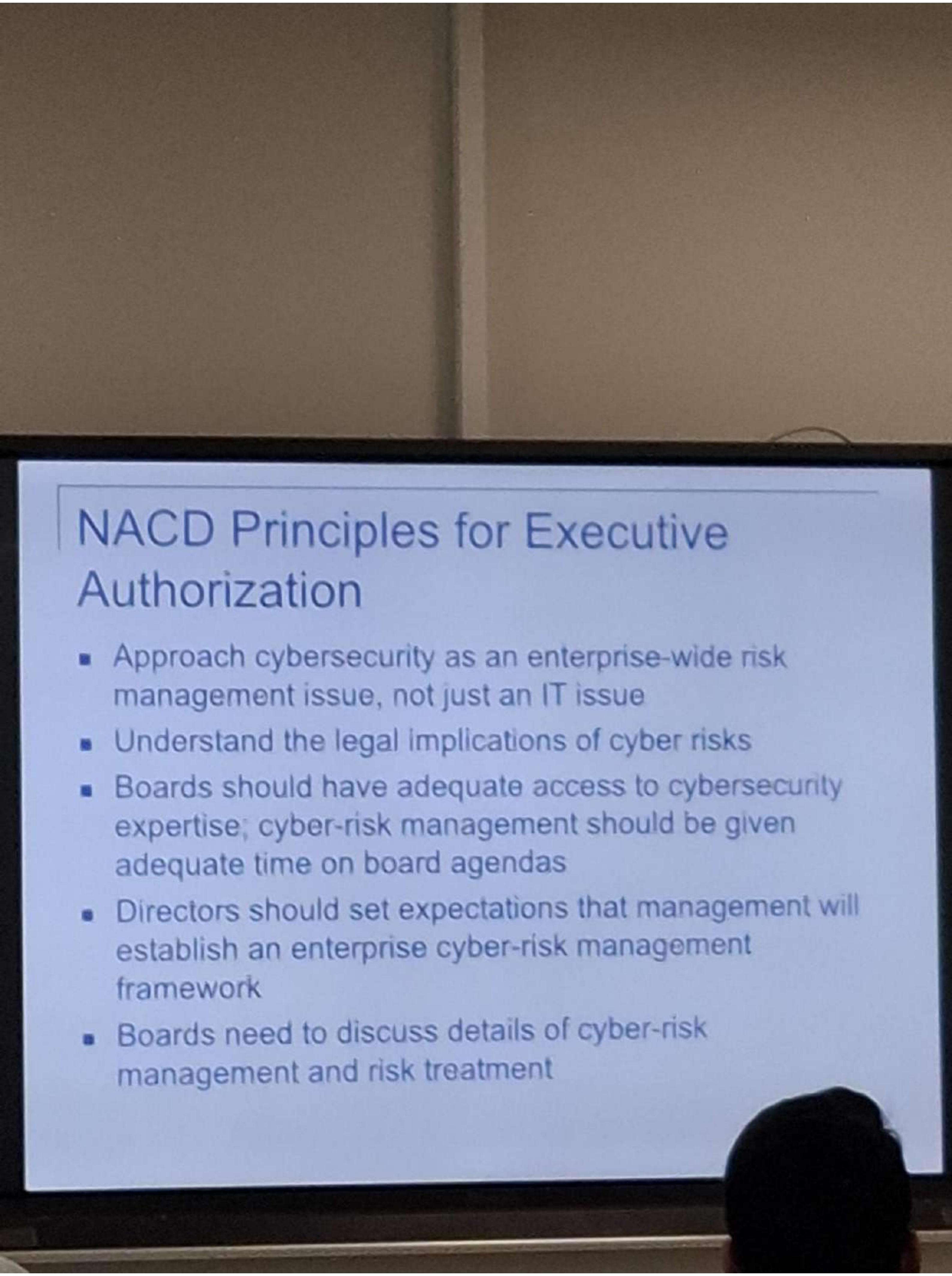
Policy Statement:

- The company must have written cybersecurity policies.
- Executive management is responsible for establishing the mandate and general objectives of the cybersecurity policy.
- The policies must support organizational objectives.
- The policies must comply with relevant statutory, regulatory, and contractual requirements.
- The policies must be communicated to all relevant parties both within and external to the company.
- As applicable, standards, guidelines, plans, and procedures must be developed to support the implementation of policy objectives and requirements.
- For the purpose of educating the workforce, user-level documents will be derived from the cybersecurity policy, including but not limited to Acceptable Use Policy, Acceptable Use Agreement, and Information Handling Instructions.
- Any cybersecurity policy distributed outside the organization must be sanitized.
- All documentation will be retained for a period of six years from the last effective date.



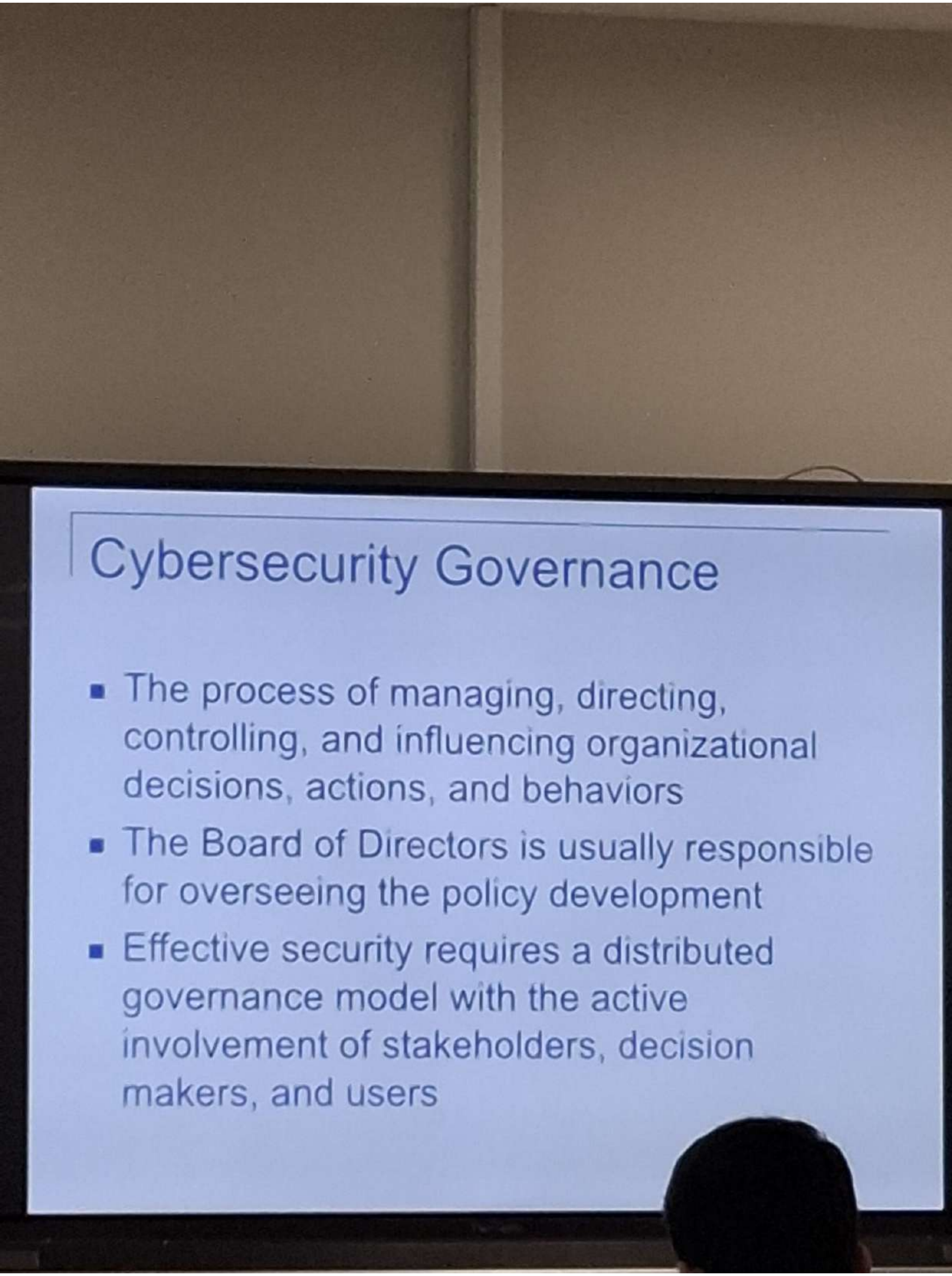
Authorization of Cybersecurity Policy

- Executive management should authorize policy
  - Owners
  - Directors
  - Executive officers
- Executive management is responsible for and can be held legally labile for the protection of information assets



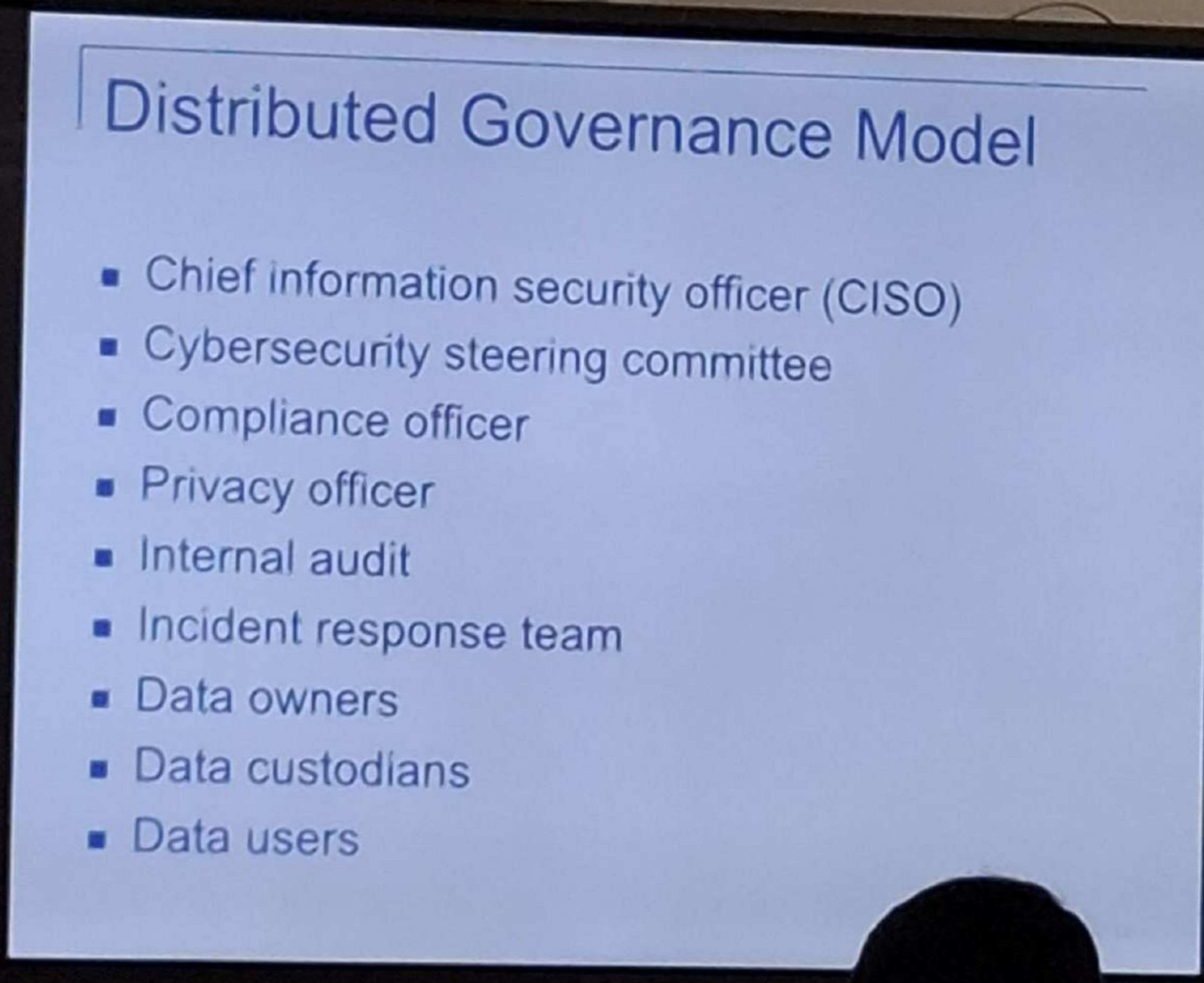
NACD Principles for Executive Authorization

- Approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue
- Understand the legal implications of cyber risks
- Boards should have adequate access to cybersecurity expertise; cyber-risk management should be given adequate time on board agendas
- Directors should set expectations that management will establish an enterprise cyber-risk management framework
- Boards need to discuss details of cyber-risk management and risk treatment



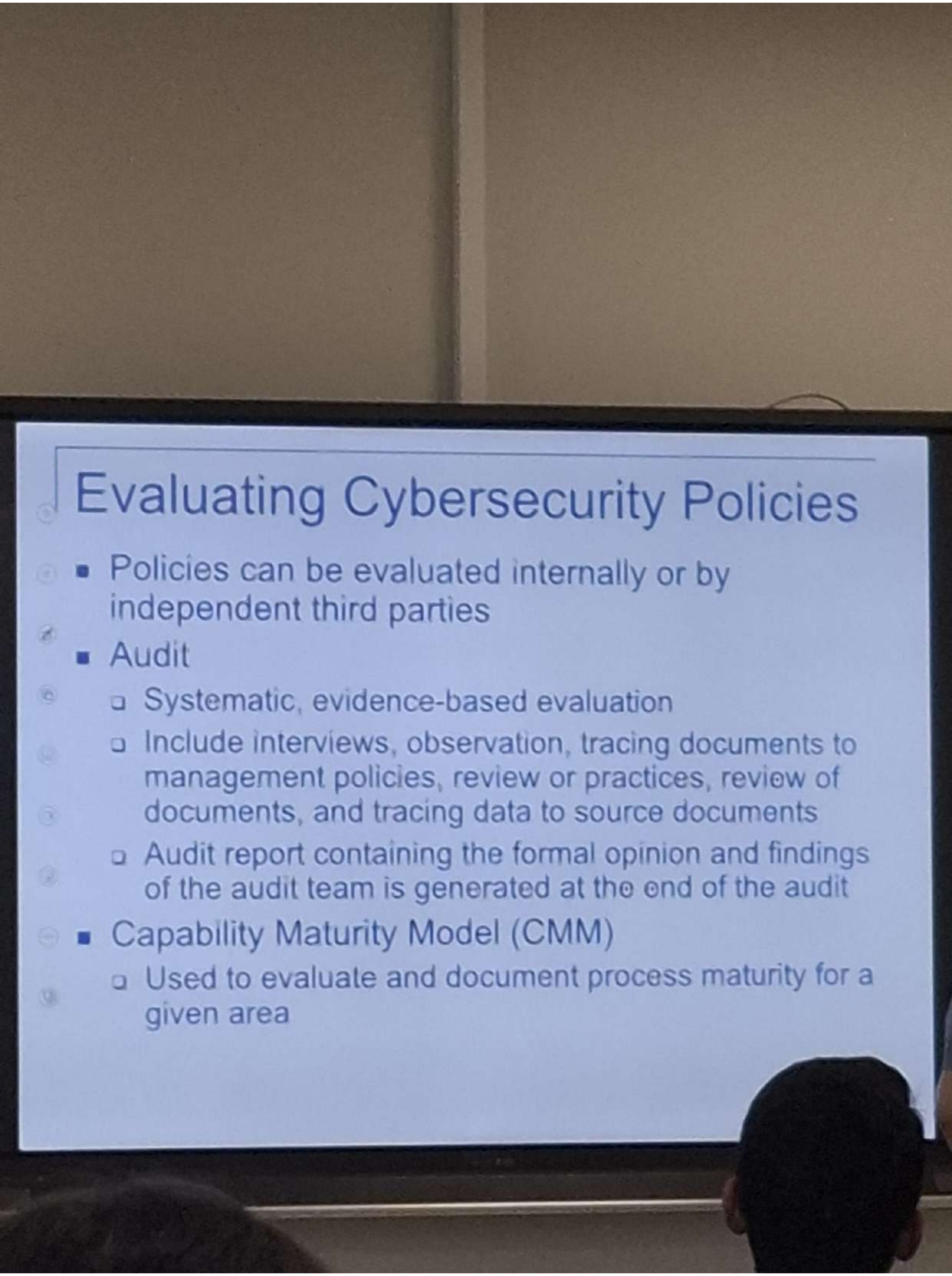
Cybersecurity Governance

- The process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors
- The Board of Directors is usually responsible for overseeing the policy development
- Effective security requires a distributed governance model with the active involvement of stakeholders, decision makers, and users



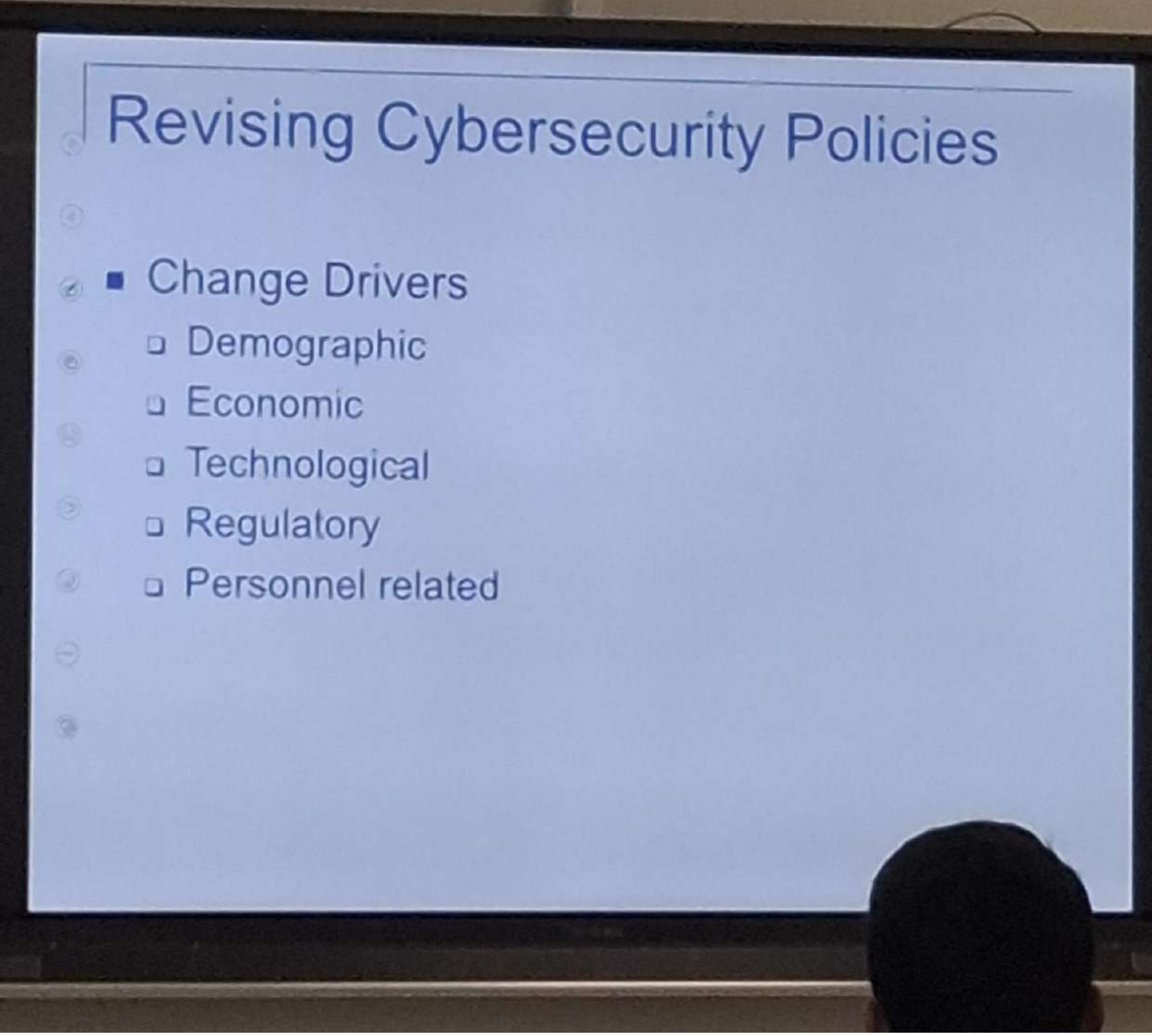
Distributed Governance Model

- Chief information security officer (CISO)
- Cybersecurity steering committee
- Compliance officer
- Privacy officer
- Internal audit
- Incident response team
- Data owners
- Data custodians
- Data users



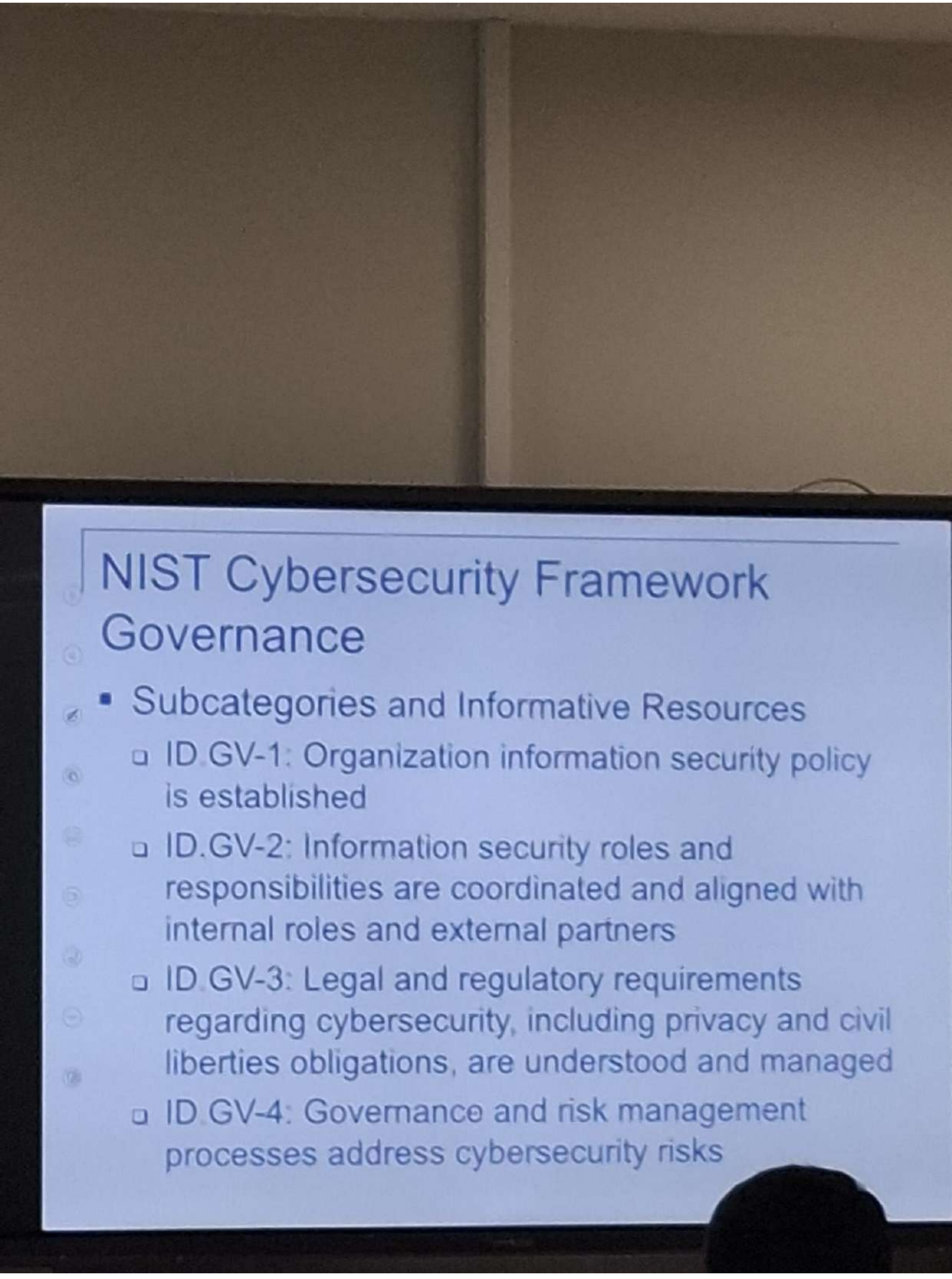
Evaluating Cybersecurity Policies

- Policies can be evaluated internally or by independent third parties
- Audit
  - Systematic, evidence-based evaluation
  - Include interviews, observation, tracing documents to management policies, review or practices, review of documents, and tracing data to source documents
  - Audit report containing the formal opinion and findings of the audit team is generated at the end of the audit
- Capability Maturity Model (CMM)
  - Used to evaluate and document process maturity for a given area



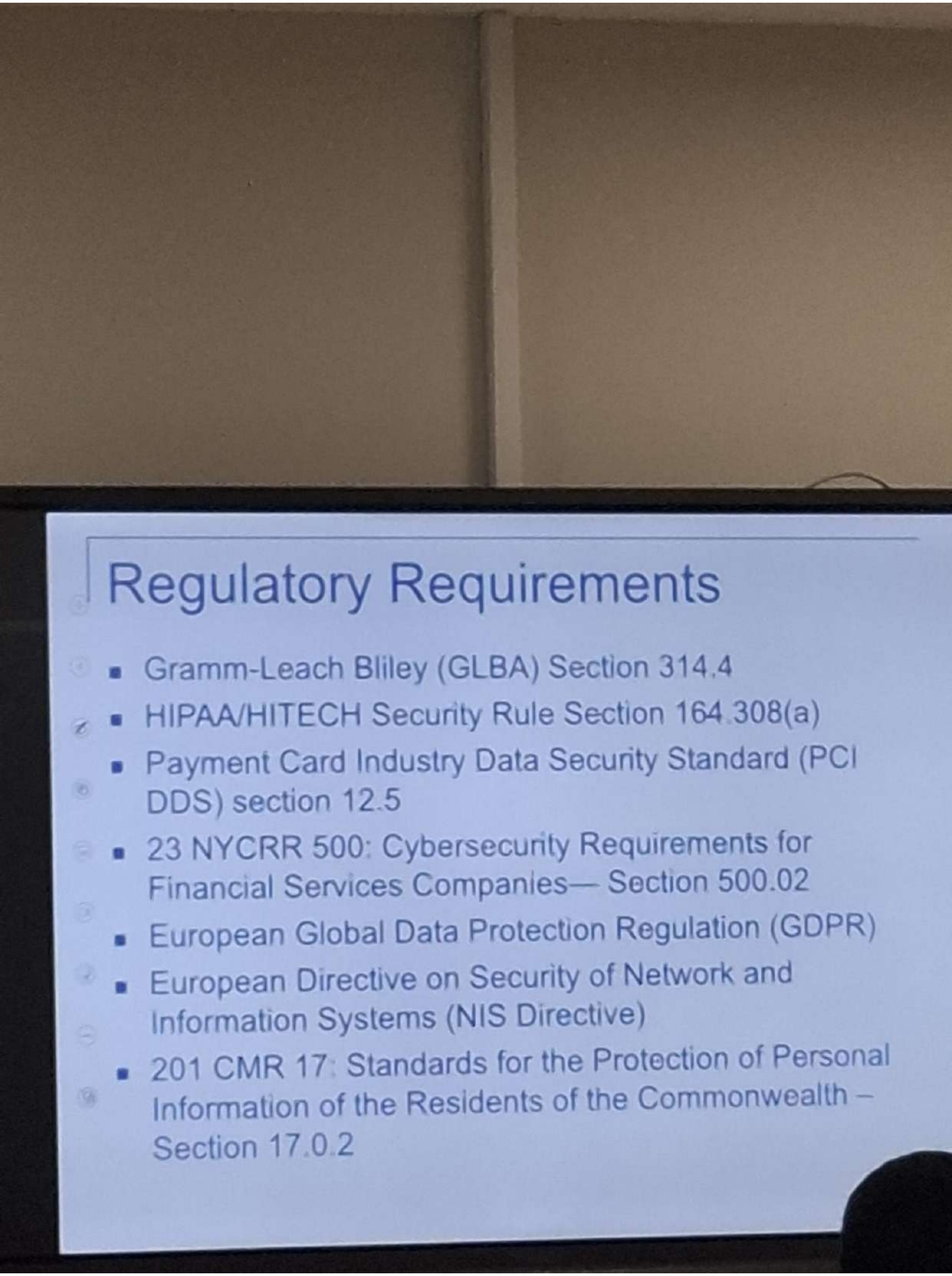
Revising Cybersecurity Policies

- Change Drivers
  - Demographic
  - Economic
  - Technological
  - Regulatory
  - Personnel related



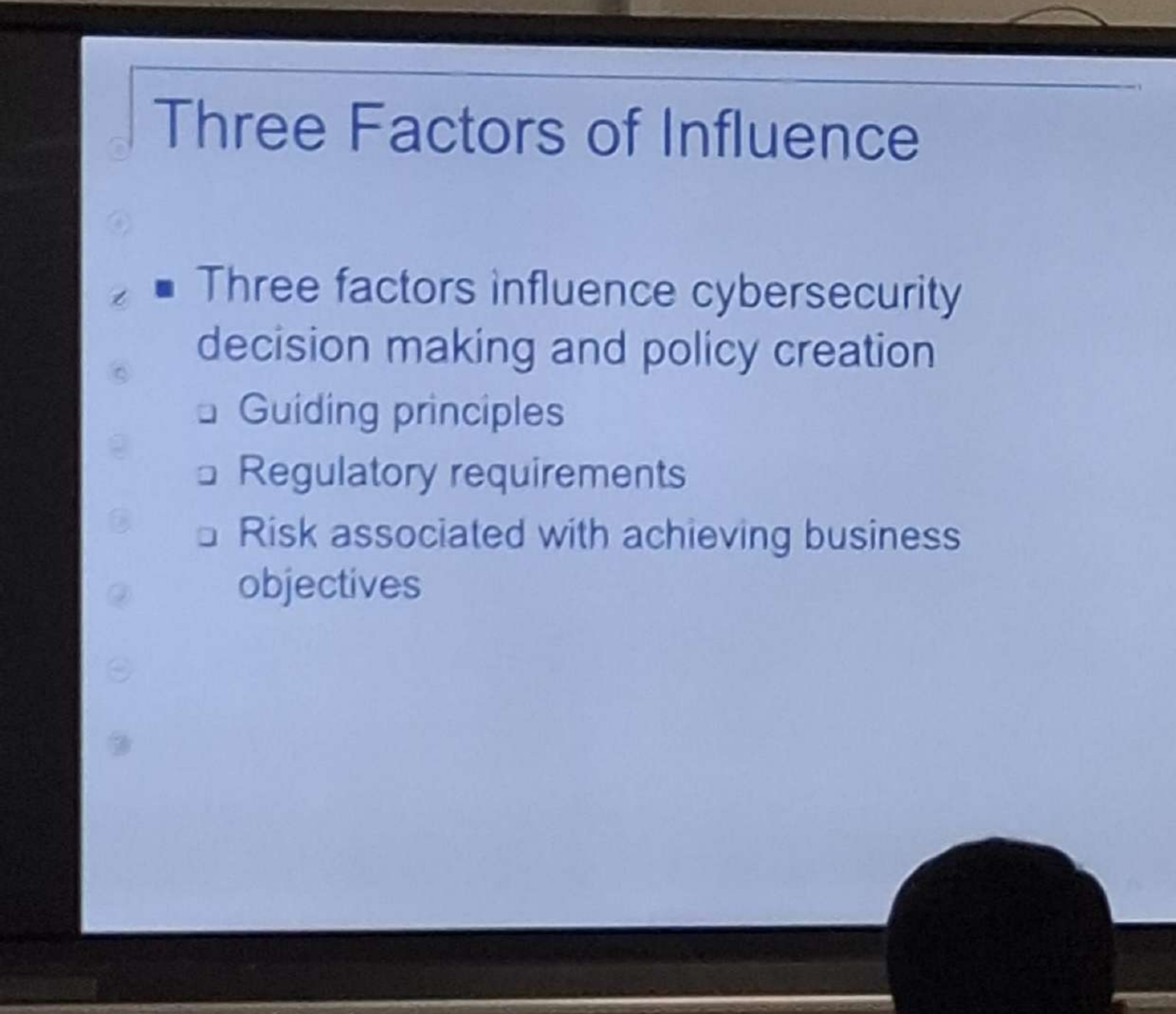
NIST Cybersecurity Framework Governance

- Subcategories and Informative Resources
  - ❑ ID.GV-1: Organization information security policy is established
  - ❑ ID.GV-2: Information security roles and responsibilities are coordinated and aligned with internal roles and external partners
  - ❑ ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
  - ❑ ID.GV-4: Governance and risk management processes address cybersecurity risks



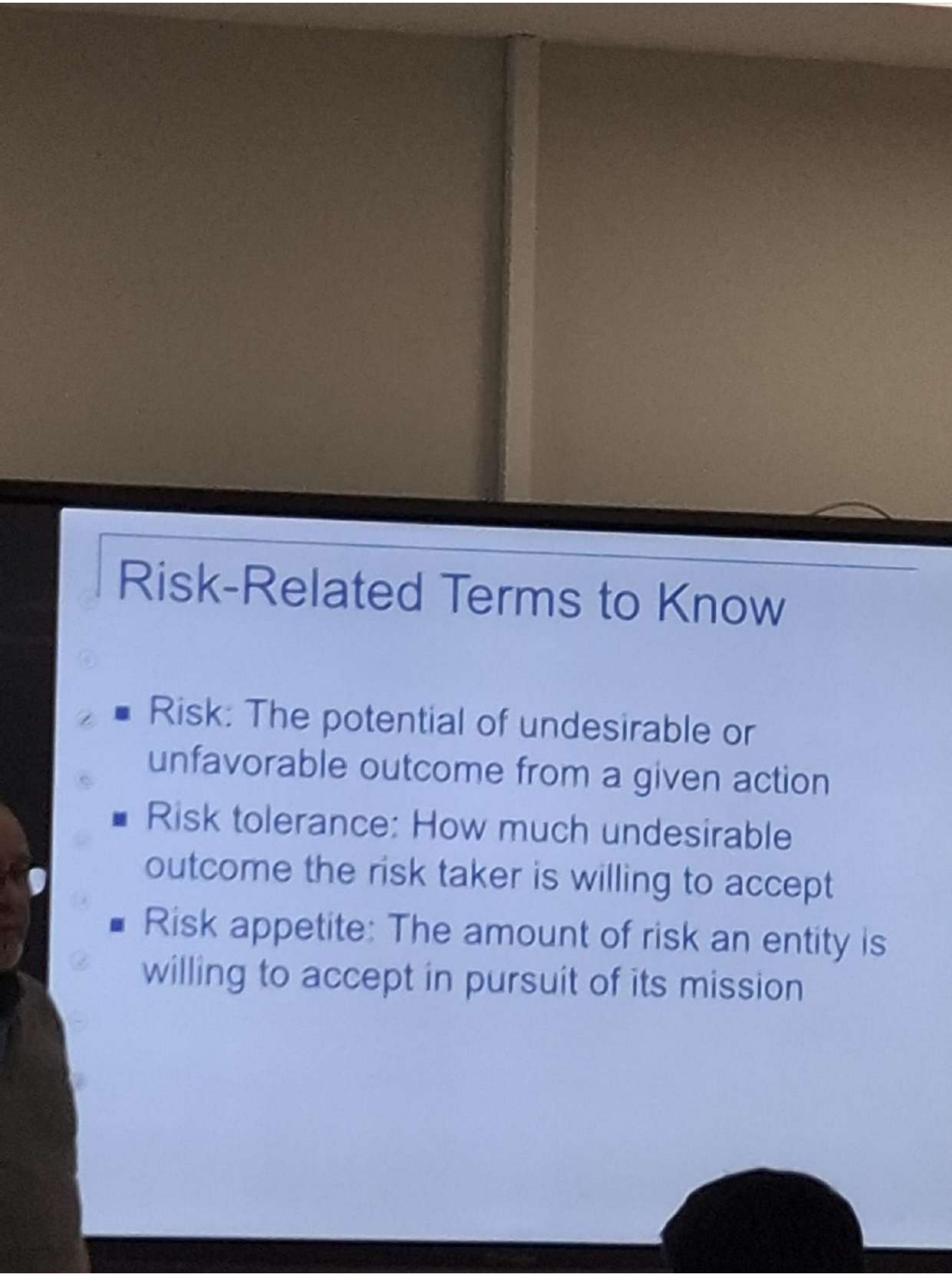
Regulatory Requirements

- Gramm-Leach Bliley (GLBA) Section 314.4
- HIPAA/HITECH Security Rule Section 164.308(a)
- Payment Card Industry Data Security Standard (PCI DDS) section 12.5
- 23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies— Section 500.02
- European Global Data Protection Regulation (GDPR)
- European Directive on Security of Network and Information Systems (NIS Directive)
- 201 CMR 17: Standards for the Protection of Personal Information of the Residents of the Commonwealth – Section 17.0.2



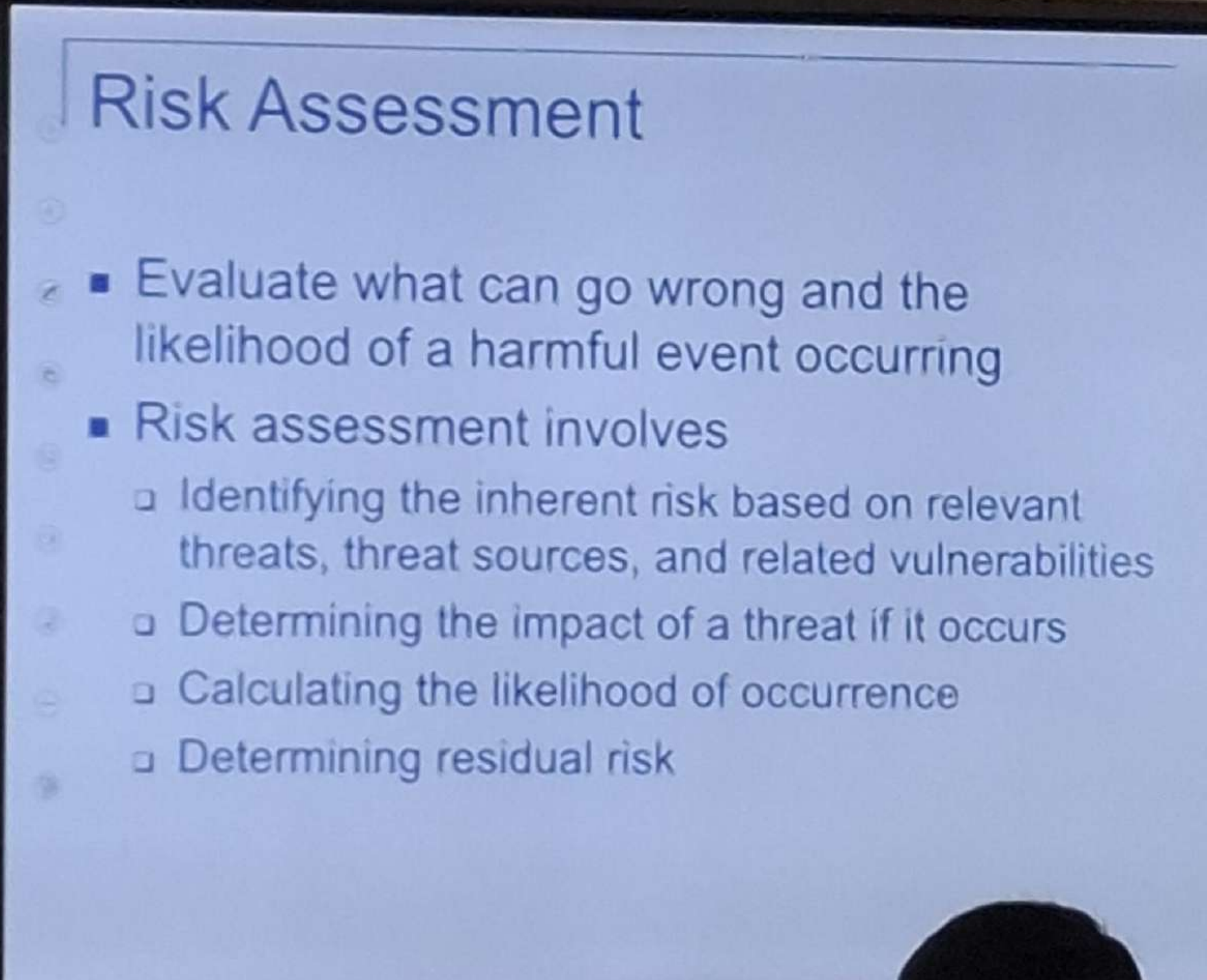
Three Factors of Influence

- Three factors influence cybersecurity decision making and policy creation
  - Guiding principles
  - Regulatory requirements
  - Risk associated with achieving business objectives



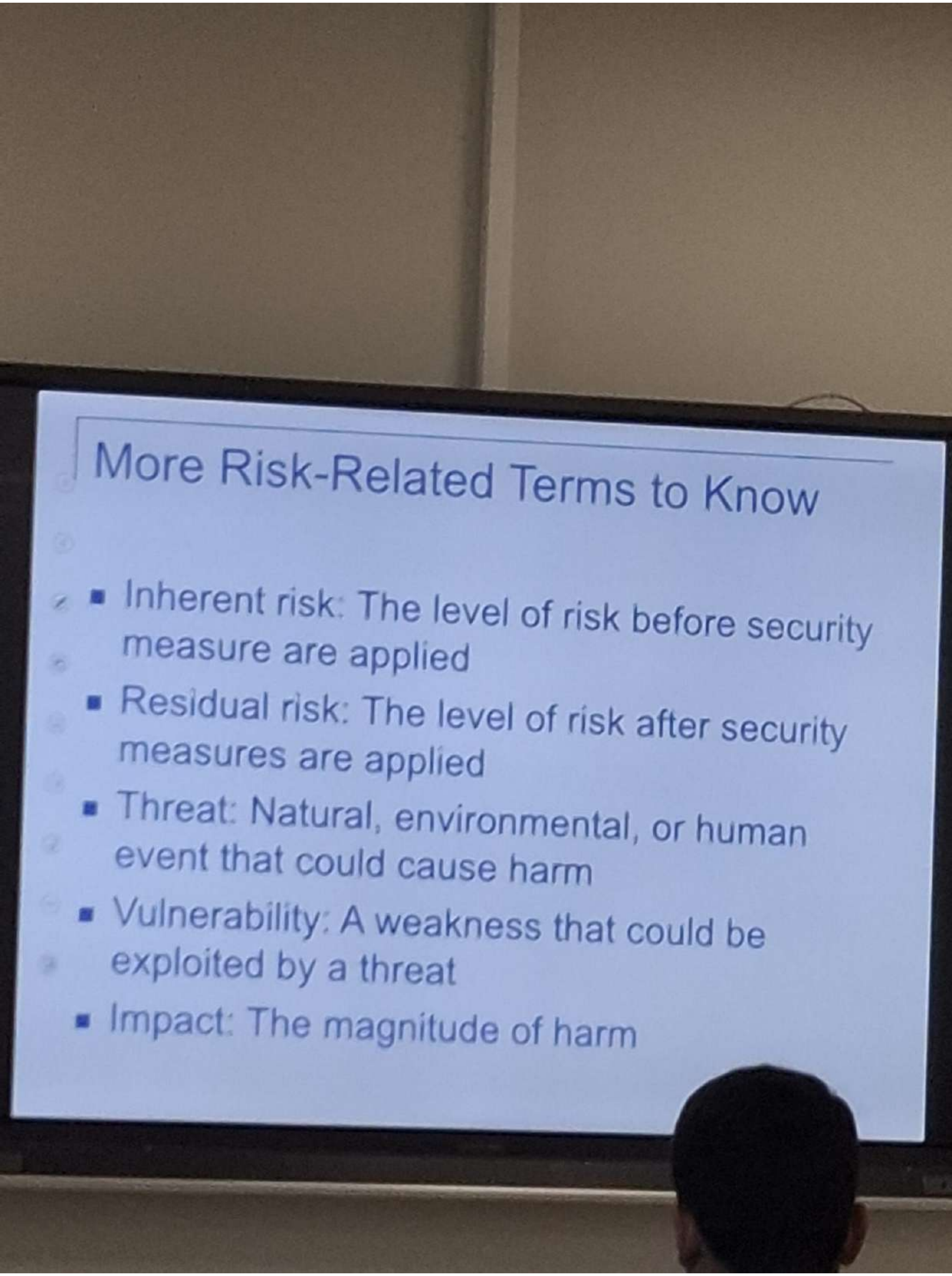
Risk-Related Terms to Know

- Risk: The potential of undesirable or unfavorable outcome from a given action
- Risk tolerance: How much undesirable outcome the risk taker is willing to accept
- Risk appetite: The amount of risk an entity is willing to accept in pursuit of its mission



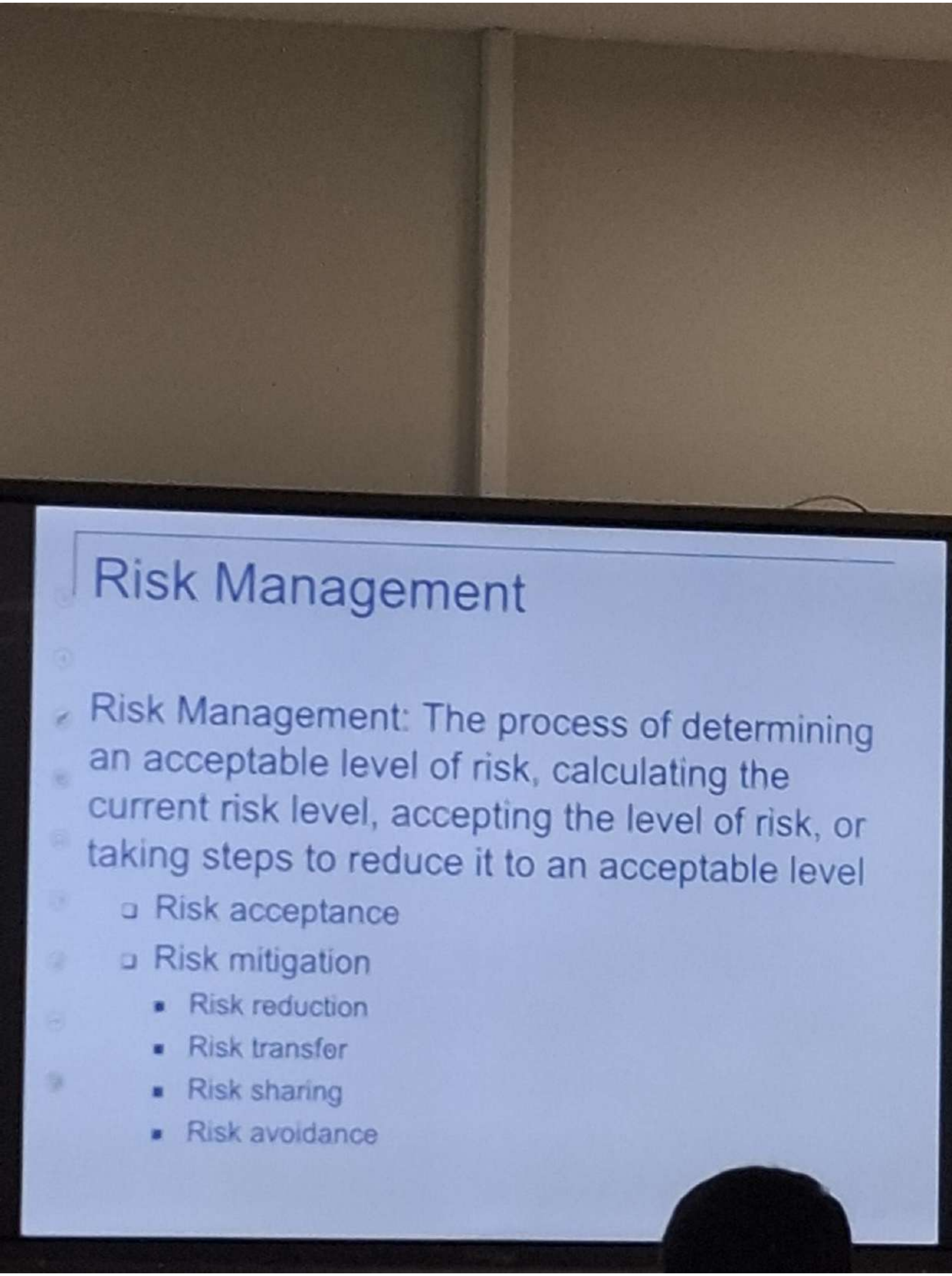
Risk Assessment

- Evaluate what can go wrong and the likelihood of a harmful event occurring
- Risk assessment involves
  - Identifying the inherent risk based on relevant threats, threat sources, and related vulnerabilities
  - Determining the impact of a threat if it occurs
  - Calculating the likelihood of occurrence
  - Determining residual risk



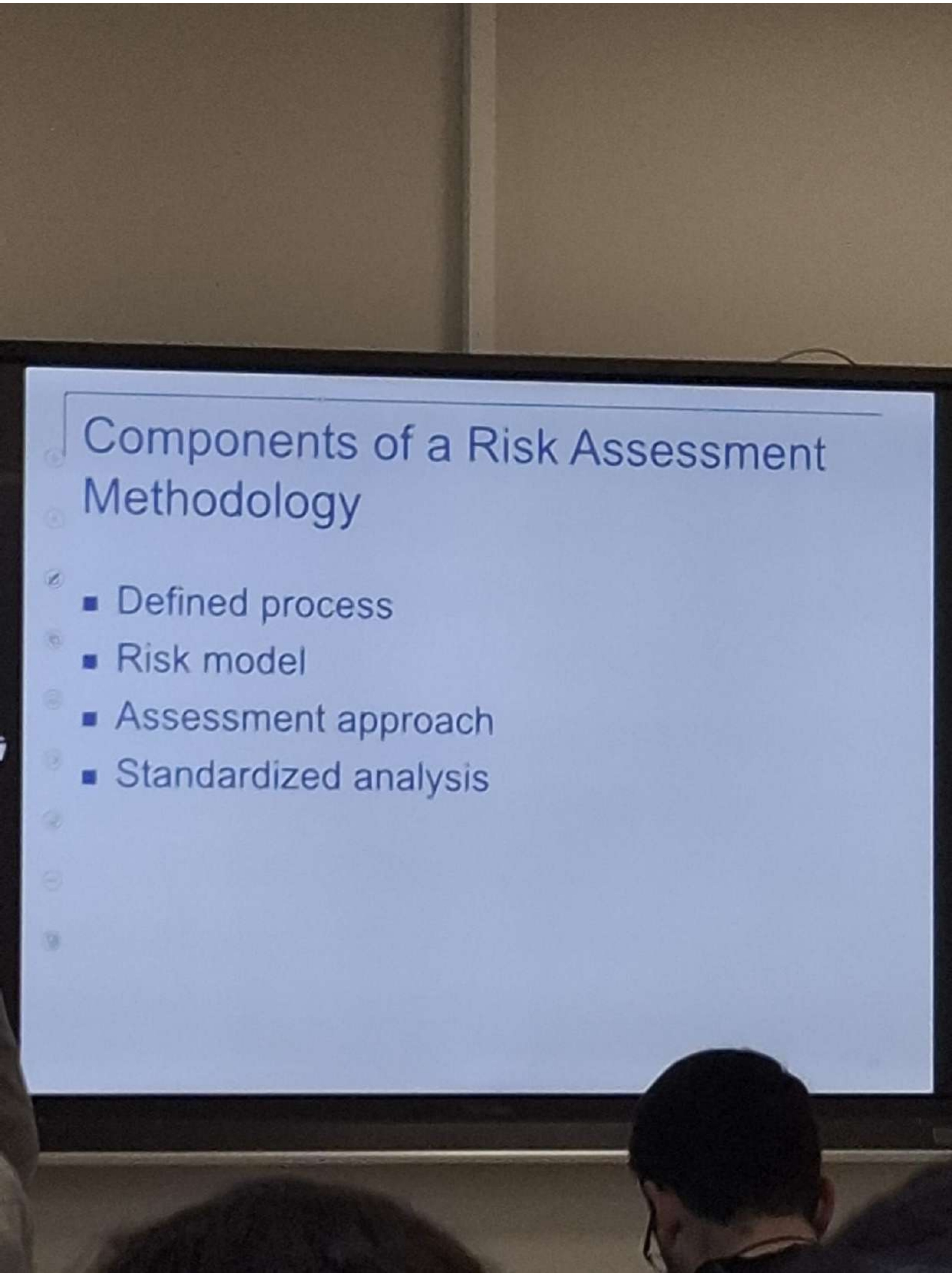
More Risk-Related Terms to Know

- Inherent risk: The level of risk before security measure are applied
- Residual risk: The level of risk after security measures are applied
- Threat: Natural, environmental, or human event that could cause harm
- Vulnerability: A weakness that could be exploited by a threat
- Impact: The magnitude of harm



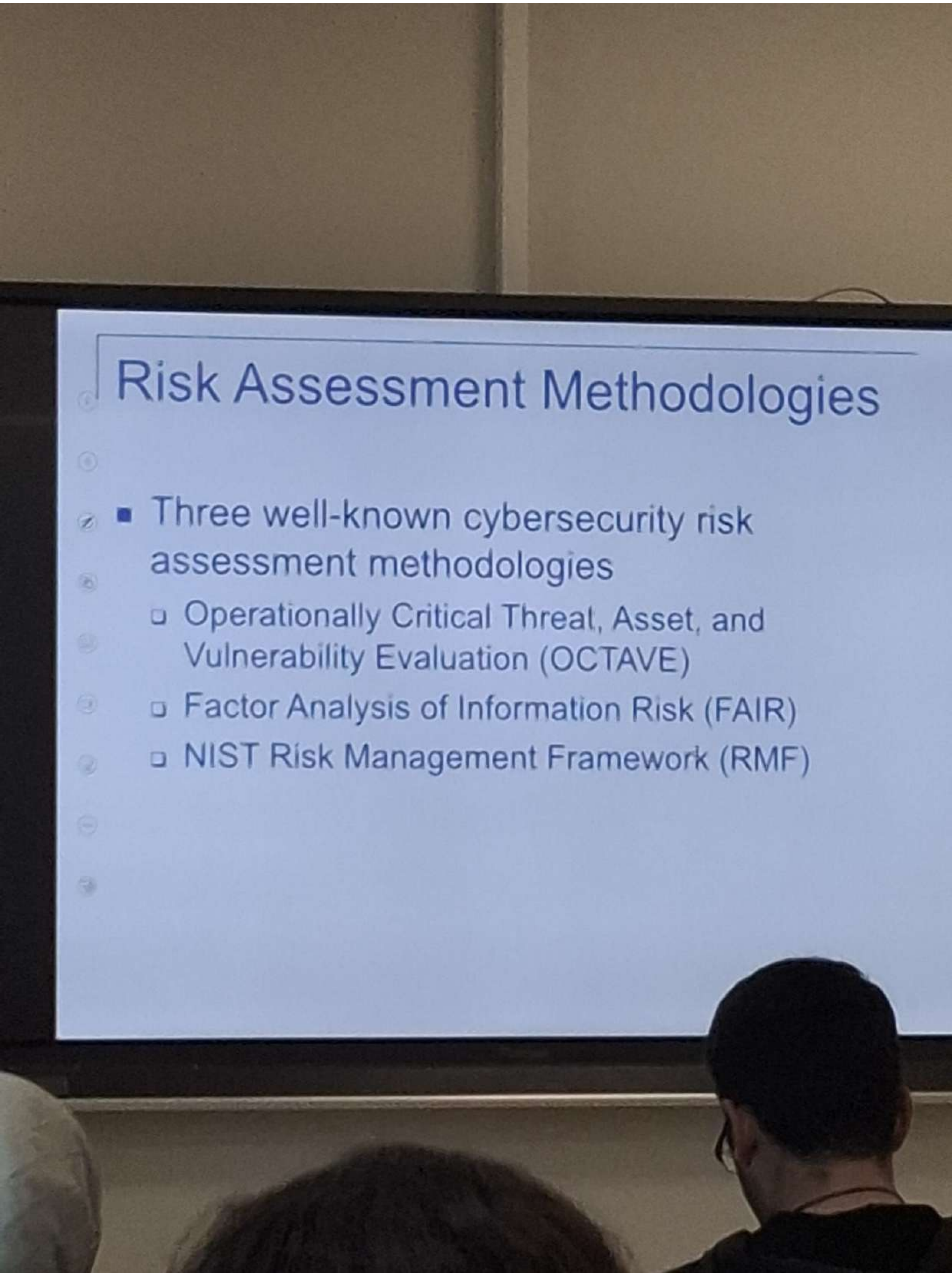
Risk Management

- Risk Management: The process of determining an acceptable level of risk, calculating the current risk level, accepting the level of risk, or taking steps to reduce it to an acceptable level
  - Risk acceptance
  - Risk mitigation
    - Risk reduction
    - Risk transfer
    - Risk sharing
    - Risk avoidance



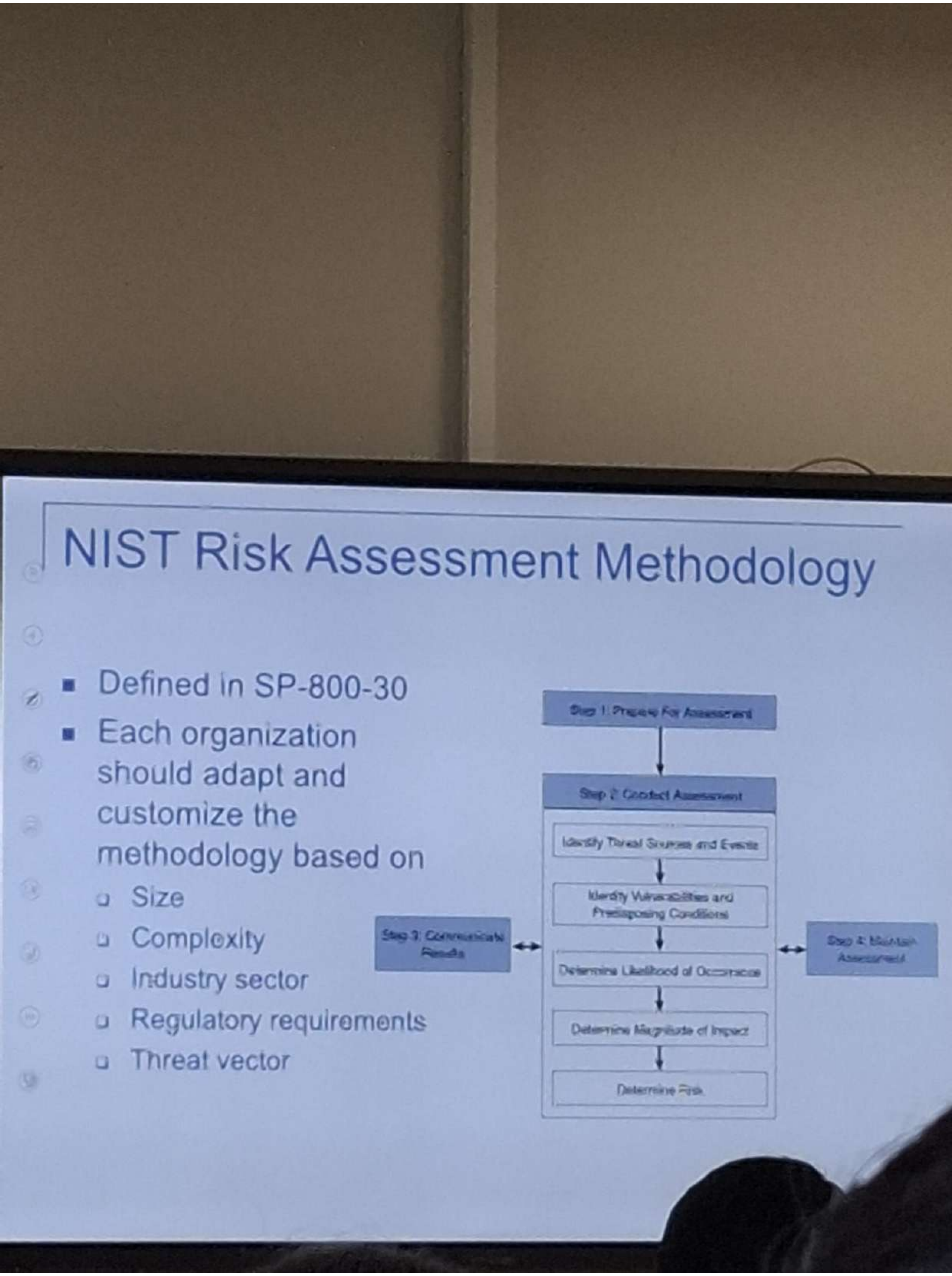
Components of a Risk Assessment Methodology

- Defined process
- Risk model
- Assessment approach
- Standardized analysis



Risk Assessment Methodologies

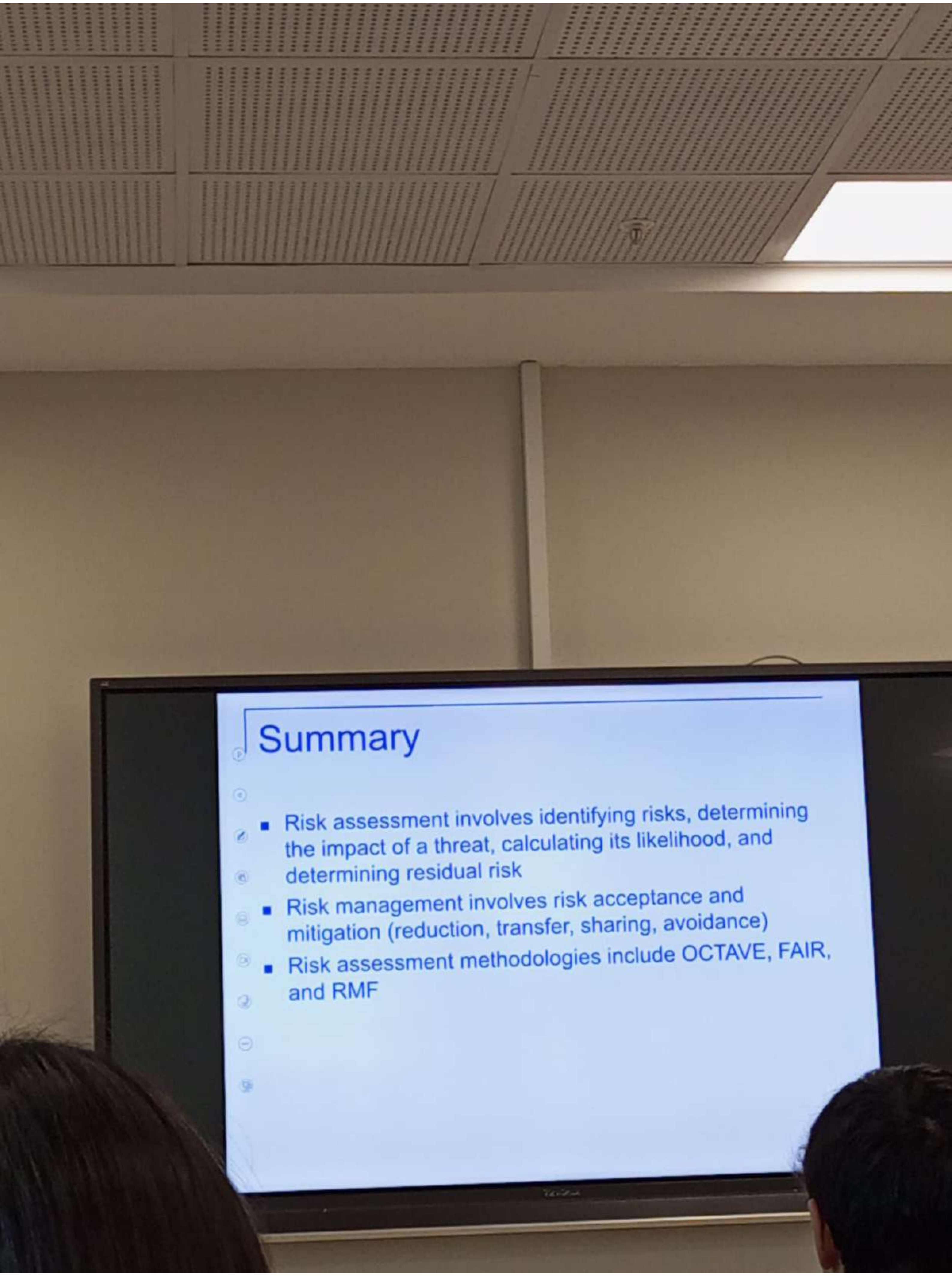
- Three well-known cybersecurity risk assessment methodologies
  - Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
  - Factor Analysis of Information Risk (FAIR)
  - NIST Risk Management Framework (RMF)



NIST Risk Assessment Methodology

- Defined in SP-800-30
- Each organization should adapt and customize the methodology based on
  - Size
  - Complexity
  - Industry sector
  - Regulatory requirements
  - Threat vector

Step 1: Prepare For Assessment
Step 2: Conduct Assessment
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment



Summary

- Risk assessment involves identifying risks, determining the impact of a threat, calculating its likelihood, and determining residual risk
- Risk management involves risk acceptance and mitigation (reduction, transfer, sharing, avoidance)
- Risk assessment methodologies include OCTAVE, FAIR, and RMF