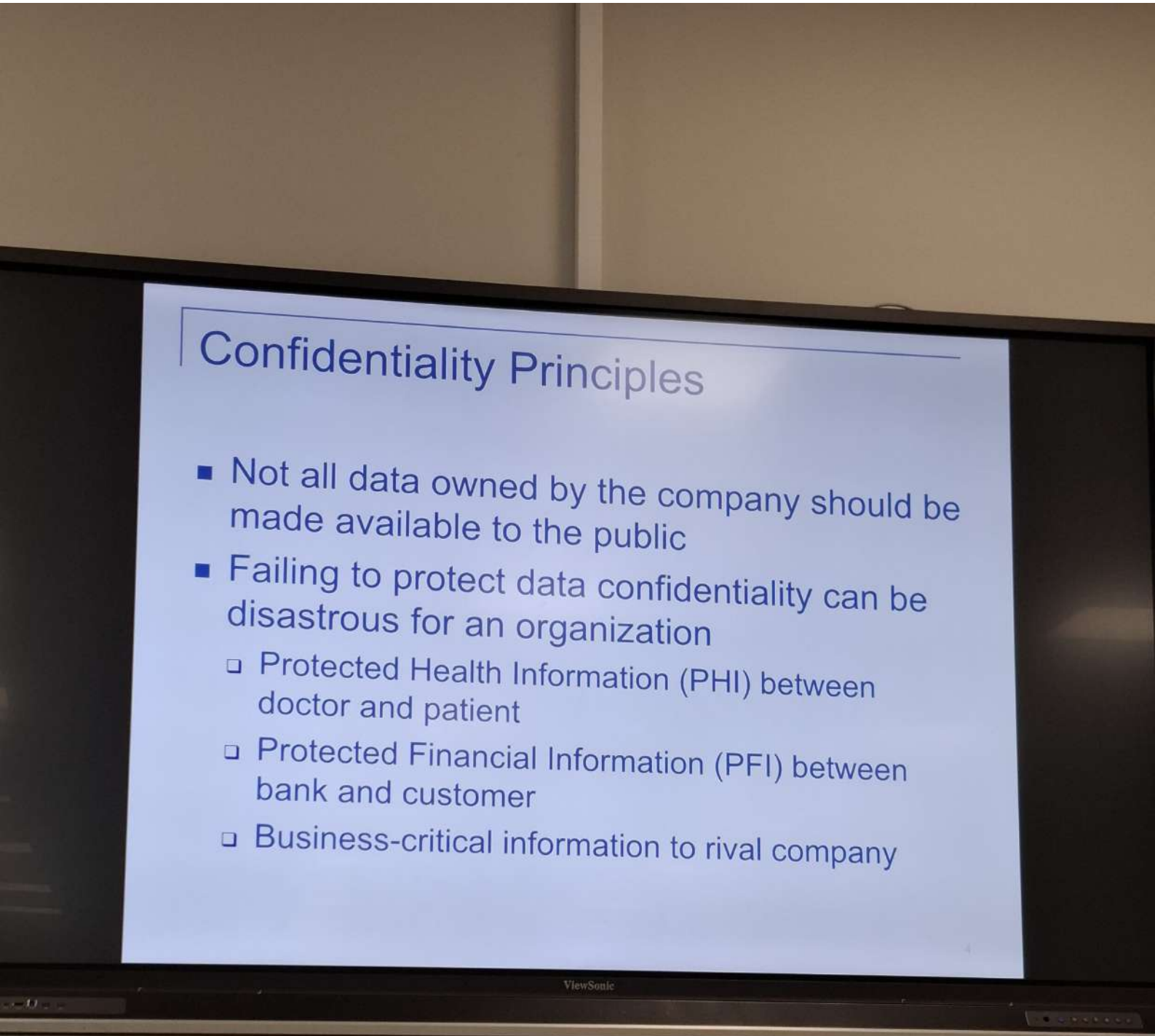
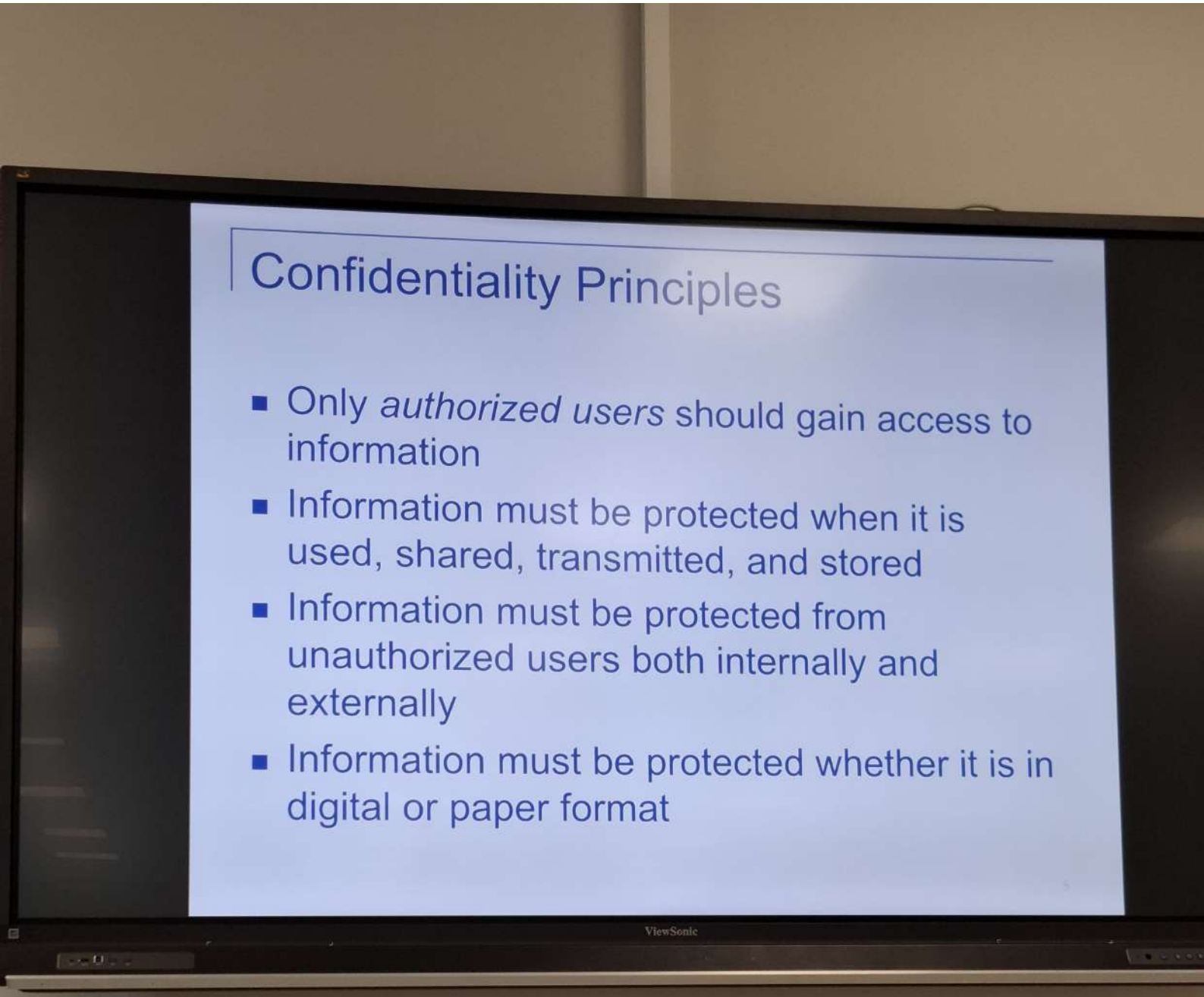
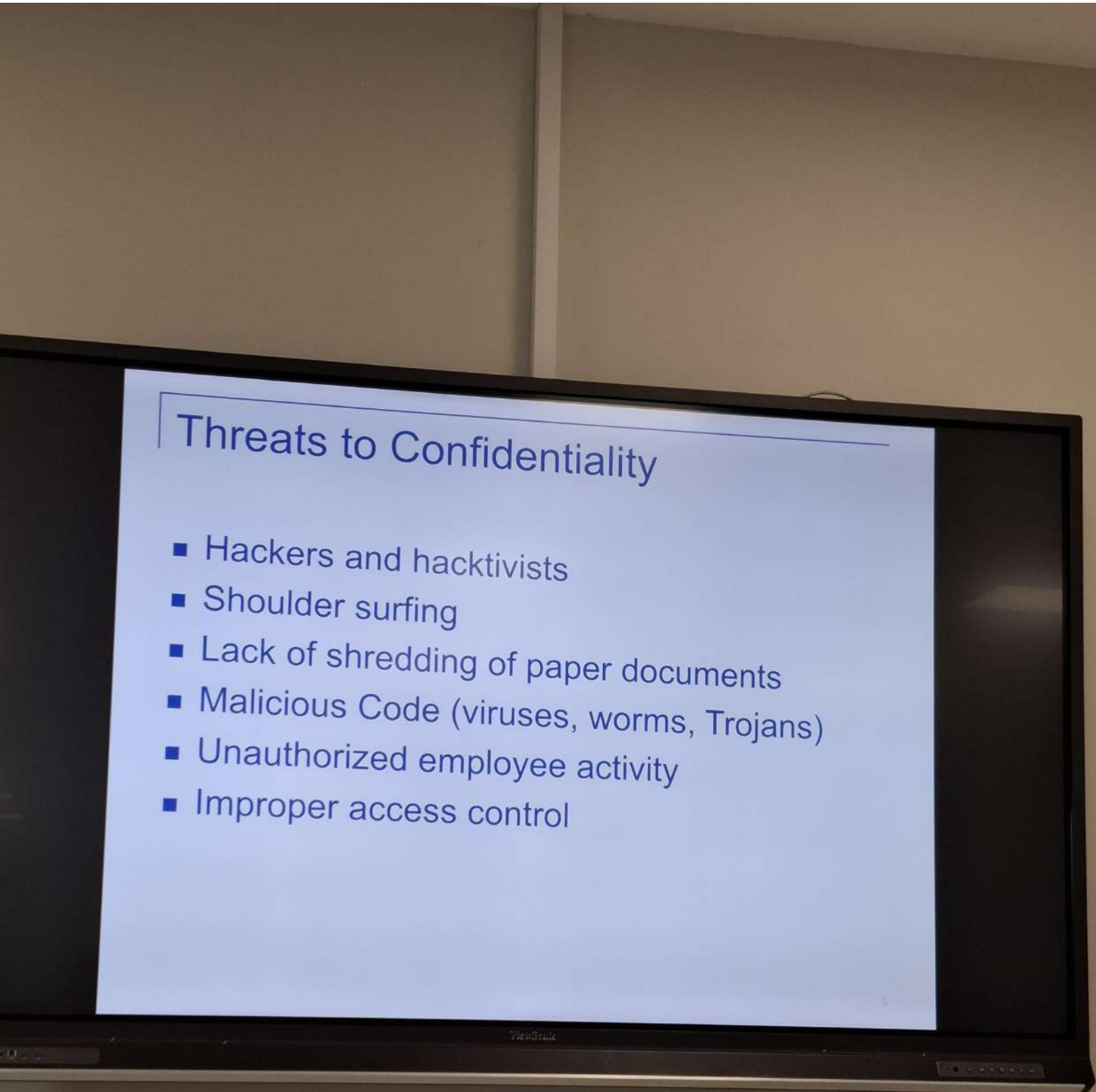
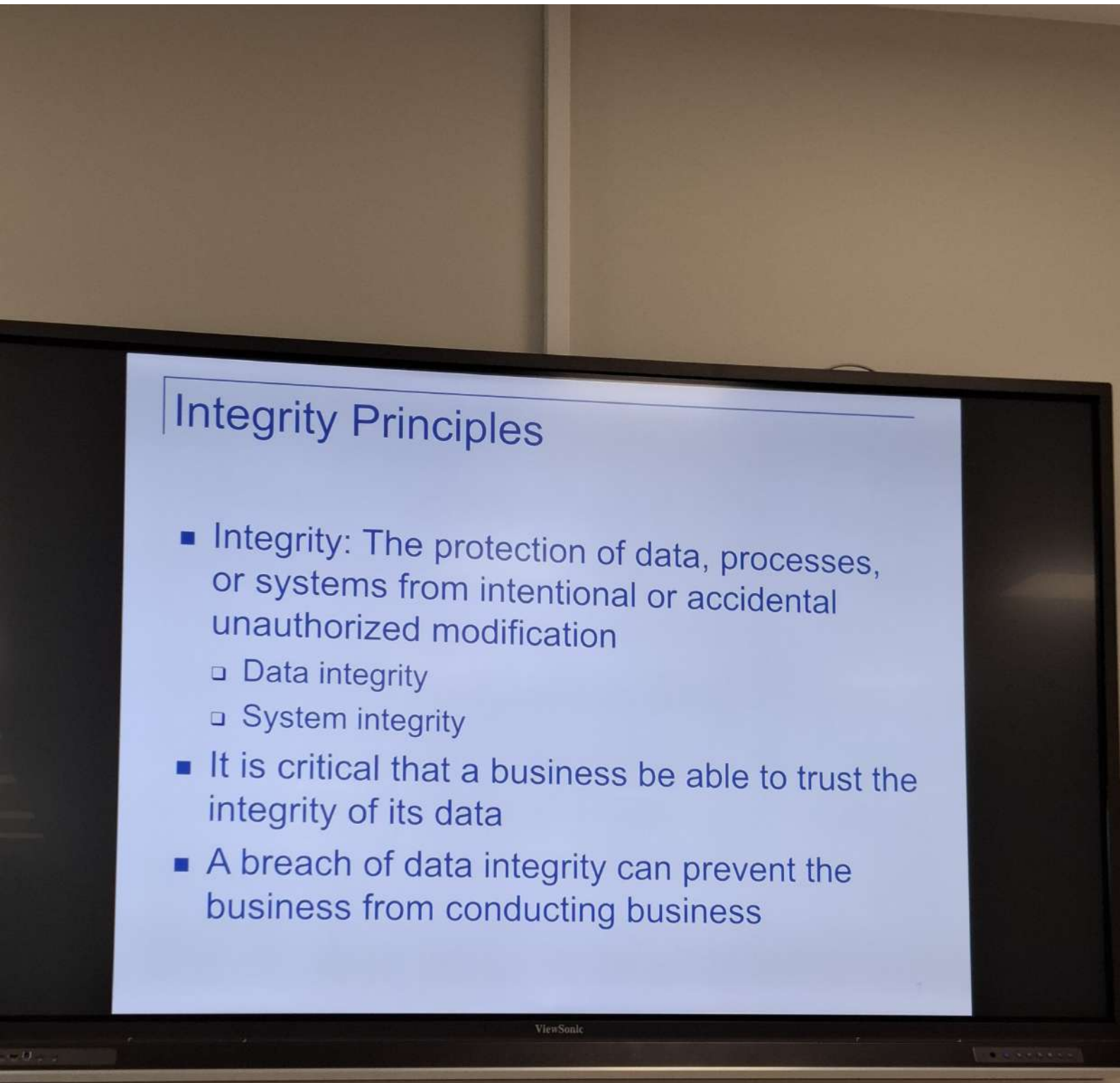
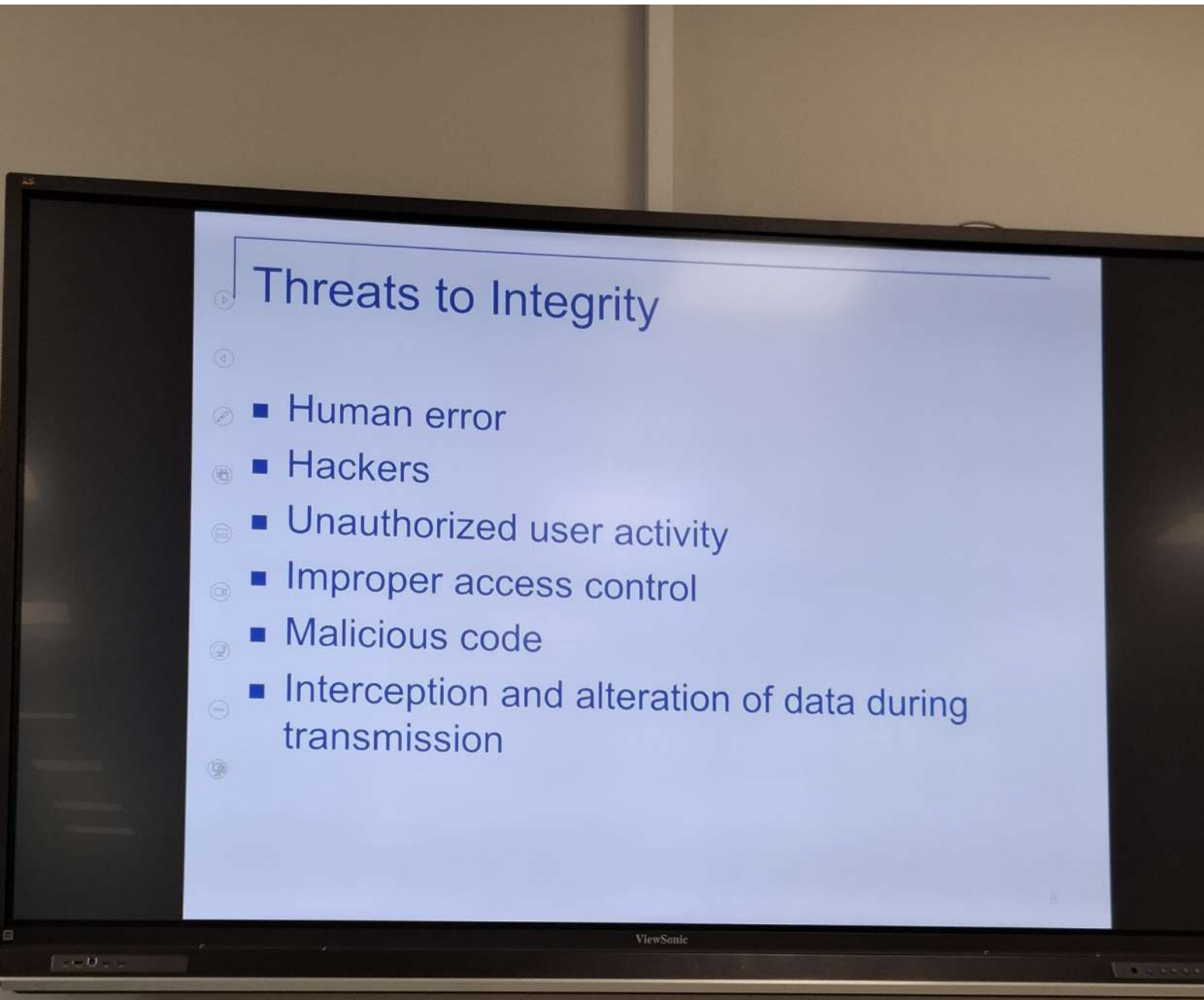
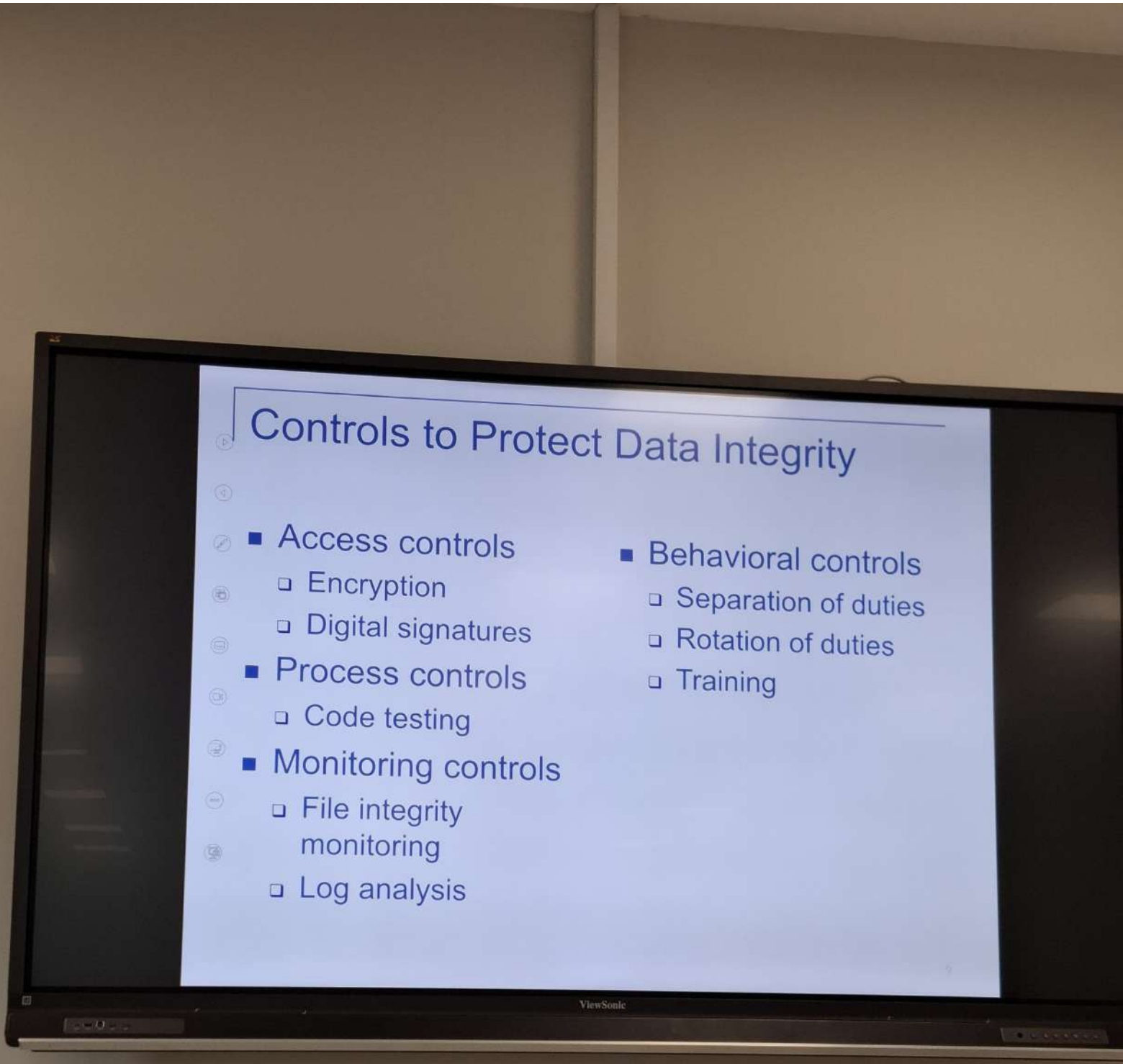

Confidentiality Principles
Not all data owned by the company should be made available to the public
Failing to protect data confidentiality can be disastrous for an organization
Protected Health Information (PHI) between doctor and patient
Protected Financial Information (PFI) between bank and customer
Business-critical information to rival company
ViewSonic

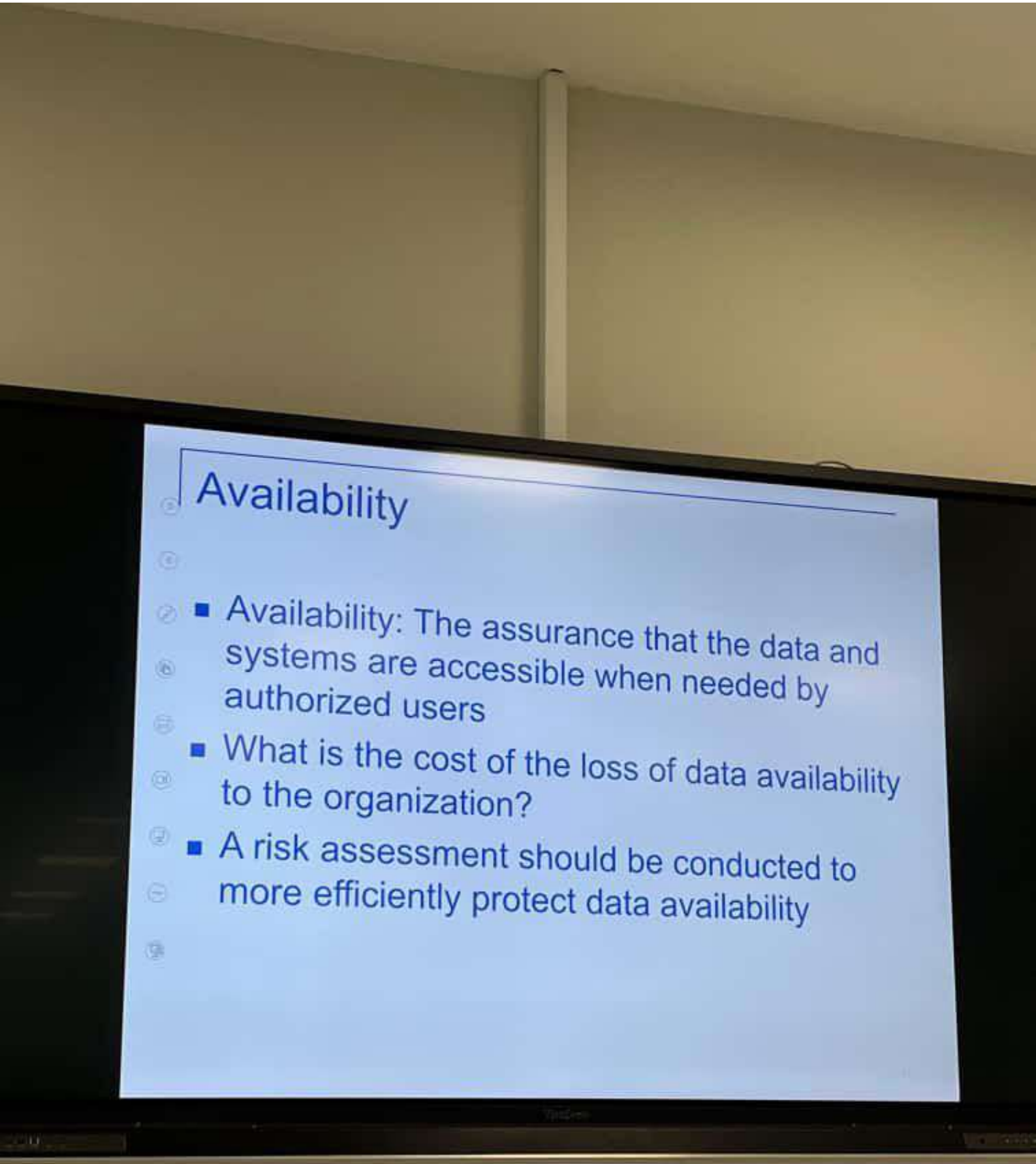

Confidentiality Principles
Only *authorized users* should gain access to information
Information must be protected when it is used, shared, transmitted, and stored
Information must be protected from unauthorized users both internally and externally
Information must be protected whether it is in digital or paper format
ViewSonic

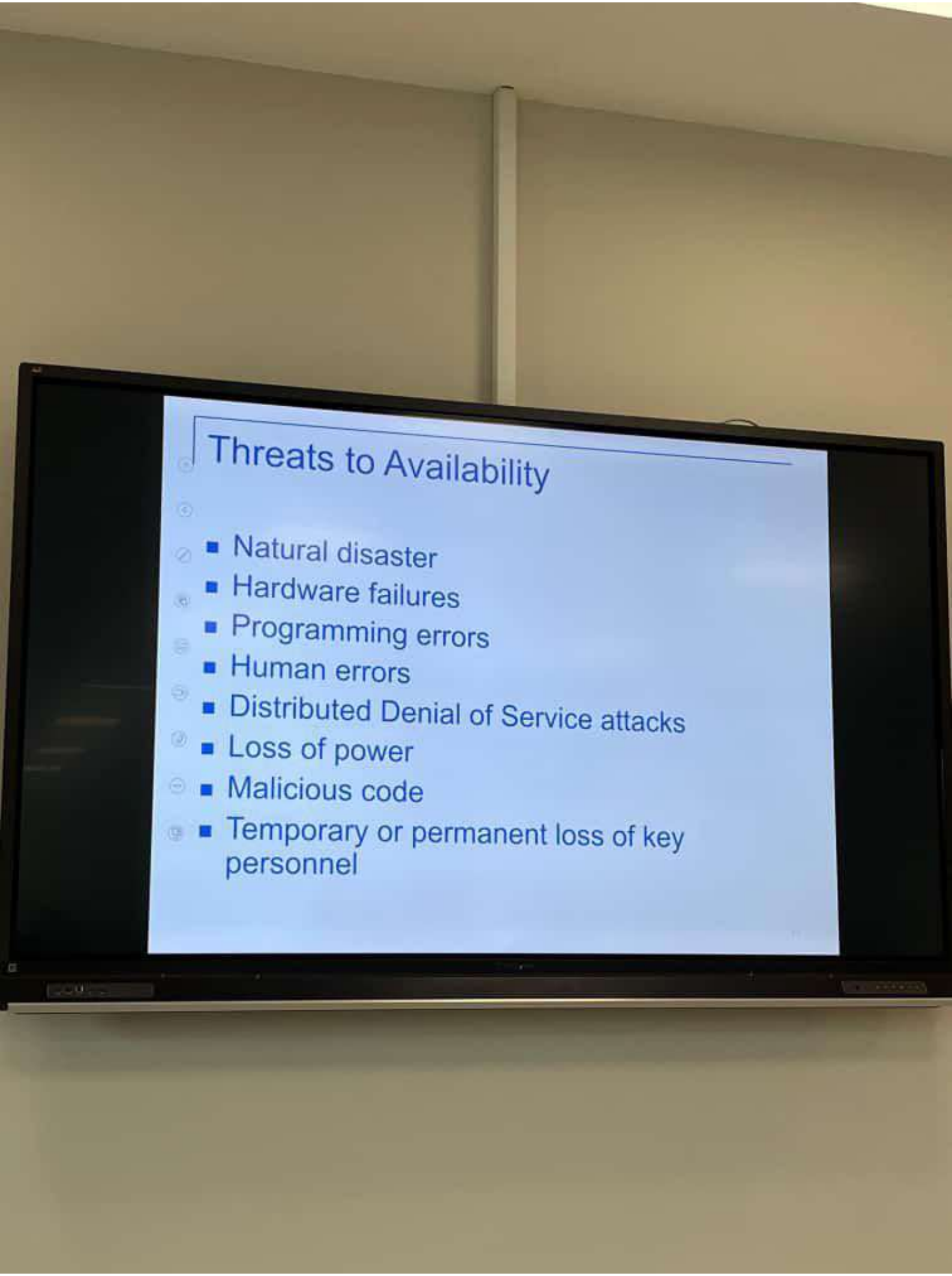

Threats to Confidentiality
Hackers and hacktivists
Shoulder surfing
Lack of shredding of paper documents
Malicious Code (viruses, worms, Trojans)
Unauthorized employee activity
Improper access control

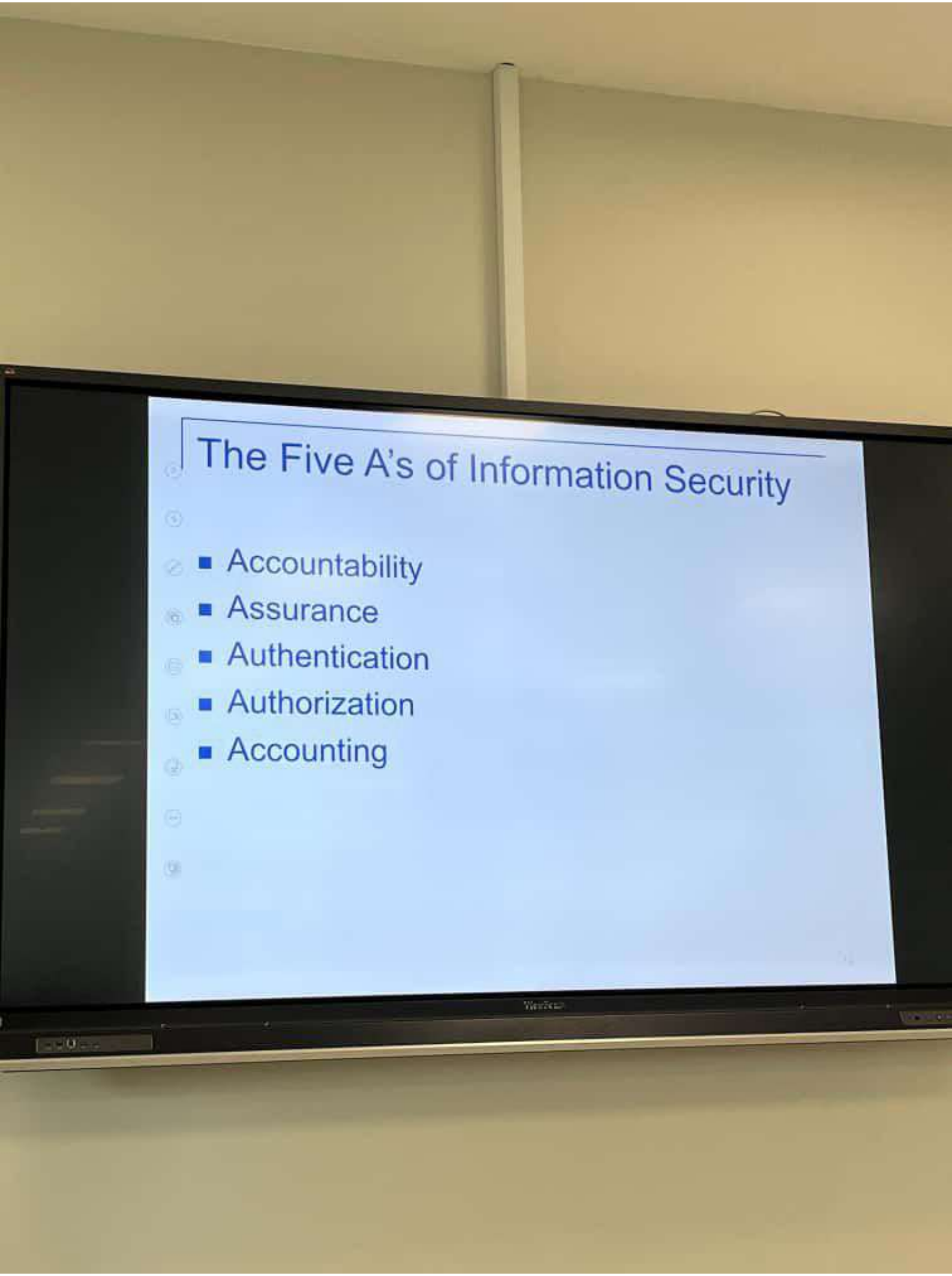

Integrity Principles
Integrity: The protection of data, processes, or systems from intentional or accidental unauthorized modification
Data integrity
System integrity
It is critical that a business be able to trust the integrity of its data
A breach of data integrity can prevent the business from conducting business
ViewSonic

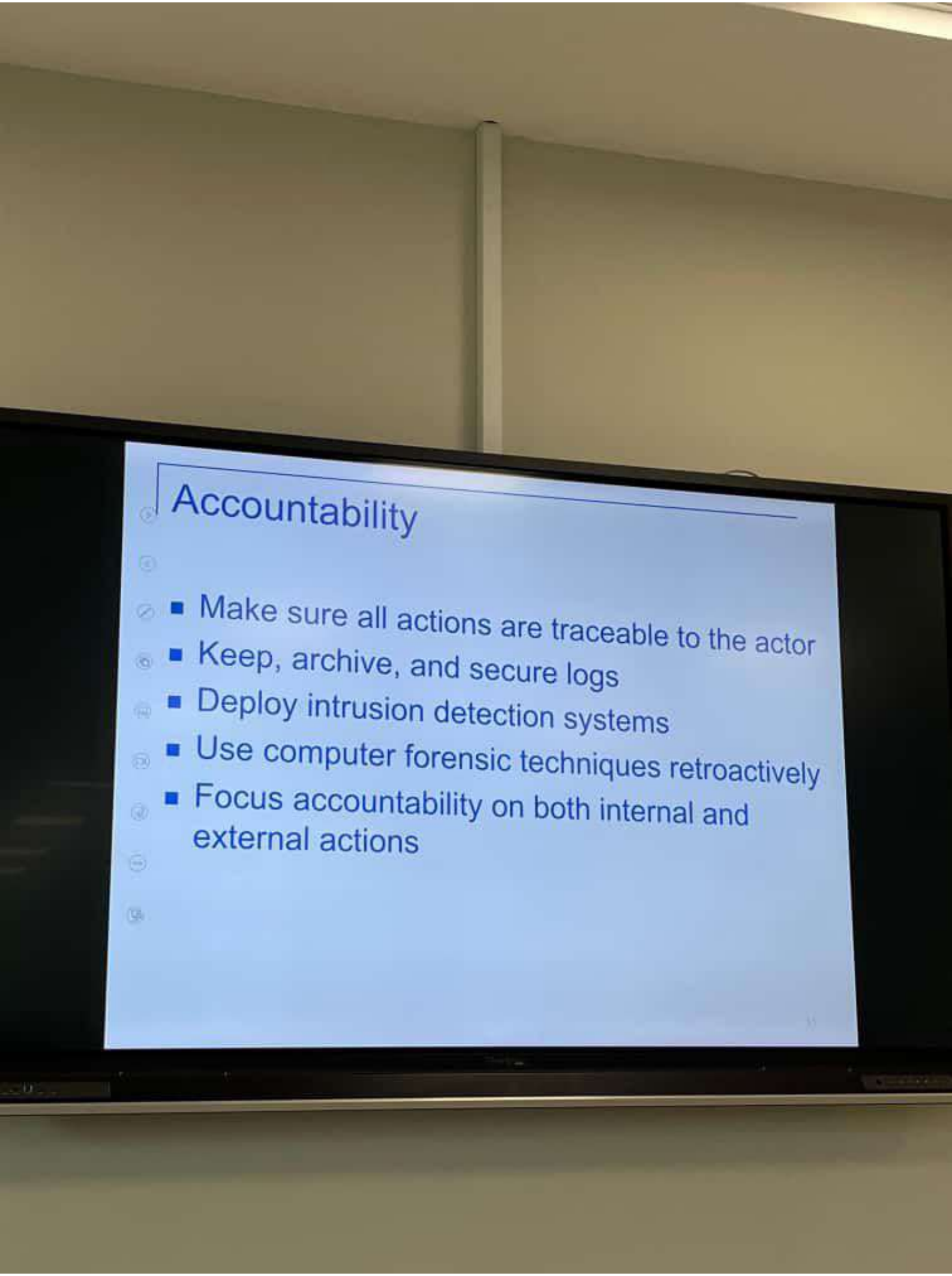

Threats to Integrity
Human error
Hackers
Unauthorized user activity
Improper access control
Malicious code
Interception and alteration of data during transmission
ViewSonic

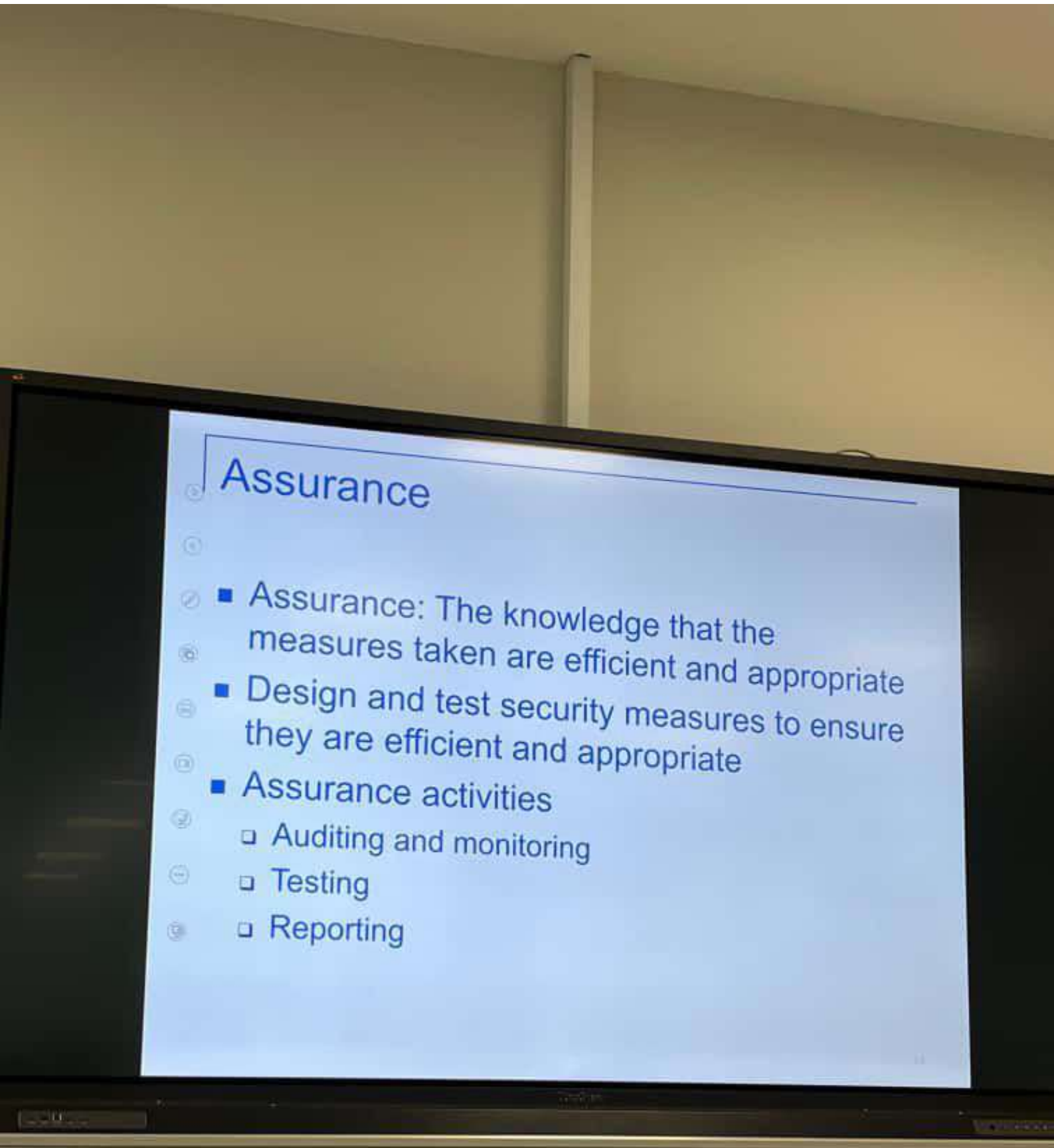

Controls to Protect Data Integrity
Access controls
Encryption
Digital signatures
Process controls
Code testing
Monitoring controls
File integrity monitoring
Log analysis
Behavioral controls
Separation of duties
Rotation of duties
Training
ViewSonic

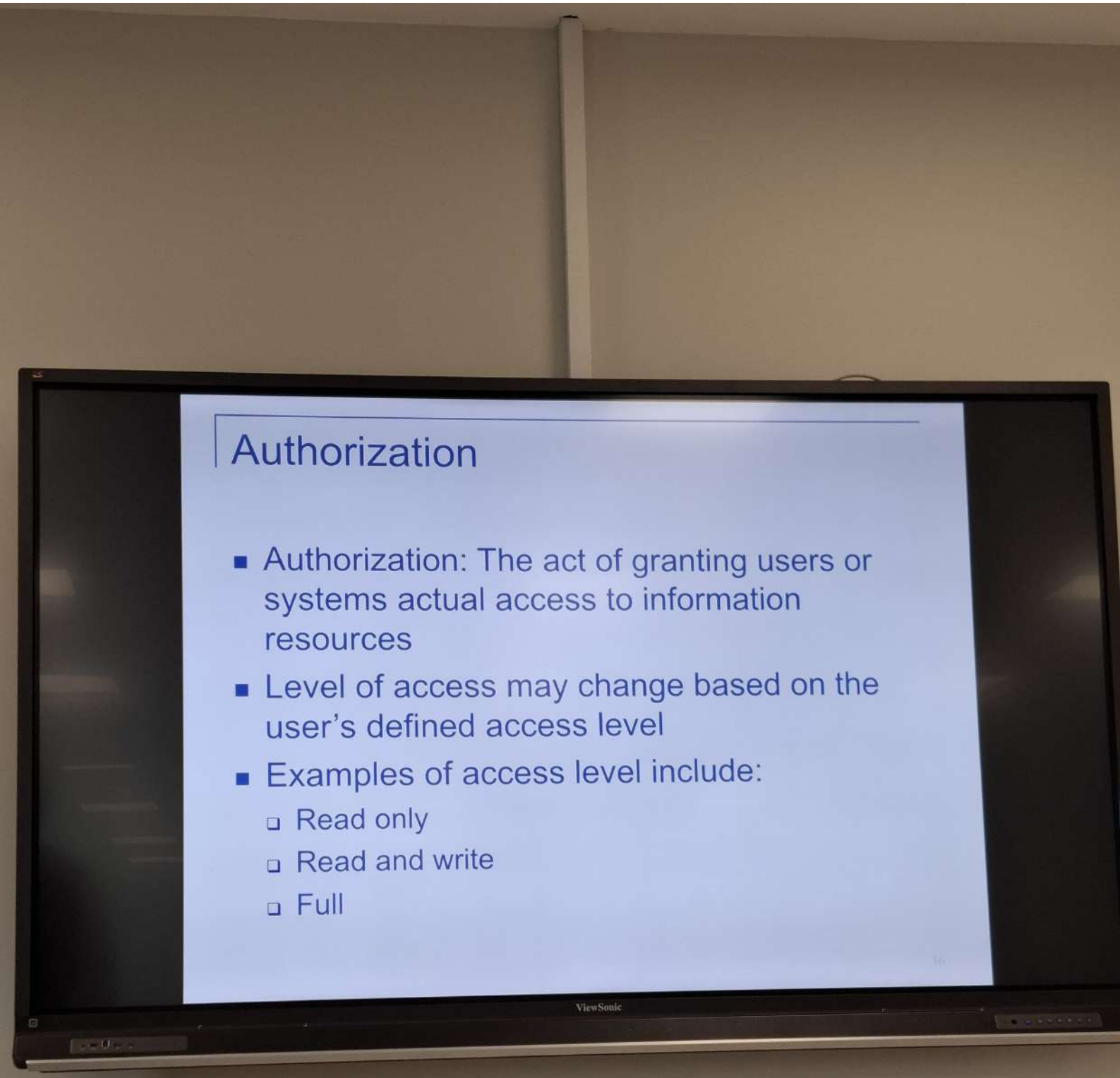

Availability
Availability: The assurance that the data and systems are accessible when needed by authorized users
What is the cost of the loss of data availability to the organization?
A risk assessment should be conducted to more efficiently protect data availability

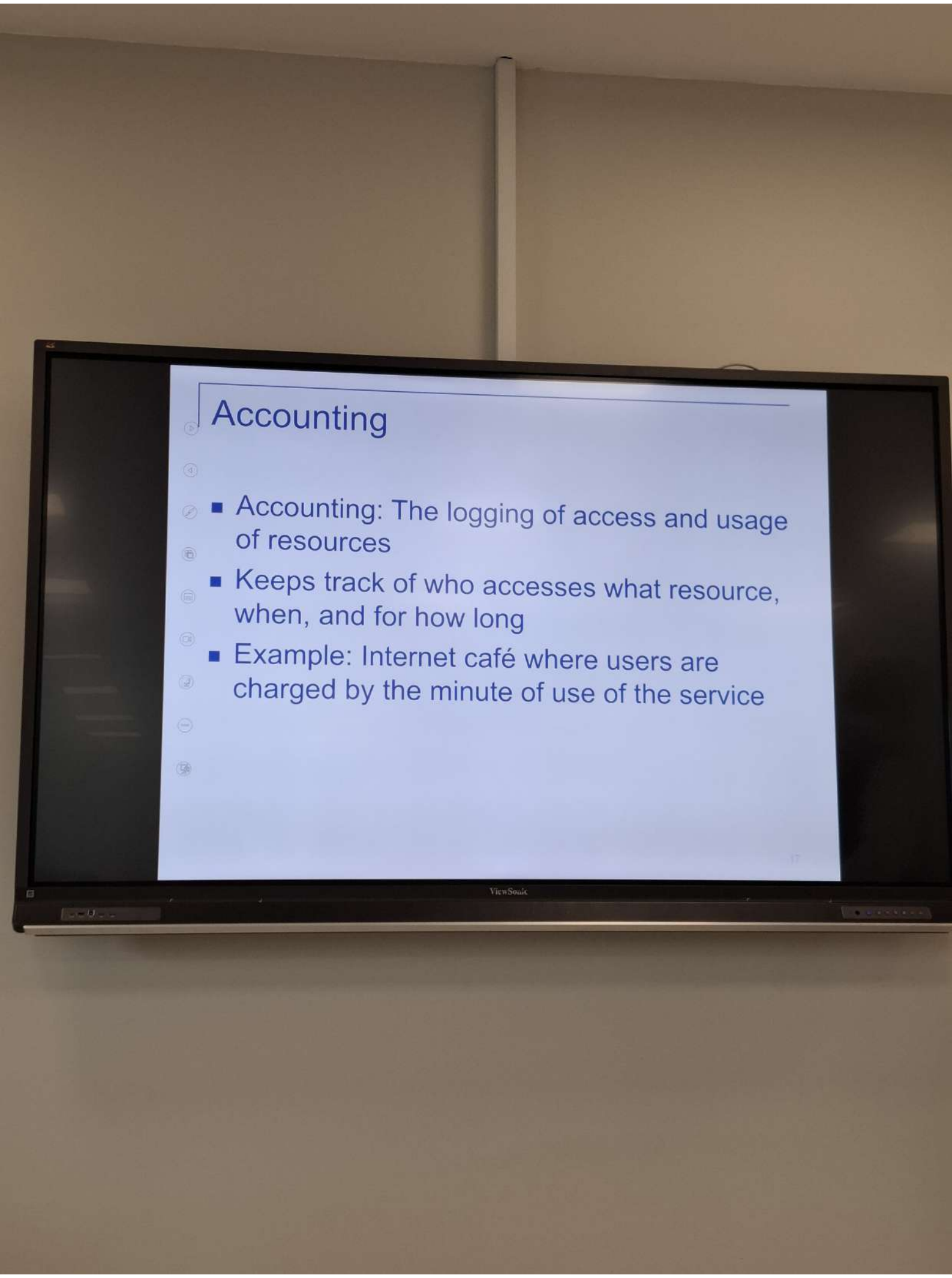

Threats to Availability
Natural disaster
Hardware failures
Programming errors
Human errors
Distributed Denial of Service attacks
Loss of power
Malicious code
Temporary or permanent loss of key personnel

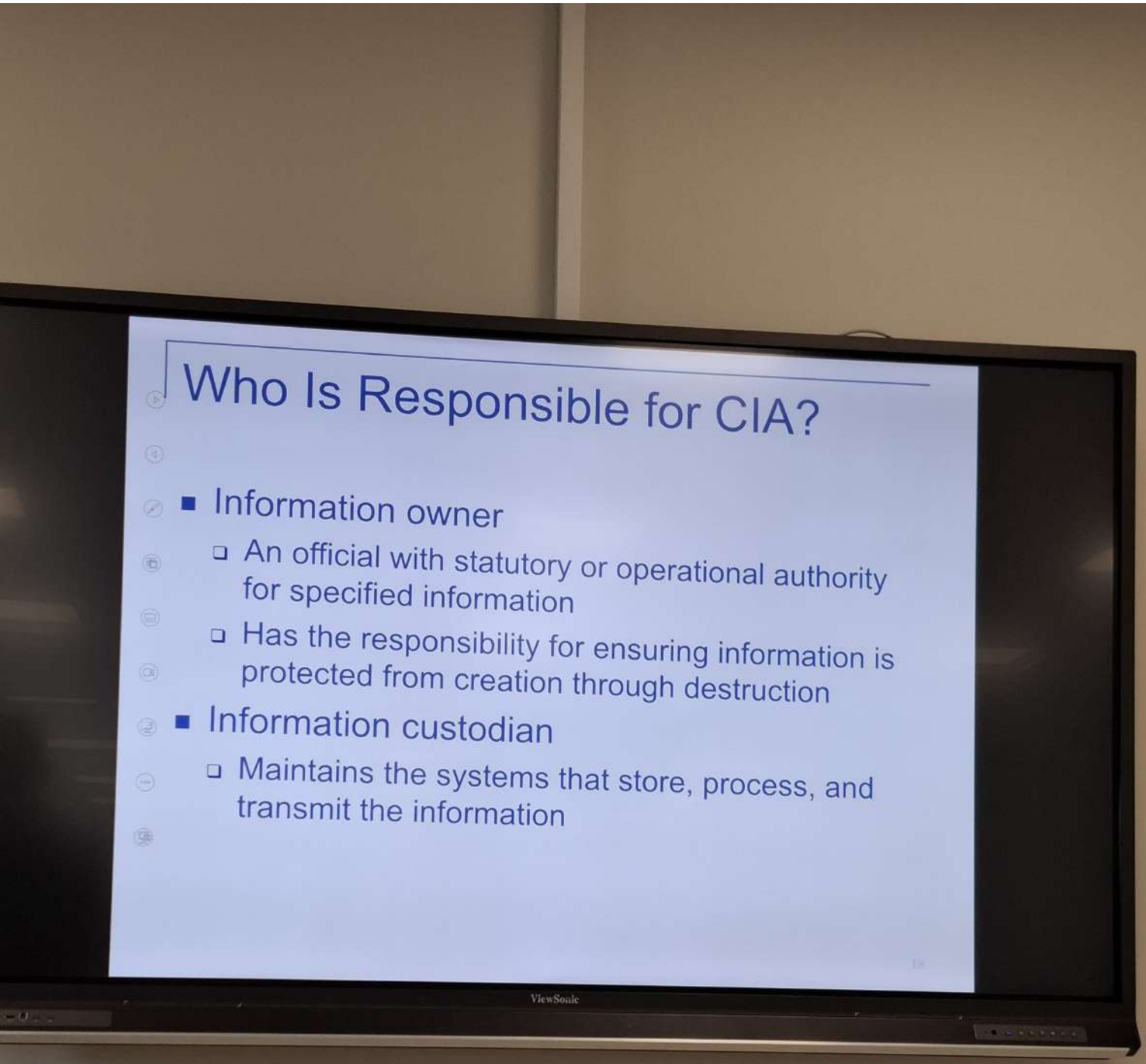

The Five A's of Information Security
Accountability
Assurance
Authentication
Authorization
Accounting

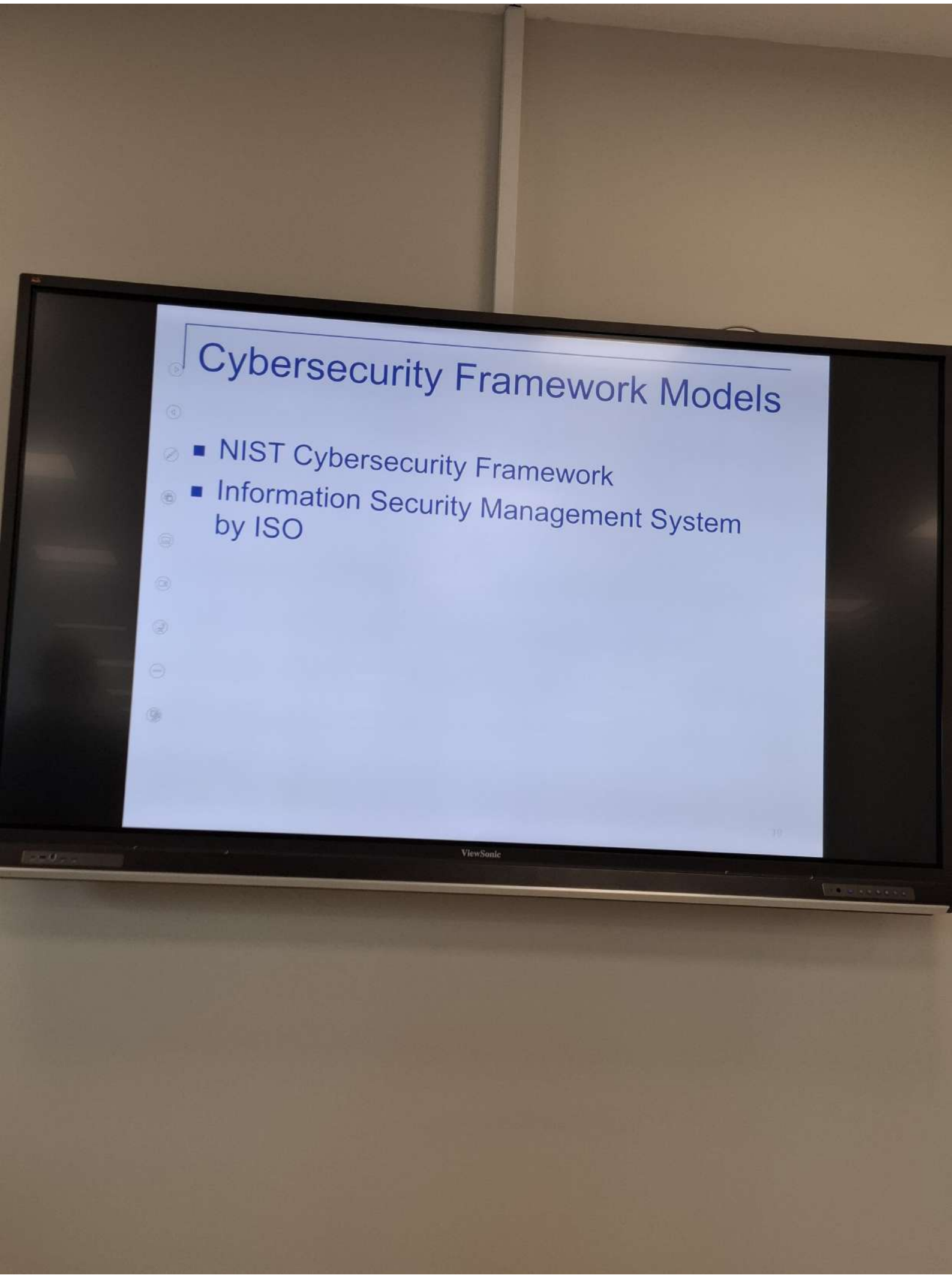

Accountability
Make sure all actions are traceable to the actor
Keep, archive, and secure logs
Deploy intrusion detection systems
Use computer forensic techniques retroactively
Focus accountability on both internal and external actions

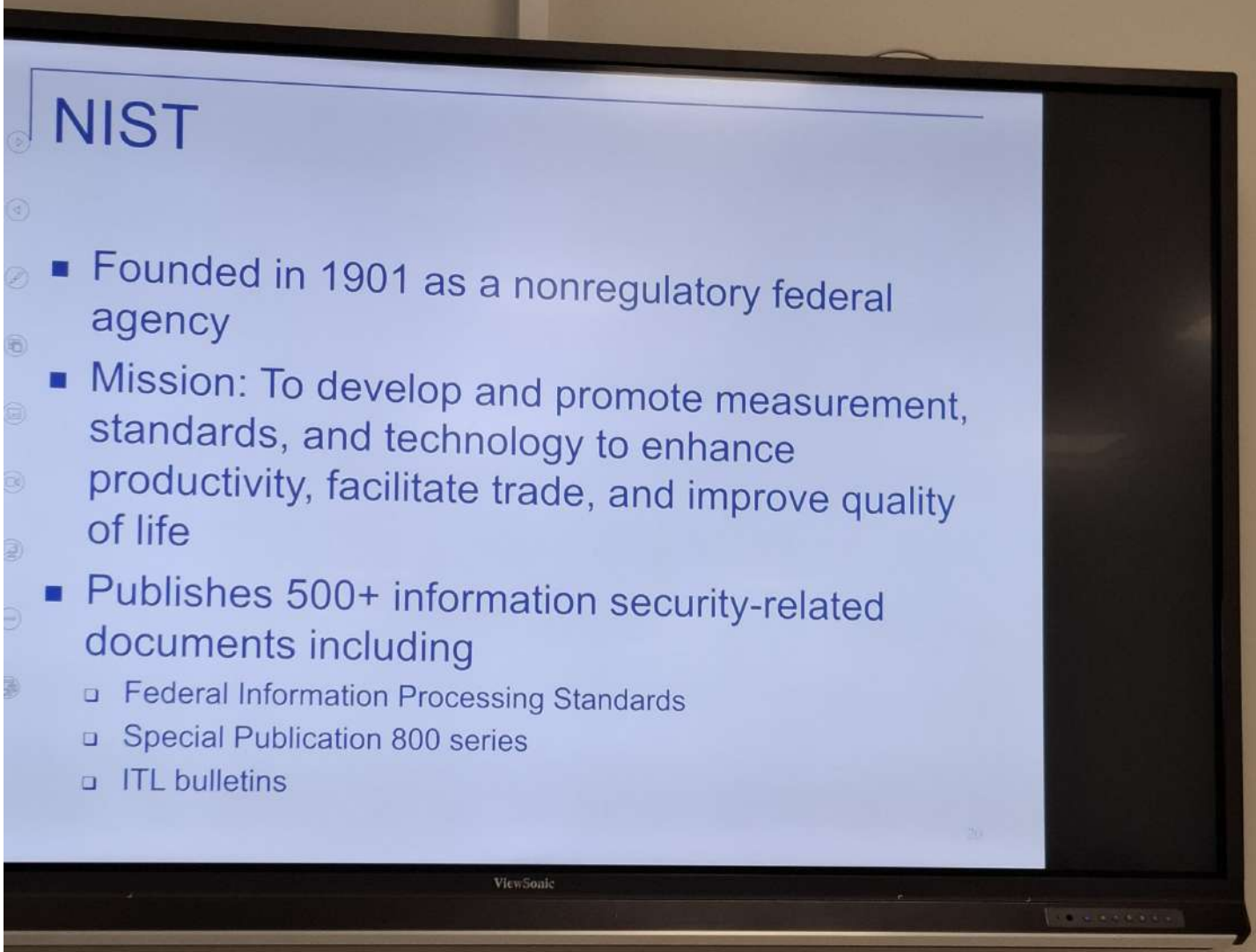

Assurance
Assurance: The knowledge that the measures taken are efficient and appropriate
Design and test security measures to ensure they are efficient and appropriate
Assurance activities
Auditing and monitoring
Testing
Reporting


Authorization
Authorization: The act of granting users or systems actual access to information resources
Level of access may change based on the user's defined access level
Examples of access level include:
Read only
Read and write
Full
ViewSonic

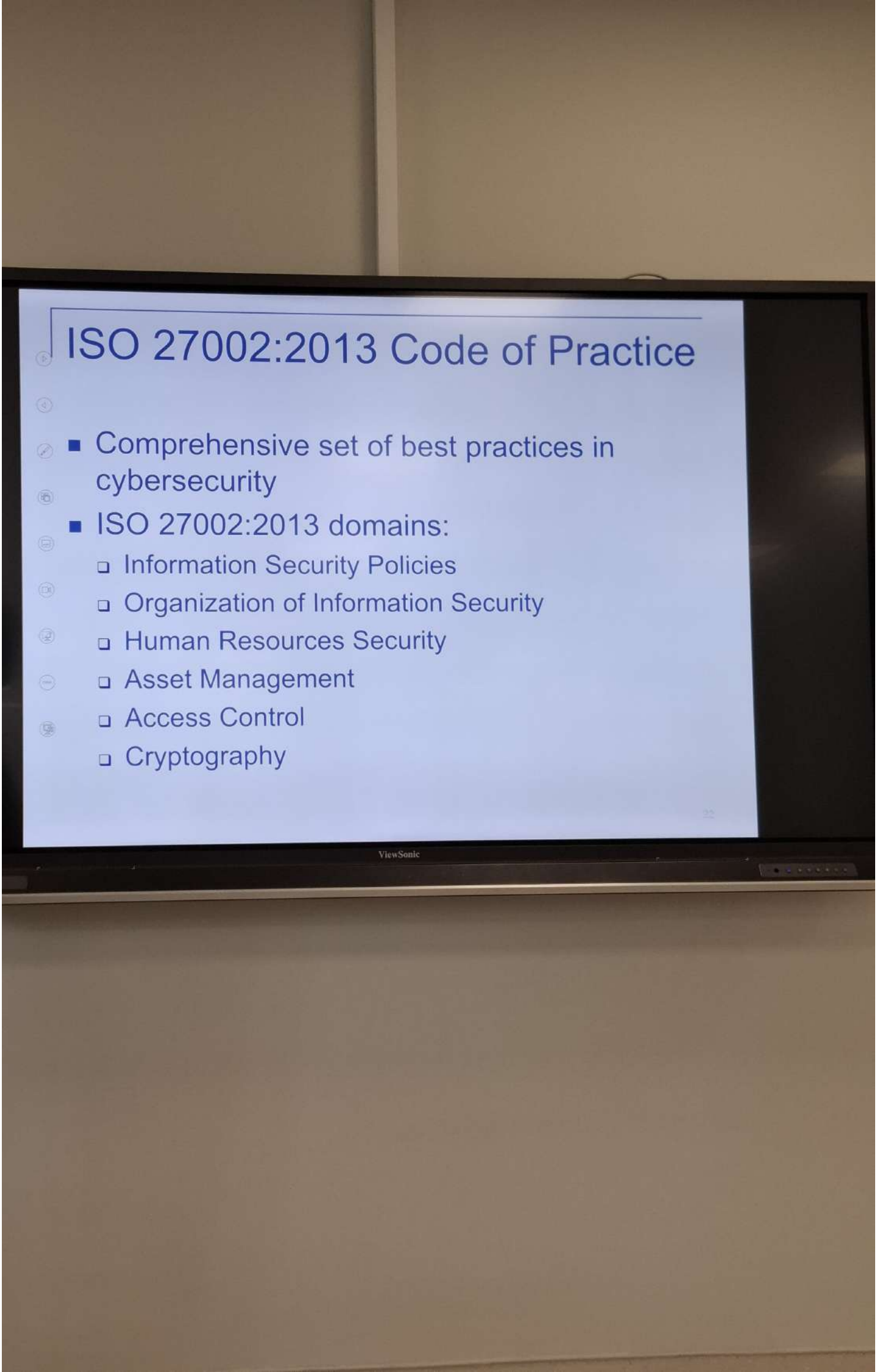

Accounting
Accounting: The logging of access and usage of resources
Keeps track of who accesses what resource, when, and for how long
Example: Internet café where users are charged by the minute of use of the service
ViewSonic

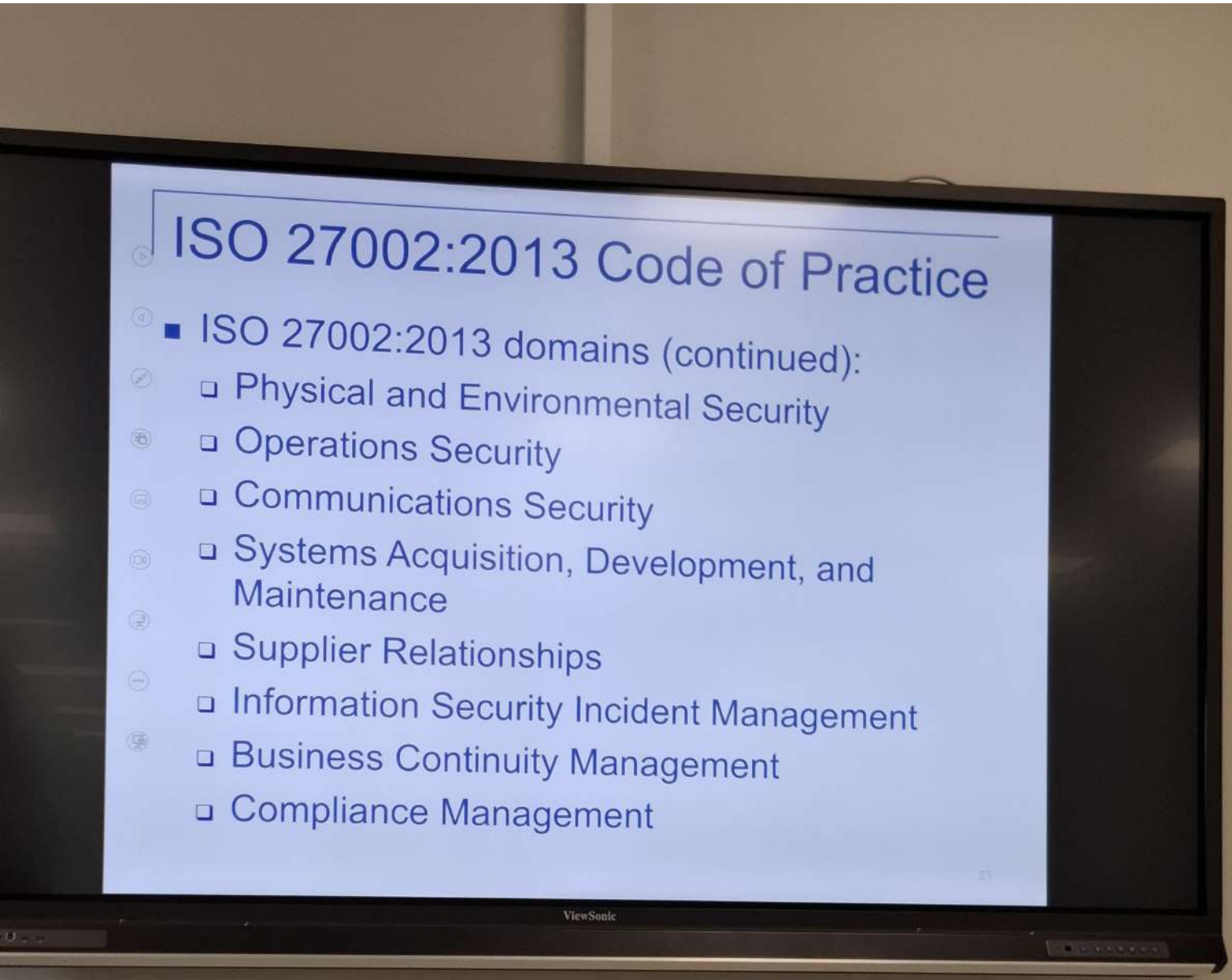

Who Is Responsible for CIA?
Information owner
An official with statutory or operational authority for specified information
Has the responsibility for ensuring information is protected from creation through destruction
Information custodian
Maintains the systems that store, process, and transmit the information
ViewSonic

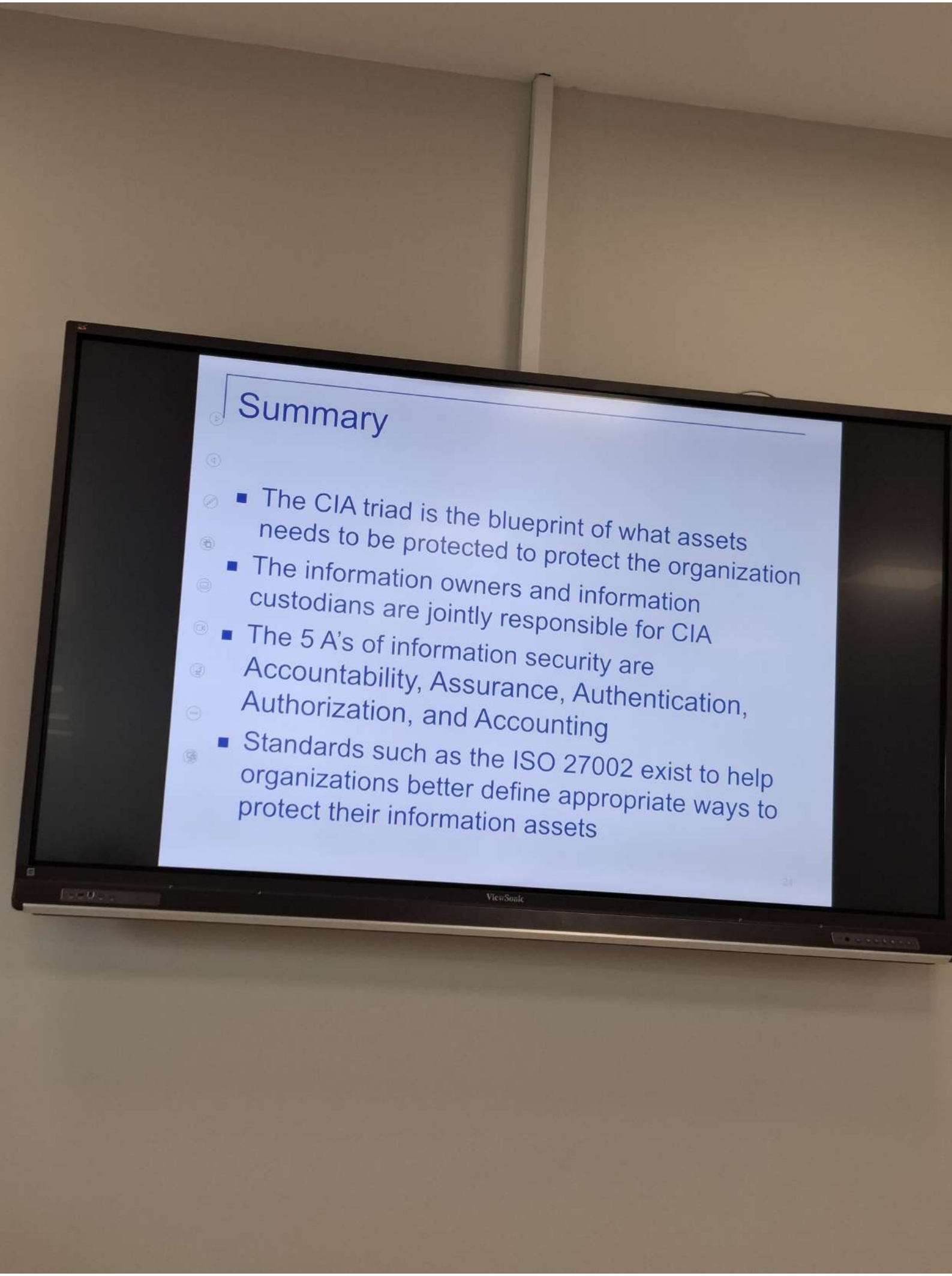

Cybersecurity Framework Models
NIST Cybersecurity Framework
Information Security Management System by ISO
ViewSonic


NIST
Founded in 1901 as a nonregulatory federal agency
Mission: To develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve quality of life
Publishes 500+ information security-related documents including
Federal Information Processing Standards
Special Publication 800 series
ITL bulletins
ViewSonic


ISO
A network of national standards institutes of 160 countries
Nongovernmental organization that has developed more than 13,000 international standards
The ISO/IEC 27000 series represents information security standards published by ISO and Electro-technical Commission (IEC)
ViewSonic


ISO 27002:2013 Code of Practice
Comprehensive set of best practices in cybersecurity
ISO 27002:2013 domains:
Information Security Policies
Organization of Information Security
Human Resources Security
Asset Management
Access Control
Cryptography
ViewSonic


ISO 27002:2013 Code of Practice
ISO 27002:2013 domains (continued):
Physical and Environmental Security
Operations Security
Communications Security
Systems Acquisition, Development, and Maintenance
Supplier Relationships
Information Security Incident Management
Business Continuity Management
Compliance Management
ViewSonic


Summary
The CIA triad is the blueprint of what assets needs to be protected to protect the organization
The information owners and information custodians are jointly responsible for CIA
The 5 A's of information security are Accountability, Assurance, Authentication, Authorization, and Accounting
Standards such as the ISO 27002 exist to help organizations better define appropriate ways to protect their information assets
ViewSonic