

Semester I

CSCH 401 : Strategic Governance of Cybersecurity Risks and Controls

UNIT I

The Importance of Cybersecurity Management: The Growing Pains of an Emerging Discipline, Understanding the Costs and Benefits of cybersecurity management to an Organization, Two Absolute Rules for Cybersecurity Work, Implementing a Strategic Response, **Control-Based Information Governance:** The Value of Formal Control, Organizing Things into a Rational Process, Information Audit and Control, Control Principles, **A Survey of Control Frameworks:** COSO Framework, IT Infrastructure Library Framework, ISO 27001, COBIT 5, IT Security Controls, General Structure and Applications. (16 hours)

UNIT II

The Importance of Controls: Goal-Based Security Controls, Implementation-Based Security Controls, The Security Control Formulation and Development Process, Control Implementation through Security Architecture Design, **Implementing a Multitiered Governance and Control Framework in a Business :** Constructing Practical Systems of Controls, Building the Security Control System, Initial Setup and Tradeoffs, **Risk Management and Prioritization Using a Control Perspective:** Five Elements of the Risk Management Process, Risk Management Plan, Implementing a Managed Risk Control Process, Planning for Effective Risk Management, Writing the Risk Management Plan, Risk Management Controls, Evaluating the Overall Policy Guidance (16 hours)

UNIT III

Control Formulation and Implementation Process: The Control Formulation Process, Creating and Documenting Control Objectives, Creating a Management-Level Control Process, Measurement-Based Assurance of Controls, **Security Control Validation and Verification:** Security Control Assessment Fundamentals, NIST Security Control Assessment Process, Common Types of Operational and Technical Security Tests, Common Operational and Technical Security Examination Techniques, **Control Framework Sustainment and Security of Operations:** Operational Assurance, Response Management, Operational Oversight and Infrastructure Assurance of Control Set Integrity (16 hours)

TextBooks

- (1). "The Complete Guide to Cybersecurity Risks and Controls", Anne Kohnke, Dan Shoemaker, Ken Sigler, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016
- (2). "Securing an IT Organization through Governance, Risk Management, and Audit", Ken Sigler, Dr. James L. Rainey, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016
- (3). "A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)", Anne Kohnke, Dan Shoemaker, Ken Sigler, Internal Audit and IT Audit Series, CRC Press Taylor & Francis Group, 2016
- (4). "Cybercrimes: A Multidisciplinary Analysis", Sumit Ghosh, Elliot Turrini, Springer, 2010