SETON HALL
UNIVERSITY™
1856

Cyber Intelligence 4U
Seton Hall University

Enterprise Cybersecurity in Digital Business
Basic Certificate Program 2024
Syllabus

CYBER
INTELLIGENCE 4U

Table of Contents

Enterprise Cybersecurity in Digital Business
Basic Certificate Program 2024

Program Overview

Cyber is a business issue. This is a program about business impacts. The best cyber, privacy, compliance and risk managers have a good foundational cyber understanding and need to have a well-rounded solid skill set of core business acumen in terms of analytical skills, and critical thinking focused on cyber risks. This program is about creating thought leaders and critical thinkers who can bridge these gaps. This program is holistic and starts with the basics, covering terminology, breach case studies, cyber program roles, processes and tools. It moves deeper into the integrated cyber risk perspective while exploring the newest regulations, security assessment frameworks, forensics and auditing techniques, cyber risk management and cyber strategy using hands on learning to inventory digital assets, perform privacy assessments, quantify exposures and risk model.

The Enterprise Cybersecurity in Digital Business Basic Certificate Program is a rigorous self-paced online curriculum led by prominent cybersecurity experts, many of whom advise governments, agencies, and industry bodies around the world. The program brings together executives, experts, innovators, and regulators to address cybersecurity from a digital point of view and leaves the student empowered.

This program is ideal for the following roles and departments: CISO, CRO, DPO, Board of Directors, Compliance, Audit, Security Manager, Security Team, IT Team, Vendor Team

Students will be empowered by:

- The ability to understand cyber holistically from a business perspective across regulation, compliance, security standards and risk. Students will be able to strategize how to lower cyber risk and work with stakeholders to increase cyber resilience.
- An in-depth understanding of cyber exposures and scores that determine show crown jewel exposures, identify hidden exposures, determine cyber insurance needs, and identify gaps in the programs across security, compliance and privacy.
- Hands on learning with the ValuRisQ product that allows students to use live or dummy data to risk model, quantify exposures, perform a privacy impact assessment and deliver board reports with KPIs and metrics that empower the board.
- A premier certificate from Seton Hall University, as validation of newfound cybersecurity knowledge and skills, as well as access to a global network of likeminded cybersecurity professionals.

Required Text

Managing Cyber Risk - Strategies for Surviving and Thriving in the age of Interconnectivity and Innovation, Evans; 1st Edition, ISBN-13: 978-0367177737.

Prerequisites

No prior knowledge of IT or cyber is required.

Note: This syllabus is subject to change based on the needs of the class.

Module 1: Cybersecurity Basics

Module Description
This module introduces cybersecurity from a business point of view based on research with the Fortune 1000 and cyber insurance industry using a digital asset methodology. In 2001, 10% of a business was digital, today 85% of an organization's value is digital. The module focuses on building student understanding of cybersecurity from how cyber evolved out of information technology, addresses key cyber-related business and technical roles, demonstrates the consequences of poor cyber hygiene and reviews cybersecurity trends.

In addition to the evolution of cyber, students learn to communicate in the language of cybersecurity, study data breaches, attack surfaces, today's enterprise threats, and enterprise cybersecurity program components.

Module Grade
Each student is expected to satisfy the following requirements:

- Quizzes (100%)

Module 2: Regulations, Standards and Frameworks

Module Description
This module provides an introduction to cybersecurity regulation based on industry, geography, government, and data type. It explores standards and frameworks, aligning them to security control tests. Regulations covered at the Federal level are the Healthcare Information Portability and Accounting Act (HIPAA), the Securities Exchange Commission (SEC), the Graham Leach Bliley Act (GLBA), and the Fair Practices Act. Regulations at the state level focus on new privacy laws, including the California Consumer Protection Act (CCPA), State privacy acts in Maine, Nevada, and Colorado, and the New York State Department of Financial Services Part 500 (NY CRR 500), and the Insurance Data Security Act. The module covers both organizational and third-party requirements.

Here are the main objectives found in this module to map control assessment requirements to the following laws:

- **Federal Regulations** – Including FTC, FCC, OCIE, HHS and GLBA Laws
- **State Regulations** – Including CCPA, NYS DFS, State Privacy Laws, and the Insurance Data Security Act
- **Industry Standards** – Including PCI
- **European Regulations** – Including GDPR
- **Frameworks** – Including ISO27001, PCI-DSS, NIST 800-53, NIST CSF, COBIT, CIS Top20 Controls, etc.

Module Grade
Each student is expected to satisfy the following requirements:

- Quizzes (100%)