









# Building an Effective Cybersecurity Program Syllabus (Sample)

---

-  **Instructor:** Tari Schreider
-  **Phone:** 678.595.2818
-  **Email:** [trschreider@gmail.com](mailto:trschreider@gmail.com)
-  **Description:** A study of cybersecurity principles, practices, frameworks, standards, and best practices necessary to design, build and manage a cybersecurity program. Discussion covers cybersecurity program architecture, defining a governance foundation, building a threat and vulnerability capability, building a risk management capability, implementing defense in depth strategies and applying service management concepts.
-  **Prerequisites:** Prerequisites can be assigned once the course level has been determined.
-  **Required Text:** Building an Effective Cybersecurity Program – Author: Tari Schreider – Publisher: Rothstein Publishing – ISBN: **Print** – 9781944480530, **PDF** – 9781944480554 – **EPUB** – 9781944480547
-  **Duration:** Can be Taught as an 8- or 16-Week Course
-  **Class Length:** One or two 90-minute Classes Held Weekly
-  **Credits:** 3 Credits
-  **Overview:** In this course, you will study how to build a cybersecurity program from a Chief Information Security Officer's (CISO) perspective.
- The course is designed as a roadmap to guide students through the phases of creating a comprehensive cybersecurity program to protect information and assets.

Essential program design methodologies and authoritative industry security and privacy standards are covered to explain how to define and implement governance, risk and compliance components.

An overview of the most critical information and asset protection technologies and controls are presented along with how to define the necessary policies, procedures and processes to effectively manage and operate a cybersecurity program.

Students will learn key cybersecurity program management disciplines consisting of program staffing, budget management, third-party risk management, cyber risk insurance, and security awareness training. Creating threat, vulnerability, intelligence, and risk management functions are covered in depth along with how to apply service management concepts to automate and improve security and privacy services.

The course also covers the latest developments in integrating application development, operations and security (DevSecOps), security operations (SecOps), security automation and orchestration (SAO), and emerging technologies.



### **Outcomes:**

After completing this course, students should be able to:

- Create a cybersecurity program blueprint to guide the creation of a pragmatic program to protect information and assets.
- Understand the differences and advantages of information asset protection technologies and services and how they're used to create a layered protection strategy.
- Identify and categorize threats and vulnerabilities using cybersecurity intelligence.
- Manage and mitigate risk through the application of risk treatment options consisting of key controls, cyber risk insurance, compensating controls and risk avoidance.
- Develop an information and asset security governance and management program that aligns with organizational strategies by evaluating business requirements, applicable laws, regulations, standards, and best practices.

- Identify supply chain threats introduced by third-party security breaches and disruptions.
- Identify and evaluate cybersecurity program maturity levels and how to improve program efficiency through the adoption of service management.



## Projects:

During the course, students can be responsible for the following example projects:

- **Papers:**
  - **Cyber Threats** – Research and create a PowerPoint presentation on critical cybersecurity threats facing organizations today.
  - **Defense-in-Depth Model** – Build a defense-in-depth model identifying technologies aligned to the open systems interconnection (OSI) model and defend their selection of products and services.
  - **Control Standard Comparison** – Compare two cybersecurity control standards outlining their respective advantages and disadvantages providing a recommendation of adoption.
  - **Team Paper** – Team presentations of assigned course project using the cybersecurity program design toolkit.
- **Case Studies:**
  - **Ransomware Attack** – Identify and research a major organization that has experienced a ransomware attack and detail their impacts and response.
  - **Security Awareness** – Create a company profile based on a public information and create a security awareness program aligned to their workforce.
  - **Security Testing** – Select a public company, identify their web service presence and recommend effective security testing strategies.
- **Labs:**
  - **Risk Assessment** – Identify a common web application to perform a risk assessment using the provided excel-based risk assessment tool. Recommend a risk treatment plan to mitigate the identified risk.
  - **Security Metrics** – Create supporting metrics for each cybersecurity technology or service identified in the previously created defense-in-depth model.

- **Security Budget** – Create a cybersecurity program organization budget based on the previously created defense-in-depth model. Include acquisition, deployment and maintenance costs.



**Schedule:**

The following provides an overview of the 16-week course with associated assignments:

Week	Assignments
1	<p><b>Topic:</b> Standardized Cybersecurity Program Design  <b>Readings:</b> As assigned in classroom  <b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Course introduction and overview</li> <li>○ Today’s cybersecurity threats</li> <li>○ Cybersecurity program drivers</li> <li>○ Role of the cybersecurity architect</li> <li>○ Roadmap</li> <li>○ Emerging cybersecurity technologies</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Cyber threats</li> <li>○ Case study – Cybersecurity architect job market</li> <li>○ Lab – Industry drivers</li> </ul>
2	<p><b>Topic:</b> Designing a Cybersecurity Program  <b>Readings:</b> As assigned in classroom  <b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Program design methodology</li> <li>○ Development approach – ADDIOI Model™</li> <li>○ Architectures, frameworks and models</li> <li>○ Program design guide</li> <li>○ Design principles</li> <li>○ Architectural views</li> <li>○ Program blueprint</li> <li>○ Program structure</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Architecture comparison</li> <li>○ Case study – Most commonly used frameworks</li> <li>○ Lab – Risk assessment</li> </ul>
3	<p><b>Topic:</b> Cybersecurity Frameworks &amp; Models  <b>Readings:</b> Assigned in classroom  <b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Introduction to frameworks and models</li> <li>○ HITRUST® CSF®</li> <li>○ Information Security Forum (ISF) Framework</li> <li>○ ISO/IEC 27001/27002</li> <li>○ NIST Cybersecurity Framework (CSF)</li> </ul>

Week	Assignments
	<p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – ISO vs NIST control libraries</li> <li>○ Case Study – Ransomware attack</li> <li>○ Lab – Achieving HIPAA compliance with HITRUST</li> </ul>
4	<p><b>Topic:</b> Cybersecurity Program Technologies – Part A</p> <p><b>Readings:</b> As assigned in classroom</p> <p><b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Application security</li> <li>○ Authentication</li> <li>○ Cloud security</li> <li>○ Container security</li> <li>○ Data loss prevention</li> <li>○ Digital forensics</li> <li>○ Distributed Denial of service mitigation</li> <li>○ Deception technology</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Cloud security domain analysis</li> <li>○ Case study – None</li> <li>○ Lab – None</li> </ul>
5	<p><b>Topic:</b> Cybersecurity Program Technologies – Part B</p> <p><b>Readings:</b> Assigned in classroom</p> <p><b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Domain name service attack security</li> <li>○ Encryption</li> <li>○ Endpoint protection</li> <li>○ Firewalls (FW)</li> <li>○ Identity access management (IDAM)</li> <li>○ Internet of Things (IoT) Security</li> <li>○ Intrusion protection systems (IPS)</li> <li>○ Network access control (NAC)</li> <li>○ Open source software protection</li> <li>○ Privileged account management (PAM)</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – IoT domain analysis</li> <li>○ Case study – None</li> <li>○ Lab – None</li> </ul>
6	<p><b>Topic:</b> Cybersecurity Program Technologies – Part C</p> <p><b>Readings:</b> As assigned in classroom</p> <p><b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Security information and event management (SIEM)</li> <li>○ Security Orchestration, Automation and Response (SOAR)</li> <li>○ Threat intelligence platform (TIP)</li> </ul>

Week	Assignments
	<ul style="list-style-type: none"> <li>○ User and entity behavior analysis (UEBA)</li> <li>○ Virtualization security</li> <li>○ Vulnerability management</li> <li>○ Web filtering</li> <li>○ Whitelisting</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Virtualization security analysis</li> <li>○ Case study – None</li> <li>○ Lab – None</li> </ul>
7	<p><b>Topic:</b> Cybersecurity Training &amp; Program Maturity</p> <p><b>Readings:</b> As assigned in classroom</p> <p><b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Security training program</li> <li>○ Awareness training</li> <li>○ Cybersecurity personnel roles and responsibilities</li> <li>○ Security talent development</li> <li>○ Training</li> <li>○ Certifications</li> <li>○ Culture of security</li> <li>○ Phishing attack training</li> <li>○ Ransomware simulations</li> <li>○ Maturing cybersecurity programs</li> <li>○ Maturity models and ratings</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Security awareness presentation</li> <li>○ Case study – Research and report on effective security awareness techniques</li> <li>○ Lab – None</li> </ul>
8	<p><b>Topic:</b> Cybersecurity Program Governance &amp; Policies</p> <p><b>Readings:</b> As assigned in classroom</p> <p><b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Governance overview</li> <li>○ Governance playbook</li> <li>○ Governance frameworks</li> <li>○ Governance oversight board</li> <li>○ Policy model</li> <li>○ Policy management</li> <li>○ Policy management products</li> <li>○ GRC software</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Governance playbook</li> <li>○ Case study – Research and report on most published policies</li> </ul>

Week	Assignments
	<ul style="list-style-type: none"> <li>○ Lab – None</li> </ul>
9	<p><b>Topic:</b> Threat Management &amp; Intelligence Gathering</p> <p><b>Readings:</b> As assigned in classroom</p> <p><b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Cyber threats</li> <li>○ Cyber threat categories</li> <li>○ Threat taxonomies</li> <li>○ Threat frameworks</li> <li>○ Threat actors</li> <li>○ Threat hunting</li> <li>○ Threat modeling</li> <li>○ Threat detection solutions</li> <li>○ Threat metrics</li> <li>○ Threat maps</li> <li>○ Advisory profiles</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Threat actor profile</li> <li>○ Case study – Physical threat taxonomy</li> <li>○ Lab – None</li> </ul>
10	<p><b>Topic:</b> Attack Surface &amp; Vulnerability Management</p> <p><b>Readings:</b> As assigned in classroom</p> <p><b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Attack surface classification and management</li> <li>○ Attack surface mapping</li> <li>○ Shadow IT</li> <li>○ Vulnerability management overview</li> <li>○ Vulnerability scanning</li> <li>○ Patch management</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Attack surface</li> <li>○ Case study – Security testing approaches</li> <li>○ Lab – None</li> </ul>
11	<p><b>Topic:</b> Risk Management</p> <p><b>Readings:</b> As assigned in classroom</p> <p><b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Cyber risk landscape</li> <li>○ Risk appetite and tolerance</li> <li>○ Risk threshold and acceptance</li> <li>○ Inherent vs. residual risk</li> <li>○ Annualized loss expectancy (ALE)</li> <li>○ Cyber risk assessments</li> <li>○ Business Impact assessments (BIA)</li> <li>○ Risk registry</li> <li>○ Cyber risk frameworks, standards and models</li> </ul>

Week	Assignments
	<ul style="list-style-type: none"> <li>○ Cyber risk treatment plans</li> <li>○ Risk monitoring and management</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Quantitative vs qualitative risk advantages and disadvantages</li> <li>○ Case study – Most commonly used risk models</li> <li>○ Lab – Risk assessment</li> </ul>
12	<p><b>Topic:</b> Incident Response &amp; Operations Integration</p> <p><b>Readings:</b> As assigned in classroom</p> <p><b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Incident response overview</li> <li>○ Incident response model</li> <li>○ Incident response management products</li> <li>○ Security automation and orchestration (SAO)</li> <li>○ DevSecOps overview</li> <li>○ DevSecOps factory model</li> <li>○ Software-defined security (SDSec)</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Quantitative vs qualitative risk advantages and disadvantages</li> <li>○ Case study – Security stories</li> <li>○ Lab – Risk assessment</li> </ul>
13	<p><b>Topic:</b> Defense-in-Depth Strategy</p> <p><b>Readings:</b> As assigned in classroom</p> <p><b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Defense-in-depth overview</li> <li>○ OSI security model and countermeasures</li> <li>○ Depth-in-depth layers</li> <li>○ GRC domain</li> <li>○ Threat and vulnerability management domain</li> <li>○ Application, database and software security domain</li> <li>○ Security operations (SecOps) domain</li> <li>○ Device and data protection domain</li> <li>○ Cloud service and infrastructure protection domain</li> <li>○ Zero-trust model</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Success or failure of deploying a zero-trust model</li> <li>○ Case study – OSI Model threat alignment</li> <li>○ Lab – Risk assessment</li> </ul>
14	<p><b>Topic:</b> Security Program Testing</p> <p><b>Readings:</b> As assigned in classroom</p> <p><b>Key Concepts:</b></p>



Week	Assignments
	<ul style="list-style-type: none"> <li>○ Security testing overview</li> <li>○ Penetration testing</li> <li>○ Red teaming</li> <li>○ Bug bounties</li> <li>○ War gaming</li> <li>○ Tabletop testing</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Success of commercial bug bounty programs</li> <li>○ Case study – Inhouse vs. contracted penetration advantages and disadvantages</li> <li>○ Lab – Ransomware simulation</li> </ul>
15	<p><b>Topic:</b> Service Management</p> <p><b>Readings:</b> As assigned in classroom</p> <p><b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Information Technology Service Management (ITSM)</li> <li>○ Cybersecurity service management</li> <li>○ Cybersecurity service management framework</li> <li>○ Service management catalog</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – None</li> <li>○ Case study – None</li> <li>○ Lab – Service management catalog</li> </ul>
16	<p><b>Topic:</b> Program Management Disciplines &amp; Team Project Presentation</p> <p><b>Readings:</b> As assigned in classroom</p> <p><b>Key Concepts:</b></p> <ul style="list-style-type: none"> <li>○ Budget management</li> <li>○ Procurement</li> <li>○ Project management</li> <li>○ Cybersecurity insurance</li> <li>○ Third-party risk management</li> </ul> <p><b>Assignments:</b></p> <ul style="list-style-type: none"> <li>○ Participate in classroom discussions</li> <li>○ Paper – Team project paper</li> <li>○ Case study – None</li> <li>○ Lab – None</li> </ul>



### Instructor Notes

The following are important notes for institutions considering incorporating Building an Effective Cybersecurity Program as part of their cybersecurity curriculum:

- The sample syllabus can be used in both an 8-week and 16-week configuration.

- The course can be delivered as a 100-level to Master-level format. The emphasis of depth would be applied by the instructor. Labs, case studies and papers can be made more complex to match the course level.
- Papers, case studies and labs are suggestions, many other materials exist within the text to create other projects.
- The total estimated classroom time is 48 hours.
- The total projected study and project time is 48 hours.
- Completion of the course would prepare students to sit for one of the following information security certifications:
  - CompTIA® Security+
  - Global Information Assurance Certification (GIAC)
  - ISACA – CSX Cybersecurity Fundamentals Certificate

**Note:** Noted certifications do not require job experience.

## **Support**

Institutions committing to this coursebook would receive the following support:

- Author will guest lecture via Skype on a topic related to the course material for one-hour.
- Author will provide two hours of instructor phone and/or email support during the first semester the course is taught.
- Course delivery materials provided consist of instructor sample syllabus, delivery courseware, activity assignments, and a test bank of 50 questions.