CYBERSECURITY TECHNOLOGY MANAGEMENT CERTIFICATE

The 3-course Cybersecurity Technology Management Certificate provides students with a background in both the technological and managerial skills needed to be an effective cybersecurity professional in today’s IT enterprises.

Students will learn how to assess how organizational preparedness against cyber threats and how to manage their aftermath, including ensuring continuity of IT functions. Students also develop a strategy for designing and building cloud security architectures. An emphasis on ethical, legal, policy and regulatory concerns is embedded throughout the program.

Curriculum

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPST 381</td>
<td>Cybersecurity Governance</td>
<td>3</td>
</tr>
<tr>
<td>CPST 382</td>
<td>Cybersecurity Incident Response Management</td>
<td>3</td>
</tr>
<tr>
<td>CPST 383</td>
<td>Cloud Security Strategy and Architecture</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Total Hours</td>
<td>9</td>
</tr>
</tbody>
</table>

Optional:

• Advanced Topics in Cybersecurity Technology Management: The optional course is included to address up-to-the-minute topics, such as emerging threats, insider threats, latest application delivery processes, and practices, etc.

Learning Outcomes

The Cybersecurity Technology Management Certificate is designed to give IT professionals a solid background in the skills needed to be an effective Cybersecurity Professional in today’s IT Enterprises.

Students in this program will be able to:

• Explain the strategic importance of effective, interdisciplinary, and multifunctional enterprise information security governance and information security management program and its execution
• Evaluate the effectiveness and potential application of multiple information security governance structures and information security management programs for variant enterprise scenarios with consideration for strategic, operational, ethical, social, environmental, and risk factors
• Apply foundational knowledge of governance, risk, and compliance (GRC) concepts as they relate to legal, regulatory, and standards-based environments, such as HIPAA, FISMA, NERC, PCI DSS, GLBA, SOX, FERPA, COPPA, and others. Students will describe and identify policy frameworks, legal and compliance implications, and best practices.
• Describe the phases associated with the preparation and organization of incident response operations; Define threat management and its role in incident response; Develop an incident response plan
• Identify the known threats, risks, vulnerabilities, privacy issues and regulatory requirements associated with Cloud-based IT services; Understand the concepts and guiding principles for designing and implementing appropriate safeguards and countermeasures for Cloud-based IT services
• Design and build secure Cloud architectures that assure secure isolation of physical and logical infrastructures.