



**School of Hi-Tech
and Cyber Security**
The Center for Designated Programs
Bar-Ilan University



ISACA



Certificate Studies Chief Information and Cyber Security Officers (CISO) and Data Protection Officers (DPO)

Authorised academy of international organizations:
ISC2 ISACA EC-COUNCIL

Bar-Ilan University, The Center for Designated Programs
The Unit for Structured Programs and Certificate Studies
hitech-school.biu.ac.il | 052-5886002 :טו197

* Non-academic studies



Chief Information Security Officer (CISO) & Data Protection Officer (DPO)

Including preparation for the international certifications:
CISSP, CISM, CC, CIPP/E, C|CISO

Academic Director: Mr. Eran Shaham, Manager of the School of Hi-Tech and Cyber Security

Academic Advisors: Mr. Oren Yeger, Adv. Efrat Grinbaum, Mr. Nitzan Levi and Mr. Hillel Kobrovski

With its extensive training experience in a range of information and cyber security professions, in both the technical and management areas, and with thousands of students filling positions in the Israeli and international markets, Bar-Ilan University is proud to present the most advanced program in Israel for training Chief Information Security Officers and Data Protection Officers.

Our program is the only one in Israel that awards two university certificates, CISO and DPO, and prepares its students for five international certifications. The program is taught by prominent lecturers in the field, and students completing the program are suitably qualified to fill the positions of Chief Information Security Officer and Data Protection Officer in global companies. **Thanks to the university's academic partnership with ISACA and ISC2, among the most well-known organizations in the information security field worldwide, students are taught by lecturers internationally certified by these organizations.**

A CISO is a Security Enabler in the organization. On the one hand the officer is familiar with the various aspects of information security and manages technological teams, and on the other hand has a sharp business perspective, thus is also proficient in risk management and in managing the information security budget. The CISO's role has grown in recent years due to growing and more stringent global regulatory requirements, alongside with the business needs of the organizations. Currently the CISO must also have an understanding of legal matters related to the technological field.

The DPO is the Data Protection Officer, who oversees the organization's data protection strategy and its implementation, in order to ensure GDPR compliance and familiarity with the CCPA. In Israel the DPO is also responsible for compliance with the Israeli Privacy Protection Regulations that entered into force in May 2018, as well as for fulfilling the conditions required from any company that maintains commercial relations with Europe.



Description of the Program

The course prepares the students for five prestigious international certifications:

- CC (Certified in Cybersecurity) offered by ISC2
- CISSP (Certified Information Systems Security Professional) offered by ISC2
- CISM (Certified Information Security Manager) offered by ISACA
- CIPP/E (Certified Information Privacy Professional) offered by IAPP
- C|CISO (Certified CISO) offered by the EC-Council

Passing the international exams, together with the Bar-Ilan University CISO certificate and DPO certificate, is an excellent entry point into a continuously developing field. It's the beginning of an interesting, challenging and rewarding career in a knowledge-intensive industry.

Advantages of the Program

- Preparation for two positions: CISO and DPO, in one intensive course.
- Bar-Ilan University awards two prestigious certificates to the graduates of the CISO course and the DPO course:
- In addition, the following certificates are also awarded:
 - INCD Cyber Defense Doctrine 2.0 completion certificate
 - ISC2 CC - Course completion certificate
 - ISC2 CISSP - Course completion certificate
 - ISACA CISM - Course completion certificate
- The only study course in Israel that prepares you for five prestigious international certifications awarded by the best organizations: CC, CISM, CIPP/E, CISSP, C|CISO.
- The educational team is comprised of information security officers with international experience and high-level certifications in the field.
- During the CISO and DPO course students meet hear lectures delivered by guest lecturers, who hold senior positions in the various cyber and data privacy protection field.
- Preparation for the international exams using a cloud platform developed for the course.
- Direct digital communication channels connecting the lecturers, students and the academic advisor.
- Recordings of the lectures enable students to review the study material, after the lecture, anytime and anywhere.
- Students are accompanied individually during and after the course of their studies.



Meet the Teaching Faculty in the CISO and DPO Course:

About the Academic Director and Manager of the School of Hi-Tech and Cyber Security, Mr. Eran Shaham:

- Rich experience of over 30 years as a lecturer and training manager in the cyber and information security fields.
- Manager of the School of Hi-Tech and Cyber Security at Bar-Ilan University.
- Manage the authorized training centers of the leading virtualization, networking and information security companies in the world – AWS, Amazon, VMware, EC-Council, Check Point, and ISC2, and trains integrators in advanced courses.
- Has been training Check Point customers and partners in advanced technologies for over 20 years.
- Established and managed certificate courses in computers at the Technion - Division of Continuing Education & External Studies at the Technion for 8 years in Tel Aviv, Haifa and Jerusalem.
- Established and managed the Malam-Team Group Malam Team Training Center, responsible for training the Group's 4,000 employees.
- Managed the information security community at Microsoft Israel.

About the Academic Advisor, Mr. Oren Yeger:

- Cloud architect and cyber protection expert.
- Rich experience in technology training in the IDF and in the academy
- The professional leader and senior lecturer in the combined CISO & DPO course at Bar-Ilan University, and holds international certifications – CISSP and CISM.
- Served in the IDF 8200 Unit, and has 25 years of experience in international enterprise companies, among them IBM and Oracle, in core positions in the IT, middleware and cloud fields.
- Recognized as an AWS Accredited Educator and an AWS Community Builder, and helps plan cloud security solutions in technologically challenging environments.
- CISO and DPO positions in recent years, as well as a senior consultant.



About the Academic Advisor, Mr. Hillel Kobrovski:

- Strategy consultant and technology mentor in the following fields: cybersecurity, technology trends and forecasts, organizational innovation, technology futurology, and professional technological training.
- Assistance and accompaniment of technology companies in business and marketing development: development of new products and services, new marketing and distribution channels, preparing business and strategic plans, establishing training and professional development centers.
- Senior lecturer on technological innovation: efficiency, computing miniaturization, green development.
- Over 19 years of training experience, of thousands of students and hundreds of courses and lectures.
- A certified Check Point instructor since 1999, a senior Trainer at Fortinet since 2007, and a senior instructor at Cisco Israel since 2018.

About the Academic Advisor, Adv. Efrat Grinbaum:

- Professional lead of DPO course content.
- Over 12 years of experience in areas of data privacy law.
- Privacy Manager, manages the privacy area in Israel of the multinational corporation Johnson & Johnson in Israel.
- A partner in founding MyEDPO, that accompanies Israeli and global companies and organizations in Israel and around the world/worldwide on/regarding compliance with the various privacy regulations and provides DPO services to dozens of companies in different and varied activity areas.
- Holds an LL.B from Bar-Ilan University and an MBA from the College of Management Academic Studies.
- Lectures at international conferences and teaches courses and workshops on privacy.
- Has extensive familiarity with GDPR regulations and other/additional privacy regulations, from characterization/specifications to methodology integration in organizations. Also engages in accompanying organizations in complying with Israeli Privacy Protection Regulations.



About the Academic Advisor, Mr. Nitzan Levi:

- Holds a B.Sc in Software Engineering, and an M.A. in Governance with a specialization in Counter-Terrorism and Homeland Security from Reichman University.
- Certified systems analyst from the Israeli Chamber of Information Technology.
- Certified ISC2 and ISACA lecturer.
- Rich/Extensive training experience, with a focus on information security courses, technology courses and in secure development.
- Cyber protection, secure development and IT audit expert.
- 18 years of experience in software development, architecture, information security and cyber, acquired while filling a range of positions in the software and high-tech industry in Israel.
- In recent years fills the position of Information Security Manager, managing development, leading international projects and senior consultant on cyber and information security.

Target Audience

- Those with a business background, who want to incorporate security management into their profession.
- Individuals with physical security background.
- Graduates of Bar-Ilan University CND – Certified Network Defender course.

Prerequisites

- Students must have an entry level of technical terms in English.
- Pass an admission interview with the academic advisor.

Course Format

- **Course begins: August 1st, 2024.**
- **Course duration:** about seven months, Mondays and Thursdays, 05:30 – 09:30 PM.
- The course curriculum includes **270 academic hours.**



Tuition

- **Registration fee:** 480 NIS.
- **Tuition:** 15,000 NIS.

Course location

- The course takes place at the School of Hi-Tech and Cyber Security, Bar-Ilan University campus, Ramat Gan and simultaneously via Zoom.

Certificate Eligibility

- 80% class attendance (or via Zoom) and completing all course assignments is required.
- Students who fulfill the course requirements, will be awarded two certificates from Bar-Ilan University, the School of Hi-Tech and Cyber Security.

Comments

- The opening of the program will be subject to the number of registrants.
- The registration fee is not included in the tuition and is **non-refundable**, except in the event the course does not open, subject to the Bar-Ilan University certificate studies rules and regulations.
- The School of Hi-Tech and Cyber Security informs registrants that there may be changes in the program curriculum, in the class schedule or in any other matter. Notification of any change shall be given to registrants, subject to the Bar-Ilan University certificate studies rules and regulations .

Registration Procedures

- Course registration will be conducted through Eran Shaham Ltd, for Bar-Ilan University.

For details and registration
please contact:

Esther Asulin

052-5886002

esther.asulin@biu.ac.il

Sample Certificates



Curriculum

The program is comprised of fourteen domains areas, which prepare students for the international exams, and together provide in-depth acquaintance with the world and roles of the CISO & DPO.

Domain 1: Preparation

- Understand the three different lab topologies.
- Defense technologies in a complex firewall lab.
- Attack technologies in a complex attack lab.
- Evaluation of defense and attack tools and methods.

Domain 2: Security and Risk Management

- Apply concepts of confidentiality, integrity and availability.
- Evaluate and apply security governance principles.
- Determine compliance requirements.
- Understand legal and regulatory issues that pertain to information security in a global context.
- Understand, adhere to, and promote professional ethics.
- Develop, document, and implement security policy, standards, procedures, and guidelines.
- Identify, analyze, and prioritize Business Continuity (BC) requirements.
- Contribute to and enforce personnel security policies and procedures.
- Understand and apply risk management concepts.
- Understand and apply threat modeling concepts and methodologies.



- Apply risk-based management concepts to the supply chain.
- Establish and maintain a security awareness, education, and training program.
- Integrate risk, threat and vulnerability identification and management into life cycle processes (e.g., project management, development, and procurement and employment life cycles).
- Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven basis.

Domain 3: Asset Security

- Identify and classify information and assets.
- Determine and maintain information and asset ownership.
- Ensure appropriate asset retention.
- Determine data security controls.
- Establish information and asset handling requirements.

Domain 4: Privacy

- Data protection laws.
- Personal data.
- Controllers and processors.
- Processing personal data.
- Information provision.
- Data subjects' rights.
- Security of processing.
- Accountability.
- Cross-border data transfers.
- Supervision and enforcement.
- Compliance.
- Privacy governance.
- Applicable laws and regulations.
- Data assessments.
- Policies.
- Training and awareness.
- Protecting personal information.
- Data breach incident plans.
- Israeli Privacy Protection Regulations that entered into force in May 2018.
- GDPR Regulations and CCPA Regulations.



Domain 5: Information Security Governance, Program Development and Management

- Develop an information security strategy aligned with business goals and objectives.
- Align information security strategy with corporate governance.
- Develop business cases justifying investment in information security.
- Identify current and potential legal and regulatory requirements affecting information security.
- Identify drivers affecting the organization and their impact on information security.
- Obtain senior management commitment to information security.
- Define roles and responsibilities for information security throughout the organization.
- Establish internal and external reporting and communication that support information security.
- Develop and maintain plans to implement the information security strategy.
- Specify the activities to be performed within the information security program.
- Ensure alignment between the information security program and other assurance functions (e.g., physical, human resources, quality, IT).
- Identify internal and external resources (e.g., finances, people, equipment, Systems) required to execute the information security program.
- Ensure the development of information security architectures (e.g., people, processes, technology).
- Establish, communicate and maintain information security policies that support the security strategy.
- Design and develop a program for information security awareness, training and education.
- Ensure the development, communication, and maintenance of standards, procedures and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.
- Integrate information security requirements into the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement).
- Develop a process to integrate information security controls into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties).
- Establish metrics to evaluate the effectiveness of the information security program.
- Ensure that noncompliance issues and other variances are resolved in a timely manner.



Domain 6: Security Architecture and Engineering

- Implement and manage engineering processes using secure design principles.
- Understand the fundamental concepts of security models.
- Select controls based upon systems security requirements.
- Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption).
- Assess and mitigate the vulnerabilities of security architectures and solution elements.
- Assess and mitigate vulnerabilities in web-based systems.
- Assess and mitigate vulnerabilities in mobile systems.
- Assess and mitigate vulnerabilities in embedded devices.
- Apply cryptography.
- Apply security principles to site and facility design.
- Implement site and facility security controls.
- The security implications of the adoption of emerging technologies.

Domain 7: Communication and Network Security

- Communication and network security fundamentals.
- Implement secure design principles in network architectures.
- Implement secure communication channels according to design.
- Security of networks, systems, applications and data.
- Security Architecture principles.

Domain 8: Identity and Access Management (IAM)

- Control physical and logical access to assets.
- Manage identification and authentication of people, devices, and services.
- Integrate identity as a third-party service.
- Implement and manage authorization mechanisms.
- Manage the identity and access provisioning lifecycle.

Domain 9: Security Assessment and Testing

- Design and validate assessment, test, and audit strategies.
- Conduct security control testing.
- Collect security process data (e.g., technical and administrative).
- Analyze test output and generate report.
- Conduct or facilitate security audits.



Domain 10: Security Operations

- Understand and support investigations.
- Understand requirements for investigation types.
- Conduct logging and monitoring activities.
- Securely provisioning resources.
- Understand and apply foundational security operations concepts.
- Apply resource protection techniques.
- Operate and maintain detective and preventative measures.
- Implement and support patch and vulnerability management.
- Understand and participate in change management processes.
- Implement recovery strategies.
- Implement Disaster Recovery (DR) processes.
- Test Disaster Recovery Plans (DRP).
- Participate in Business Continuity (BC) planning and exercises.
- Implement and manage physical security.
- Address personnel safety and security concerns.

Domain 11: Software Development Security

- Understand and integrate security in the Software Development Life Cycle (SDLC).
- Identify and apply security controls in development environments.
- Assess the effectiveness of software security.
- Assess security impact of acquired software.
- Define and apply secure coding guidelines and standards.

Domain 12: Cloud Security

- Cloud Architecture.
- Cloud Governance and Enterprise Risk Management.
- Cloud Legal Issues: Contracts and Electronic Discovery.
- Cloud Compliance and Audit Management.
- Cloud Identity, Entitlement, and Access Management.
- Security as a Service.
- ENISA: Benefits, Risks and Recommendations for Information Security.



Domain 13: Incident Management and Response

- Develop and implement processes for detecting, identifying, analyzing and responding to information security incidents.
- Establish escalation and communication processes and lines of authority.
- Develop plans to respond to, and document, information security incidents.
- Establish the capability to investigate information security incidents (e.g. forensics, evidence collection and preservation, log analysis, interviewing).
- Develop a process to communicate with internal parties and external organizations (e.g., media, law enforcement, customers).
- Integrate information security incident response plans with the organization's Disaster Recovery (DR) and business continuity plan.
- Organize, train, and equip teams to respond to information security incidents.
- Periodically test and refine information security incident response plans.
- Manage the response to information security incidents.
- Conduct reviews to identify causes of information security incidents, develop corrective actions and reassess risk.

Domain 14: Final Steps for becoming a CISO

- Strategic Planning.
- Designing, Developing, and Maintaining an Enterprise Information Security Program.
- Understanding the Enterprise Architecture (EA).
- Understanding the Organization's Procurement Program.
- Vendor Management.
- CISO presentation in front of the Board & Senior Management.
- Information Security best practices.
- Final project presentation in class.
- How to become the CISO you want to be.

**** The Center for Designated Programs reserves the right to change the study curriculum**