



# **11. Certificări profesionale în domeniul securității informațiilor**



# Certificarea profesională

---

- **Demonstrarea competențelor într-un anumit domeniu**
  - pe nivele: debutant, practician, profesionist
  - pe specializări: arhitectură, management, inginerie, audit, FW, IDS, etc
- **Beneficii pentru individ**
  - creșterea salariului
- **Beneficii pentru firmă**
  - avantaj competițional
- **Certificări independente**
  - CISA, CISM, CISSP, CEH, etc
- **Certificări pe o anumită tehnologie**
  - Microsoft, CISCO, Linux, etc
- **Centre independente de testare**
  - Centre specializate supervizate de organismele de certificare
  - Firme internaționale de testare: Pearson VUE, Thomson Prometric
- **Test grilă / pe calculator**



# Certificări independente



# International Information Systems Security Certification Consortium (ISC)<sup>2</sup>

---

- Organizație nonprofit, înființată în 1989 în USA
  - [www.isc2.org](http://www.isc2.org)
- A dezvoltat “CBK- Common Body of Knowledge” și un program de certificare pentru profesioniștii din domeniul securității sistemelor informatice
- Certificări oferite:
  - Certified Information Systems Security Professional (CISSP)
  - Certification and Accreditation Professional (CAP)
  - Systems Security Certified Practitioner (SSCP)
  - (ISC)<sup>2</sup> Associate
- Peste 63.000 de membrii certificați, din 138 de țări

# Certified Information Systems Security Professional (CISSP)

- Una din cele mai recunoscute certificări profesionale în domeniu
- 10 domenii de examinare:
  - Access Control
  - Application Security
  - Business Continuity and Disaster Recovery Planning
  - Cryptography
  - Information Security and Risk Management
  - Legal, Regulations, Compliance and Investigations
  - Operations Security
  - Physical (Environmental) Security
  - Security Architecture and Design
  - Telecommunications and Network Security
- Test grilă, 250 de întrebări multiple-choice, 6 ore, 700/1000 puncte
- Minim 4 ani de experiență în domeniu
- Aderarea la Codul de Etică Profesională al (ISC)<sup>2</sup>
- Instruire continuă pentru a putea păstra certificarea - minim 120 puncte CPE (Continuing Professional Education) la fiecare 3 ani
  - participarea la cursuri, conferințe, seminarii, etc.

# CISSP Concentrations (direcții de aprofundare)

- **Information Systems Security Architecture Professional (ISSAP) – 6 domenii de examinare**
  - Access Control Systems and Methodology
  - Cryptography
  - Physical Security Integration
  - Requirements Analysis and Security Standards, Guidelines and Criteria
  - Technology Related Business Continuity and Disaster Recovery Planning
  - Telecommunications and Network Security
- **Information Systems Security Engineering Professional (ISSEP) – 4 domenii de examinare**
  - Certification and Accreditation
  - Systems Security Engineering
  - Technical Management
  - U.S. Government Information Assurance Regulations
- **Information Systems Security Management Professional (ISSMP) – 5 domenii de examinare**
  - Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) and Continuity of Operations Planning (COOP)
  - Enterprise Security Management Practices
  - Enterprise-wide System Development Security
  - Law, Investigations, Forensics, and Ethics
  - Overseeing Compliance of Operations Security

# Certification and Accreditation Professional (CAP)

---

- Se adresează profesioniștilor implicați în procesul de certificare și acreditare a securității sistemelor informatice
- 5 domenii de examinare:
  - Understanding the Purpose of Certification
  - Initiation of the System Authorization Process
  - Certification Phase
  - Accreditation Phase
  - Continuous Monitoring Phase
- Minim 2 ani de experiență în domeniu
- Aderarea la Codul de Etică Profesională al (ISC)<sup>2</sup>
- Raportarea a minim 60 puncte CPE la fiecare 3 ani

# Systems Security Certified Practitioner (SSCP)

---

- **Se adresează specialiștilor ce implementează soluții de securitate**
- **7 domenii de examinare:**
  - Access Controls
  - Analysis and Monitoring
  - Cryptography
  - Malicious Code
  - Networks and Telecommunications
  - Risk, Response and Recovery
  - Security Operations and Administration
- **Test grilă, 125 de întrebări multiple-choice, 3 ore**
- **Minim 1 ani de experiență în domeniu**
- **Aderarea la Codul de Etică Profesională al (ISC)<sup>2</sup>**
- **Raportarea a minim 60 puncte CPE la fiecare 3 ani**



# Information Systems Audit and Control Association (ISACA)

- Asociație profesională, fondată în 1967 în USA
  - [www.isaca.org](http://www.isaca.org)
- Elaborarea de standarde cu privire la auditarea, controlul și guvernarea sistemelor informatice
- 170 de filiale în peste 60 de țări, peste 80.000 de membrii
- Publicații:
  - Standarde, ghiduri și proceduri pentru auditarea sistemelor informatice
  - Control Objectives for Information and related Technology (COBIT) v4.1
    - set de best practices (framework) pentru managementul IT într-o organizație
    - elaborat împreună cu IT Governance Institute (ITGI) în 1996
  - Information System Control Journal
- Certificări oferite:
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)
  - Certified in the Governance of Enterprise IT (CGEIT)

# Certified Information System Auditor (CISA)

- **Certificare apreciată și recunoscută pe scară largă**
- **Se adresează profesioniștilor cu experiență în domeniul auditării, controlului și securității informațiilor**
- **6 domenii de examinare:**
  - **IS Audit Process (10%)**
  - **IT Governance (15%)**
  - **Systems and Infrastructure Lifecycle Management (16%)**
  - **IT Service Delivery and Support (14%)**
  - **Protection of Information Assets (31%)**
  - **Business Continuity and Disaster Recovery (14%)**
- **Test grilă, 200 de întrebări multiple-choice, 4 ore, 450/800 puncte**
- **Minim 5 ani de experiență**
- **Aderarea la Codul de Etică Profesională al ISACA**
- **Respectarea standardelor de auditare promulgate de ISACA**
- **Raportarea a minim 20 puncte CPE anual și acumularea a minim 120 puncte CPE la fiecare 3 ani**

# Certified Information Security Manager (CISM)

- **Certificare apreciată și recunoscută pe scară largă**
- **Se adresează profesioniștilor cu experiență în domeniul managementului securității informațiilor**
- **5 domenii de examinare:**
  - Information Security Governance (23%)
  - Information Risk Management (22%)
  - Information Security Program Development (17%)
  - Information Security Program Management (24%)
  - Incident Management and Response (14%)
- **Test grilă, 200 de întrebări multiple-choice, 4 ore, 450/800 puncte**
- **Minim 5 ani de experiență**
- **Aderarea la Codul de Etică Profesională al ISACA**
- **Raportarea a minim 20 puncte CPE anual și acumularea a minim 120 puncte CPE la fiecare 3 ani**

# Certified in the Governance of Enterprise IT (CGEIT)

- **Certificare relativ nouă (2007)**
- **Se adresează profesioniștilor care ocupă poziții management în cadrul unei organizații și au experiență în guvernarea și controlul IT**
- **6 domenii de examinare:**
  - **IT Governance Framework (25%)**
  - **Strategic Alignment (15%)**
  - **Value Delivery (15%)**
  - **Risk Management (20%)**
  - **Resource Management (13%)**
  - **Performance Measurement (12%)**
- **Test grilă, 120 de întrebări multiple-choice, 4 ore, 450/800 puncte**
- **Minim 5 ani de experiență**
- **Aderarea la Codul de Etică Profesională al ISACA**
- **Raportarea a minim 20 puncte CPE anual și acumularea a minim 120 puncte CPE la fiecare 3 ani**

# SANS Institute

- **SysAdmin, Audit, Networking, and Security**
  - [www.sans.org](http://www.sans.org)
- **Fondată în 1989 ca organizație de cercetare și educație**
- **Cea mai mare sursă de informare pentru instruire în domeniul securității informațiilor**
  - Storm Center, news digest (NewsBites), vulnerability digest (@RISK), flash security alerts, peste 1.200 articole originale
  - majoritatea resurselor sunt free pentru cine întreabă
- **Cursuri de instruire în domeniul securității informațiilor**
- **Peste 165.000 de membrii din întreaga lume**
- **A înființat programul de certificare Global Information Assurance Certification (GIAC)**
  - [www.giac.org](http://www.giac.org)
- **Certificări oferite (extras):**
  - GIAC Security Essentials Certification (GSEC)
  - GIAC Certified Firewall Analyst (GCFW)
  - GIAC Certified Windows/UNIX Security Administrator (GCWN/GCUX)
  - GIAC Secure Software Programmer (GSSP-C/Java/NET)
  - GIAC Systems and Network Auditor (GSNA)
  - GIAC Certified Penetration Tester (GPEN)

# GIAC Security Essentials Certification (GSEC)

- Se adresează celor care vor să demonstreze că stăpânesc principiile securității informațiilor și sunt capabili să implementeze soluții de securitate
- Domenii acoperite de certificare:
  - Risk Assessment and Auditing
  - Host and Network Based Intrusion Detection
  - Honeypots, Firewalls and Perimeter Protection
  - Security Policy
  - Password Management
  - Security Incident Handling - The Six Steps
  - Information Warfare
  - Web Security
  - Network Fundamentals and IP Concepts and Behavior
  - Cisco Router Filters
  - Four Primary Threats for Perimeter Protection
  - PGP, Steganography
  - Anti-Viral Tools
  - Windows (2000, XP, 2003, Vista) Security Administration and Auditing
  - IIS Security
  - Unix Security Fundamentals
- Test grilă, 180 de întrebări, 5 ore, 70% (126 răspunsuri corecte)
- Recertificare la fiecare 4 ani

# International Council of Electronic Commerce Consultants (EC-Council)

---

- Organizație profesională ce are drept scop dezvoltarea comerțului electronic, stabilirea de standarde profesionale, educarea și certificarea
  - [www.eccouncil.org](http://www.eccouncil.org)
- Certificări oferite:
  - Certified Ethical Hacker (CEH)
  - Certified EC-Council Instructor (CEI)
  - Computer Hacking Forensic Investigator (CHFI)
  - EC-Council Certified Security Analyst (ECSA)
  - Certified Network Defense Architect (CNDA)
  - Licensed Penetration Tester (LPT)
  - EC-Council Certified VOIP Professional (ECVP)
  - EC-Council Network Security Administrator
  - EC-Council Certified Computer Investigator

# Certified Ethical Hacker (CEH)

---

*"To catch a thief, you must think like a thief. To protect your network from a hacker, you've got to get inside that hacker's mind."*

- **Presupune parcurgerea cursului "Ethical Hacking and Countermeasures"**
- **Testare la VUE / Prometric, 50 de întrebări multiple-choice, 2 ore, 70%**
- **Instruire continuă pentru a putea păstra certificarea - minim 20 puncte ECE (EC-Council Continuing Education Credits ) pe an**



# British Standards Institute (BSI)

---

- Organismul de standardizare din UK
  - [www.bsi-global.com](http://www.bsi-global.com)
- Fondat în 1901, are peste 5000 de angajați în 110 țări
- Domenii de activitate:
  - dezvoltarea de standarde private, naționale și internaționale
  - certificarea sistemelor și produselor
  - inspecția mărfurilor
  - training și certificări
- BS 7799-1, 7799-2 ⇔ ISO 17799 ⇔ ISO 27001, 27002
- Certificări oferite:
  - ISO 27001:2005 Lead Auditor

# ISO 27001:2005 Lead Auditor

- **Curs de instruire de 5 zile, examinare la final în vederea obținerii certificatului**
  - Information security
  - The importance of information security
  - ISO 27001:2005
  - Reviewing security threats and vulnerabilities
  - Management of security risks
  - Selecting security controls
  - How to build an Information Security Management System (ISMS)
  - ISO 27001:2005 auditing techniques
  - Managing and leading an ISO 27001:2005 audit team
  - Interview techniques
  - Audit reporting
- **Pentru a putea emite astfel de certificări, cursul trebuie să fie înregistrat la International Register of Certificated Auditors (IRCA)**

# British Computer Society (BCS)/ Information Systems Examination Board (ISEB)

---

- Asociația specialiștilor IT, înființată în 1957 în UK
  - [www.bcs.org](http://www.bcs.org)
- Information Systems Examinations Board (ISEB) este organismul de certificare al BCS
  - certificări profesionale recunoscute de industrie, inclusiv in domeniul securității informațiilor
  - [www.iseb.org.uk](http://www.iseb.org.uk)
- Certificări oferite:
  - Certificate in Information Security Management Principles (CISMP)

# Certificate in Information Security Management Principles (CISMP)

---

- Se adresează debutanților în domeniul securității informațiilor
- Domenii de examinare:
  - Concepts & Definitions
  - Information Risk
  - Information Security Framework
  - Information Security Controls
- Test grilă, 100 de întrebări multiple-choice, 2 ore, 65/100

# Computing Technology Industry Association (CompTIA)

---

- **Organizație non-profit creată în 1982 având ca misiune dezvoltarea industriei IT**
  - [www.comptia.org](http://www.comptia.org)
- **Standarde, competențe profesionale, educație și soluții de business**
- **Certificări oferite:**
  - **CompTIA A+**
  - **CompTIA Network+**
  - **CompTIA Server+**
  - **CompTIA Linux+**
  - **CompTIA Security+**
- **Certificările oferite de CompTIA sunt recunoscute de foarte multe organizații: IBM, Microsoft, RSA Security, etc.**

# CompTIA Security+

---

- **Se adresează debutanților în domeniul securității informațiilor**
- **5 domenii de examinare:**
  - **General Security Concepts (30%)**
  - **Communication Security (20%)**
  - **Infrastructure Security (20%)**
  - **Basics of Cryptography (15%)**
  - **Operational / Organizational Security 15%**
- **Test grilă, 100 de întrebări multiple-choice, 1,5 ore, 750/900**
  - **Pearson VUE / Thompson Prometric**
- **Peste 45,000 persoane certificate**

# Alte certificări

---

- **Security Certified Network Professional (SCNP) / Security Certified Network Architect (SCNA)**
  - [www.securitycertified.net](http://www.securitycertified.net)
- **TruSecure ICSA Certified Security Associate (TICSA)**
  - [www.trusecure.com](http://www.trusecure.com)
- **CERT Certified Computer Security Incident Handler (CSIH)**
  - [www.cert.org](http://www.cert.org)



# Certificări pe o anumită tehnologie





# Microsoft

---

- **Microsoft Certified System Administrator (MCSA) – Security**
  - 2 examene pe networking
  - 1 examen pe sisteme de operare client
  - 2 examene de specializare pe securitate din care 1 poate fi echivalat cu o certificare independentă (CompTIA)
- **Microsoft Certified Systems Engineer (MCSE) – Security**
  - 4 examene pe networking
  - 1 examen pe sisteme de operare client
  - 1 examen de design de soluții securitate
  - 2 examene de specializare pe securitate din care 1 poate fi echivalat cu o certificare independentă (CompTIA)
- <http://www.microsoft.com/learning/mcp/default.msp>

# CISCO

---

- **CCNA Security**
  - CCNA + 1 Exam
- **Cisco Certified Security Professional (CCSP)**
  - CCNA Security + 5 Exams
- **CCIE Security**
- **Cisco ASA / IPS / NAC Specialist**
  - CCNA Security + 1 Exam
- [http://www.cisco.com/web/learning/le3/learning\\_career\\_certifications\\_and\\_learning\\_paths\\_home.html](http://www.cisco.com/web/learning/le3/learning_career_certifications_and_learning_paths_home.html)

# Alte certificări

---

- **Sun Microsystems**
  - Sun Certified Security Administrator (SCSECA)
- **Check Point**
  - Check Point Certified Security Principles Associate (CCSPA)
  - Check Point Certified Security Administrator (CCSA)
  - Check Point Certified Security Expert (CCSE)
  - Check Point Certified Managed Security Expert (CCMSE)
  - Check Point Certified Master Architect (CCMA)
- **RSA Security**
  - RSA Certified Systems Engineer – SecurID / PKI
- **Symantec**
  - Symantec Technology Architect (STA)
  - Symantec Certified Security Engineer (SCSE)
  - Symantec Certified Security Practitioner (SCSP)

