WHY CISSP® CERTIFICATION?
The CISSP Certification is an independent and objective measure of professional expertise and knowledge within the information security profession. In June 2004, the CISSP was the first information security credential accredited by ANSI (American National Standards Institute) to ISO Standard 17024:2003.

If you plan to build a career in information security — one of today's most visible professions — and if you have at least four full years of experience in information security, or three years and an university degree, then CISSP certification should be your next career goal.

HOW CISSP® BENEFITS YOU
The CISSP credential is a key differentiator in the selection process for information security positions, new assignments or promotions. When you achieve the CISSP designation:
• You indicate you have measured up to a globally accepted professional and ethical standard.
• You have obtained recognition and acceptance as a career professional.
• Your career opportunities are significantly enhanced.
• You have demonstrated knowledge of and competence in the 10 domains of the (ISC)² CISSP CBK®.
• You possess an internationally recognised credential.

HOW CISSP® BENEFITS YOUR ORGANISATION
Organisations staffed with CISSPs gain a competitive edge. Because the personnel protecting their data are the best in the business, these organisations demonstrate to customers, suppliers, and employees alike, the importance they place on security. Additionally, the CISSP designation reflects a properly and consistently educated IT professional staff.

Steve Lodin joined global pharmaceutical and diagnostic organisation F. Hoffman La-Roche in 1999, a year after achieving his CISSP certification. He says: “I sat the exam when I was working as an IT security consultant because I felt the credentials it established would be valuable for my future career. Nowadays, when I am looking for people to join our team, I ask for CISSP as a preferred qualification because it shows a level of competence that we need.

“F. Hoffman La-Roche is governed by the Food and Drug Administration in the U.S. and we have to conform to their requirements for well maintained and secure systems. We’re also looking to work more and more with health information, using confidential patient data for which we must show due diligence. That’s why our network security is so crucial — we need competent, qualified people to deliver that security.”

Steve Lodin
– Head of Global IT Security - F. Hoffman-La Roche
"We must not only be risk averse but we must show ourselves to be so. Externally recognized accreditation of key IS personnel sends a clear message that we are taking our IT Security seriously. The bank pursues a programme of continued education and from a group perspective the CISSP is the most recognised security qualification available. It ensures a general level of competency as opposed to a number of others on the market, and it meets with the training requirements of Credit Suisse.

From a personal point of view, it was absolutely right for me to train for and then sit the CISSP exam. Technology is so fast moving that you can't possibly keep up with all the security issues that might have an impact on our infrastructure or applications.

The CISSP was a chance for me to maintain a level of knowledge that I cannot afford to lose."

Andrew Brice
– Head of IT Security Risk - Credit Suisse Group

CORPORATE CLASS PACKAGES
(ISC)² are delighted to offer tailored CISSP CBK Review Seminar packages to enable group education:
• Discounted seminar rates
• Seminar and exam vouchers option
• On-site seminar and exam delivery option
• Provision of official seminar materials and experienced (ISC)²-CISSP Instructor
• Professional coordination and support
• Designated account management from initial contact, through to sign off and beyond

For further information, please contact Donna Garner at: dgerner@itgoverance.co.uk or call 0845 070 1750

ISO/IEC 17024
"The (ISC)²-CISSP CBK is the most comprehensive and the best course I have ever been on. Highly recommended."

Johan Brink
– National Technology Risk Manager - South Africa

"The CBK Review Seminar gave me the opportunity to interact and learn more on the topics of IT security both from the trainer and the participants. This learning is definitely better than self-study. In a gist, the Seminar was concise, precise and accurate to fastrack the CISSP domains."

Tong See Chee
- Lucent Technology, Singapore

The Official (ISC)²® CISSP® CBK® Review Seminar
Most information security professionals specialise in only one or two of the CBK domains and typically have varying degrees of knowledge in the other eight or nine. In-depth knowledge of all 10 domains is required to pass the exam. For this reason (ISC)² has developed this intensive, five-day review seminar that will refresh your knowledge and broaden your understanding of all 10 CISSP CBK domains.

The Seminar provides:
• a complete overview of the scope of the CISSP CBK;
• a comprehensive review and discussion of the topics, subtopics, and sub-subtopics of the CISSP CBK domains;
• extensive knowledge-based materials and presentations developed by (ISC)² -authorised instructors and subject matter experts;
• a self-assessment consisting of 100 questions that test your knowledge of the CISSP CBK;
• a personal critique of your results to help you focus on the topic where you need more study;
• a comprehensive student guide that addresses all materials covered by the course
# The 10 Domains of the CISSP CBK

<table>
<thead>
<tr>
<th>Information Security and Risk Management</th>
<th>Business Continuity and Disaster Recovery Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification of an organisation's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines.</td>
<td>Addresses the preservation of the business in the event of outages to normal business operations.</td>
</tr>
<tr>
<td>a. Governance</td>
<td>a. Project Scope Development and Planning</td>
</tr>
<tr>
<td>b. Organisational Behaviour</td>
<td>b. Business Impact Analysis</td>
</tr>
<tr>
<td>c. Security Awareness, Training and Education</td>
<td>c. Emergency Assessment</td>
</tr>
<tr>
<td>d. Risk Management</td>
<td>d. Business Continuity and Recovery Strategy</td>
</tr>
<tr>
<td>e. Ethics</td>
<td>e. Implementation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Telecommunications and Network Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>A collection of mechanisms that work together to create a security architecture to protect the assets of the information system.</td>
<td>Includes network structures, transmission methods, transport formats, security measures, and authentication.</td>
</tr>
<tr>
<td>a. Information Classification</td>
<td>a. Network Types and Architectures</td>
</tr>
<tr>
<td>b. Access Control Categories, Types and Threats</td>
<td>b. Wireless Transmission Technologies</td>
</tr>
<tr>
<td>d. IDS and IPS</td>
<td>d. Traditional and VOIP Telephony</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cryptography</th>
<th>Application Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>The principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.</td>
<td>Outlines the environment where software is designed and developed and explains the critical role software plays in providing security to the information system.</td>
</tr>
<tr>
<td>b. Message Integrity Controls</td>
<td>b. Application Environment and Security Controls</td>
</tr>
<tr>
<td>c. Digital Signatures</td>
<td>c. Continuity of Operations</td>
</tr>
<tr>
<td>d. Encryption Management</td>
<td>d. System Threats and Vulnerabilities</td>
</tr>
<tr>
<td>e. Cryptanalysis and Attacks</td>
<td>e. Malicious Code</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical (Environmental) Security</th>
<th>Operations Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection techniques for the entire facility, including all of the information system resources.</td>
<td>Used to identify the controls over hardware, media, and operators and administrators with access privileges to any of these resources.</td>
</tr>
<tr>
<td>b. Building Infrastructure Protection</td>
<td>b. Physical Access Control</td>
</tr>
<tr>
<td>c. Physical Control Types</td>
<td>c. Continuity of Operations</td>
</tr>
<tr>
<td></td>
<td>d. Change Control Management</td>
</tr>
<tr>
<td></td>
<td>e. Security Administrator Privileges</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Architecture and Design</th>
<th>Legal, Regulations, Compliance and Investigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, applications and controls used to enforce various levels of availability, integrity, and confidentiality.</td>
<td>Addresses computer crime laws and regulations, investigative measures and techniques, and forensic evidence gathering.</td>
</tr>
<tr>
<td>a. Components and Principles</td>
<td>a. Major Legal Systems</td>
</tr>
<tr>
<td>b. Security Models and Architecture Theory</td>
<td>b. Information System and Internet Legal Concepts</td>
</tr>
<tr>
<td></td>
<td>d. Investigation</td>
</tr>
<tr>
<td></td>
<td>e. Computer Forensics</td>
</tr>
</tbody>
</table>

**NEXT STEPS:**
To evaluate your knowledge of the 10 domains of the CISSP CBK, you can download the free CBK Study Guide from the (ISC)² Website at www.isc2.org/studyguide.

Furthermore, you can take the (ISC)² online CISSP CBK Self-Assessment, a 100-item test based on the CISSP domains in the (ISC)² CBKs. This assessment tool has proven to be a very useful mechanism for candidates wishing to identify their areas of strength and weakness within the 10 CISSP domains. See www.isc2.org/selfassessment.