Please ensure that your presentation covers one or more of the (ISC)² Common Body of Knowledge (CBK) domains on the following page. It would also help if you identified the domains during your presentation. While we fully understand that you would like to distinguish yourself in the marketplace and attract new business, we kindly ask you to keep the presentation focused on education and information. You can certainly present the distinguishing features of your product and how it solves security issues.
Thank you for your understanding.

For more information or to become an (ISC)² U.S. Military Germany Chapter sponsor, contact any Chapter Board member or contact us using the information provided below:

Corporate Advisor
(ISC)² U.S. Military Germany Chapter
CMR 467 BOX 7000
APO AE 09096
corporateadvisor@isc2chapter-usmg.org

This policy will be reviewed and revised accordingly on an annual basis by the (ISC)² US Military Germany Chapter Board of Directors. This policy will be available for review on the Chapter website. All corporate sponsors will be responsible for reviewing this policy on an annual basis.

(ISC)² US Military Germany Chapter reserves the right to review and change the Sponsorship Program upon the recommendation and approval of the (ISC)2 US. Military Germany Chapter Board of Directors.

(ISC)^2 Common Body of Knowledge (CBK) Domains

Security and Risk Management

- Confidentiality, Integrity and Availability (CIA)
- Security Governance Principles
- Control Frameworks
- Due Care vs. Due Diligence
- CISSP for Legal and Investigation Regulatory Compliance
- Information Security Legal Issues
- Security Policies, Standards, Procedures and Guidelines
- Security Personnel
- Vendor, Consultant and Contractor Security
- Risk Management Concepts (Part 1)
- Risk Management Concepts (Part 2)
- Threat Modeling

Asset Security

- Information and Asset Classification
- Data and System Ownership (e.g. data owners, system owners)
- Protecting Privacy
- Data Retention
- Data Security Controls – protect data at rest or in transit, cryptography, etc.
- Data Handling Requirements (e.g. markings, labels, storage) – includes destruction
- Public Key Infrastructure (PKI)

Security Engineering

- Engineering processes using secure design principles
- Security models fundamental concepts
- Security evaluation models
- Certification and Accreditation
- Security capabilities of information systems
- Security architectures, designs, and solution elements vulnerabilities
- Web-based systems vulnerabilities
- Mobile systems vulnerabilities
- Embedded devices and cyber-physical systems vulnerabilities – includes IoT and devices in networks
- Database Architectures and Security
- Cryptography – PKI, digital signatures, keys, digital rights and cryptanalytic
- Site and facility design secure principles
- Physical security – flooding, fires, storage security and more strictly "physical" issues

Communications and Network Security

- Secure network architecture design (e.g. IP & non-IP protocols, segmentation) – wireless technology, cryptography applied to communications
- Secure network components – access control, transmission media, communication hardware

- Secure communication channels – VPN, VLAN, instant messaging, remote collaboration
- Firewalls, IDS & IPS
- Network attacks and countermeasures

Identity and Access Management

- Access Control Categories
- Identification and Authentication of people and devices – identity management, registration, credentials, techniques for authentication including biometrics.
- Authorization
- Identity as a Service (e.g. cloud identity)
- Third-party identity services (e.g. on premise)
- Access Control Attacks
- Identity and Access Provisioning Lifecycle (e.g. provisioning review)

Security Assessment and Testing

- Assessment and test strategies
- Security process data (e.g. management and operational controls)
- Security control testing
- Test outputs (e.g. automated, manual)
- Security architectures vulnerabilities

Security Operations

- Investigations support and requirements – digital forensics, regulatory concerns
- Logging and monitoring activities – IDPS, event management, monitoring of systems
- Provisioning of resources
- Foundational security operations concepts – assign roles, monitor access privileges, information lifecycle
- Resource protection techniques
- Incident management – from incident to remediation to after-incident review
- Preventative measures – IDPS, sandboxing, honeypots, firewall, malware prevention
- Patch and vulnerability management
- Change management processes
- Recovery strategies – backup, multiple operation sites
- Disaster recovery processes and plans
- Business continuity planning and exercises
- Physical security
- Personnel safety concerns

Software Development Security

- Security in the software development lifecycle
- Development environment security controls
- Software development models
- Software security effectiveness – auditing, risk analysis
- Acquired software security impact
- Software testing