

Moving IT Managers from “Have to” to “Want to” do Security!

Key Elements

How to effectively conduct and control certifications and accreditations.

-

Learn how to balance cost, responsibilities, and acceptable risk.

-

How organization’s operations, mission and culture influence security.

-

Non-technical explanations of complex IT security concepts, solutions and applications.

-

Gain a practical awareness of IT Security Concepts and Technology

-

Seminar is tailored to organization’s needs and objectives.

-

Understand strategies for determining which security solutions are the best.

-

Identify and find the real threats to your IT systems.

-

Presented by:

LITCHKO & ASSOCIATES, INC.
SECURE BUSINESS-BASED SOLUTIONS

IT Security: Practical, Positive, and Proactive

“How do I balance my mission, security, acceptable risk and budget?

“Do we meet OMB A-130 and FISMA requirements?”

“What is my IT system’s security risk?”

“How much security is enough?”

The key to answering these questions is to educate and motivate the information technology (IT) system’s program managers (PM) and Information Systems Owners (ISO), so they will “**want to**” take charge of their IT system’s security. Traditionally this has been a difficult “must do” task for them.

Many have tried enticing, directing, and encouraging their PM’s and ISO’s to conduct IT system’s security certifications and accreditations (C&A) and to correct the deficiencies. Approaches include using senior management directives, Inspector General (I.G.) audits, F.U.D. (fear, uncertainty and doubt), regulations, Presidential Decision Directives, and FISMA to encourage their PM’s and ISO’s. These approaches have proven to be only partially successful.

This one-day, non-technical, interactive, “motivational” seminar has achieved what the above attempts have not been able to accomplish: a major increase in PM’ and ISO’s requesting C&A’s and taking control of their IT system’s security. Why? Because the seminar provides them with confidence and an awareness of why supporting IT security is important to achieving their goals.

The seminar teaches them how to:

- conduct a C&A on their system,
- control the C&A process,
- work with IT security experts
- collaborate with other groups, and
- understand how C&A supports their professional and personal goals.

“...200% increase in requests for security assessments resulting from this course.”

Joseph Eley, IT Security Team, HRSA

By using this unique educational and motivational approach and tailoring each class to the PM’s organization’s mission and operations, this one-day seminar has proven highly effective for government PM’s and ISO’s.

This seminar is for those professionals who are responsible for oversight and management of an organization’s IT system security. Our past students been technical and non-technical individuals and have included: lawyers, nurses, managers, programmers, I.G. auditors, budgeters, and system security officers. This type of diversity provides the classes with the advantage of increased experience and knowledge on a variety of topics: organizational, managerial, fiscal, and technical. To take full advantage of this diversity, the instructors use the following approaches:

- Present a mission-based approach to solving IT security
- Explain technical concepts in non-technical, practical terms,
- Provide instruction that is tailored to the students’ organizations.
- Use interactive and cooperative-learning techniques.

This approach allows the students to become more confident with IT security. More important, it allows them to develop their own reasons for why conducting a C&A effort makes their job easier and supports their personal goals at work and home.

IT Security – Practical, Positive, and Proactive

Key Elements

Attendees interact collaboratively to find effective system security solutions.

-

Gain self-awareness of all the benefits of a conducting a C&A and being proactive.

-

Understand the relevant regulations and laws.

-

Learn to effectively interact with IT security professionals.

-

Course manual includes pertinent and dynamic security references

-

Augmented with real-world government case-studies

-

Highly-interactive, application-based and cooperative instruction.

-

Experienced IT security and management specialists.

-

Presented by:

LITCHKO & ASSOCIATES, INC.
SECURE BUSINESS-BASED SOLUTIONS

This eight-hour seminar is interactive, informative and instrumental in motivating the students to want to be proactive in securing their IT systems. To ensure that the students are confident with IT security and understand how to gain maximum leverage from the results of conducting a C&A, the seminar covers the following:

- Overview explanation of what the C&A processes are and the what the PM's, ISO's and other's responsibilities are.
- Strategies that make these processes relevant to the mission, clients, systems, regulations, policies and procedures.
- Introduction to the applicable regulation and directives.
- Components of a risk assessment: risks, threats, vulnerabilities, risk mitigation, risk management, options and recommendations.
- Basic security functions: confidentiality, integrity, availability, authentication, and non-repudiation.
- Security concepts related to the threats, vulnerabilities, requirements, countermeasures, risk management, and methods for reducing risk.
- How the results can be used to justify increases in personnel, equipment and funding to reduce residual risks.
- Facilitation techniques to gain inter-group collaboration and ownership of the results.

Each seminar provides eight to twenty students with the maximum learning experience. Using visual representations, cooperative-learning techniques, and case study analysis, the instructors will provide an efficient and interactive learning experience for the students.

Teaching this unique seminar approach requires instructors with extensive experience in managing IT systems and their security, and in advising government and corporate executives on resolving business, operational, management, organizational, policy, budget and promotional issues and developing implementation strategies. Additionally, they need to be capable of training technical and non-technical management personnel complex topics and providing real-world examples, so the attendees can quickly apply the strategies in their jobs.

Jim Litchko, CAS, has 25 years of IT security experience, managed world-wide operational IT systems, supported over 100 security assessments, held executives positions in the government and commercial industry. He has taught IT security classes at Johns Hopkins University, NIST, NSA, NASA and other institutions. Jim is also a professional member of the National Speakers Association and author of 4 security and I.C.E. books.

Al Payne, CISSP, has thirty years of IT experience, including 9 years in IT security. He has been a business owner, executive, operational manager, and strategic advisor for corporations selling security services and products to government agencies. Al is the author of an IT security book and has instructed for the Performance Institute and Intense Schools.



Jim Litchko, CAS and Al Payne, CISSP

For additional information on this and other seminars, related services, books and procuring through GSA contracts, visit to www.litchko.com or call 301-661-3984.