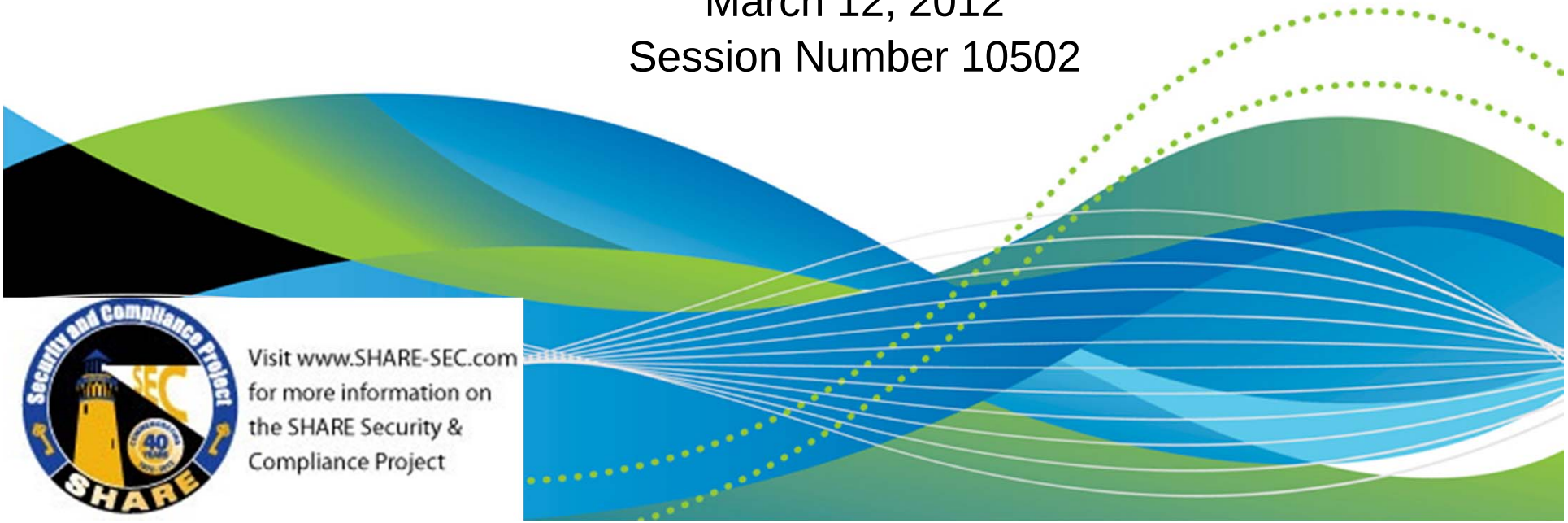
#SHAREorg

SHARE
Technology · Connections · Results

Taking the Lead – How We Get Security and Compliance Services to Our Customers

David Hayes
U.S. Government Accountability Office

March 12, 2012
Session Number 10502



Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

Leadership Needed At Every Level

- The organizations we work for and/or support depend upon us to be leaders in the delivery of security and compliance services
  - To enable them to have a leadership position in their market niche
  - To provide a sound basis in their strategic planning for the future
- As security and compliance professionals, we have to be the leaders
  - To give those who depend upon us and our services the confidence to make sound decisions in their operations, architecture, and control
  - To position us to build our profession and retain the best personnel

Characteristics of Leadership in Security and Compliance Services Delivery

- Technically accurate, complete and current knowledge of the organization's control posture
- Real time communication of that posture simultaneously to the top level decision makers and the operational level decision makers in a manner that allows both groups to efficiently take timely action
  - In our business what we don't know and/or don't communicate WILL hurt others and ourselves
- Constant awareness of current and future risk and our dependency on specific controls
  - We provide others with the ability to confidently do their jobs when they know WE are doing ours

How Do We Lead?

- Understand the difference between visibility and transparency
- Know what standards and compliance requirements are applicable, know what they represent, and embed their objectives into your organization's objectives
- Embrace internal control – operationally differentiate between activities that provide negative assurance as opposed to positive assurance
- Take responsibility: make risk identification and risk mitigation your job across the organization
- Constantly promote professional development: yours and your colleagues
- Lead by example
- Know what you don't know

Communication Solidifies Leadership

- Leaders have a message, communicate consistently and take positive measures that allow for control of the message
  - Achieve positive visibility through achieving a transparent mode of operations
  - Communicate with precision – balance technical accuracy against over-simplification
  - Without being an alarmist or being perceived as alarmist, consistently craft communications in terms of risk
  - Maintain an accurate inventory of the cost and benefits of your security and compliance services (organization-wide) and consistently include this information in your communications
- Strategically engage in outreach to external stakeholders

What Do Security Standards and Compliance Requirements Represent?

MINIMUM PERFORMANCE!

- Security and compliance leaders do the work to LEARN what the objectives of standards and compliance requirements mean to their organizations and the organization's stakeholders
- Leaders participate in the development of their organization's control objectives – doing what it takes to embed the objectives of the standards and compliance into their organization's culture

Internal Control – Supporting Positive Assurance

- We are in the internal control business – achieved, in part, through information security controls and satisfying compliance requirements.
- Just meeting the standards and being compliant probably limits management to assertions of negative assurance
- We need to take the steps necessary to substantiate that not only do controls provide protection against bad things, but, in fact, based on control objectives grounded in business requirements and risk assessments: controls are in place and working as intended all the time – AND HERE IS HOW WE KNOW…

Leadership in Risk Identification and Risk Management is Essential

- Just like the law, ignorance is not a defensible position – not being on top of all aspects of risk ensures failure
- Have an absolute inventory of the inherent risks you and your customers' face:
  - Know your customers' businesses, their regulatory environment, and their control environment
  - Know your threat environment – know who can see or touch every aspect of your data processing environment
- Know the control risks faced by your customers and by your operation
  - Know all data paths – end to end
  - Know exactly where and how your operation depends on entities external to your operational control

Leaders are Never Satisfied

- Aggressively manage to the future
  - Advance yourself and your staff - allowing professional stagnation makes you a follower
  - Accept the surety of change
  - Address key person dependencies
  - Avoid too much comfort - comfort erodes confidence
- Lead by example
- Accept the absolute certainty that you and your organization IS missing something – knowledge is never absolute and, in our business, what we don't know WILL hurt us and those who depend on us