Making Security Measurable

Business and Government
- Regulatory Compliance
  - Sarbanes-Oxley
  - HIPAA
  - FISMA
  - PCI
  - Future laws
- ROI
- Risk Management

Enterprise Security Management
- Standards
  - ISO/IEC 27000
  - COBIT
  - NIST SP800-53
  - ITIL
  - DoD 8500.2
- Security Automation
  - CND
  - FDCC/USGCB

Information Technology
- CVE
- OVAL
- CPE
- XCCDF
- CVSS
- OCIL
- CCSS
- AI
- ARF
- SCAP
- SWID
- CWE
- CWSS
- CAPEC
- CybOX
- STIX
- TAXII
- MAEC
- CEE
- EMAP
- IODEF
- RID
- RID-T

Vulnerability Management
- Patch Management
- System Assessment
- Asset Management
- Malware Protection
- Software Assurance
- Intrusion Detection
- Indicator Sharing
- Incident Coordination

Policy makers must demonstrate how IT processes meet business goals

Government, business and industry drive the requirements and mechanisms of information security

IT processes must integrate with each other while demonstrating how they meet security and policy objectives

Regulatory Compliance
- Sarbanes-Oxley
- HIPAA
- FISMA
- PCI
- Future laws

Risk Management

ROI