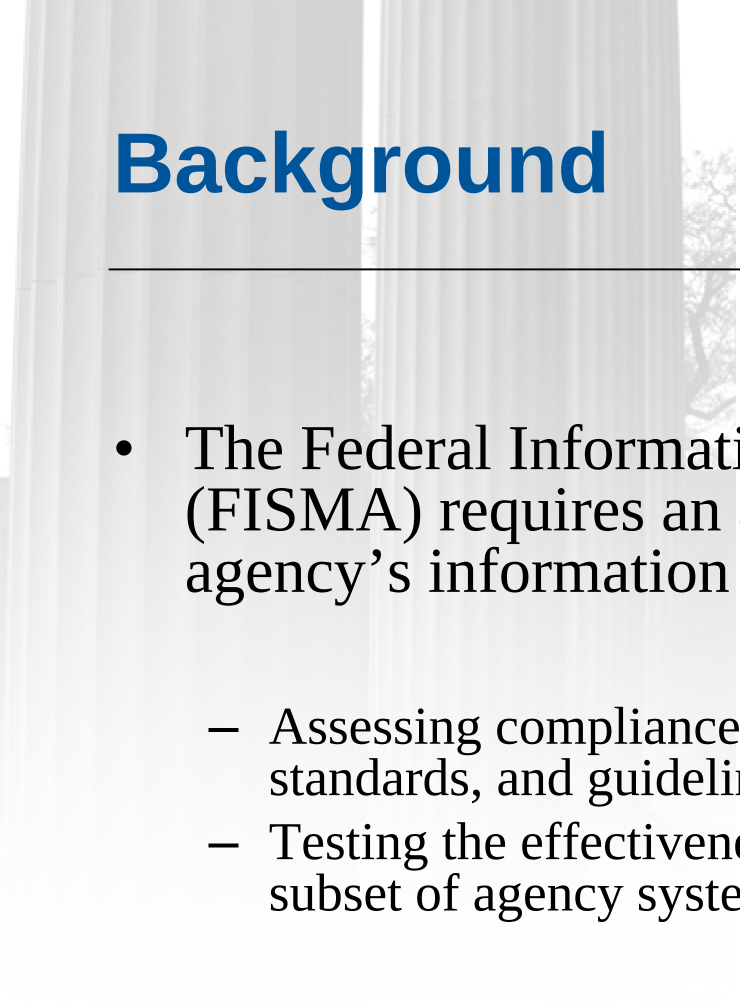
Federal Information Security Management Act Implementation: An Auditor’s Perspective

National Institute of Standards and Technology

Information Security Seminar
February 1, 2007

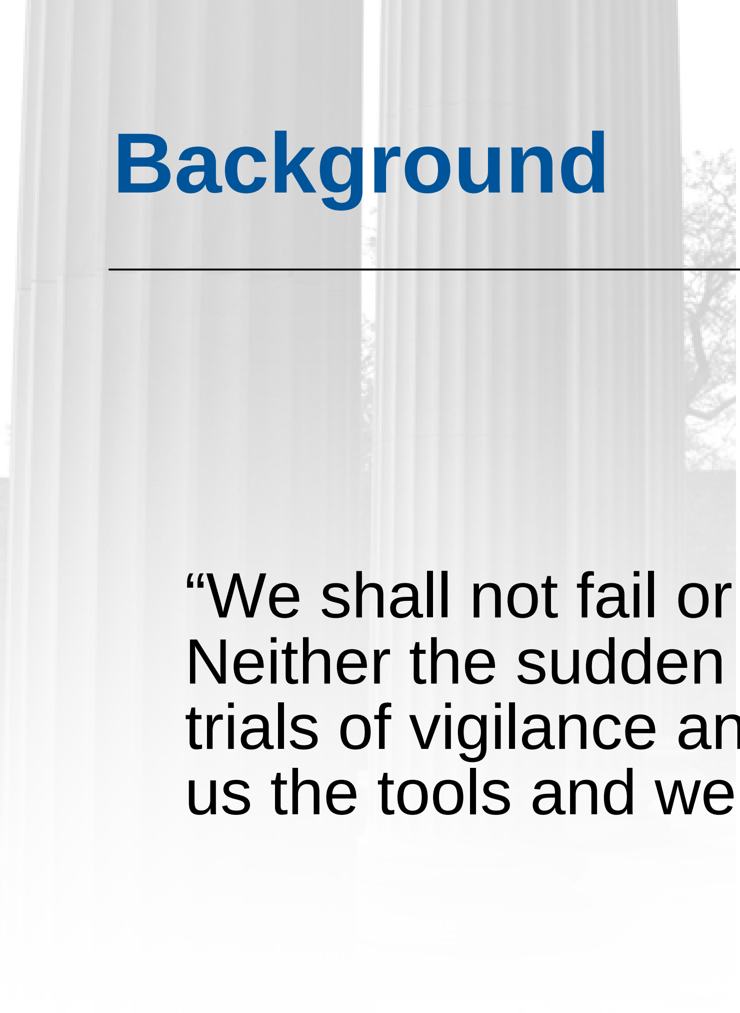
Presentation Agenda

- Background
- An Evaluation Approach



Background

- The Federal Information Security Management Act of 2002 (FISMA) requires an annual independent evaluation of each agency’s information security program and practices
  - Assessing compliance with FISMA and related policies, procedures, standards, and guidelines
  - Testing the effectiveness of policies, procedures, and practices for a subset of agency systems
- Six annual evaluations completed

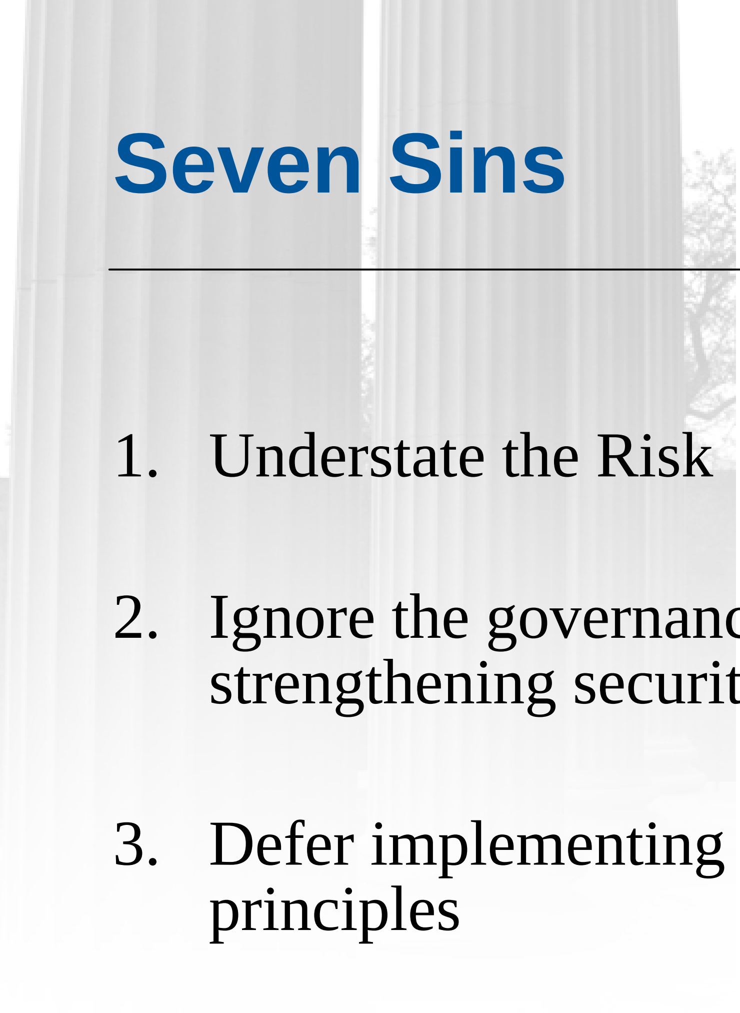


Background

"We shall not fail or falter, we shall not weaken or tire. Neither the sudden shock of battle nor the long-drawn trials of vigilance and exertion will wear us down. Give us the tools and we will finish the job."

Sir Winston Churchill, 1941

Seven Sins



1. Understate the Risk

2. Ignore the governance and cultural change component of strengthening security controls

3. Defer implementing enterprise architecture management principles

4. Downplay security in the system development life cycle

Seven Sins

5. Short-change security in the information technology capital planning and investment control process

6. Misapplying cost benefit analysis

7. View FISMA as a paper exercise

8. Blame the auditors

An Evaluation Approach

Evaluation Approach

- Program Level Assessment
  - NIST SP 800-100, Information Security Handbook, A Guide for Managers
- System Level Assessments
  - FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems
  - NIST SP 800-53, Recommended Security Controls for Federal Information Systems
- OMB Guidance
- Inspector General Framework issued in September 2006

Overall Information Security Control Assessment

Assessment of the Information Security Controls		
Control Class	**Control Assessment**	
	Effectiveness	**Attention Needed**
Program Controls		
Management Controls		
Operational Controls		
Technical Controls		
Overall Control Assessment		

Program Control Assessment

Assessment Results			
Control		**Control Assessment**	
Class	**Family**	**Effectiveness**	**Attention Needed**
Program Controls	Security Governance		
	Enterprise Architecture		
	Capital Planning and Investment Control		
	Critical Infrastructure Protection		

System Control Assessment

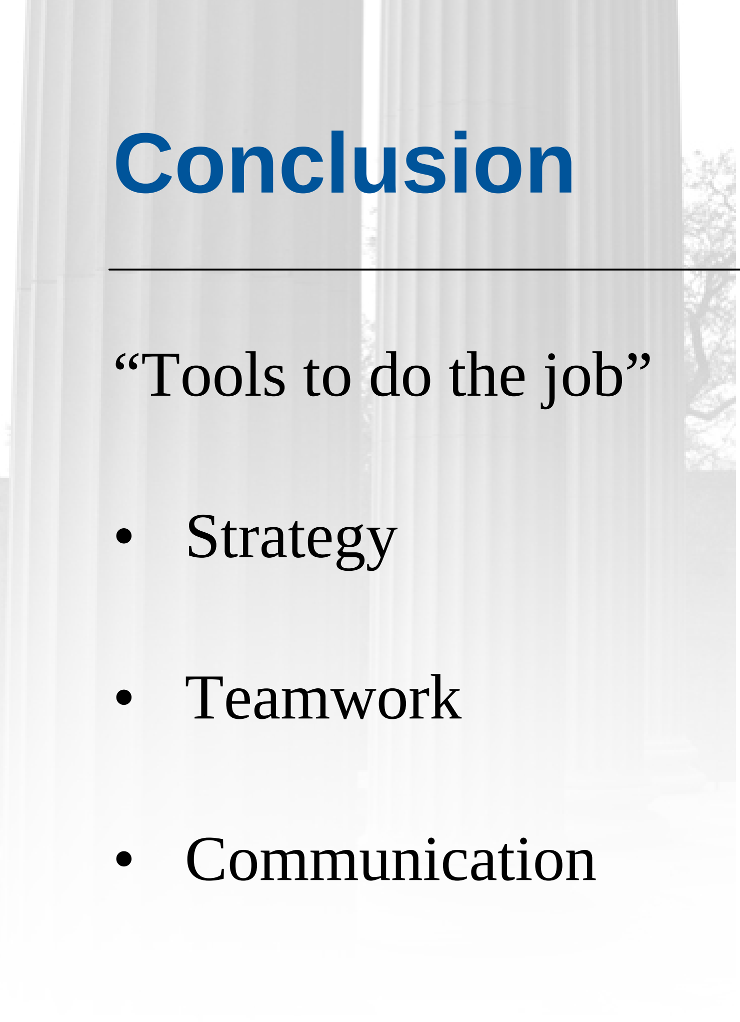
Assessment Results			
Control		Control Assessment	
Class	Family	Effectiveness	Attention Needed
Management Controls	Risk Assessment		
	Security Planning		
	System and Services Acquisition		
	Certification, Accreditation, and Security Assessments		

System Control Assessment

Assessment Results			
Control		Control Assessment	
Class	Family	Effectiveness	Attention Needed
Operational Controls	Personnel Security		
	Physical & Environmental Protection		
	Contingency Planning		
	Configuration Management		
	Maintenance		
	System and Information Integrity		
	Media Protection		
	Incident Response		
	Awareness and Training		

System Control Assessment

Assessment Results			
Control		Control Assessment	
Class	Family	Effectiveness	Attention Needed
Technical Controls	Identification and Authentication		
	Access Control		
	Audit and Accountability		
	System & Communications Protection		



Conclusion

"Tools to do the job"

- Strategy
- Teamwork
- Communication