



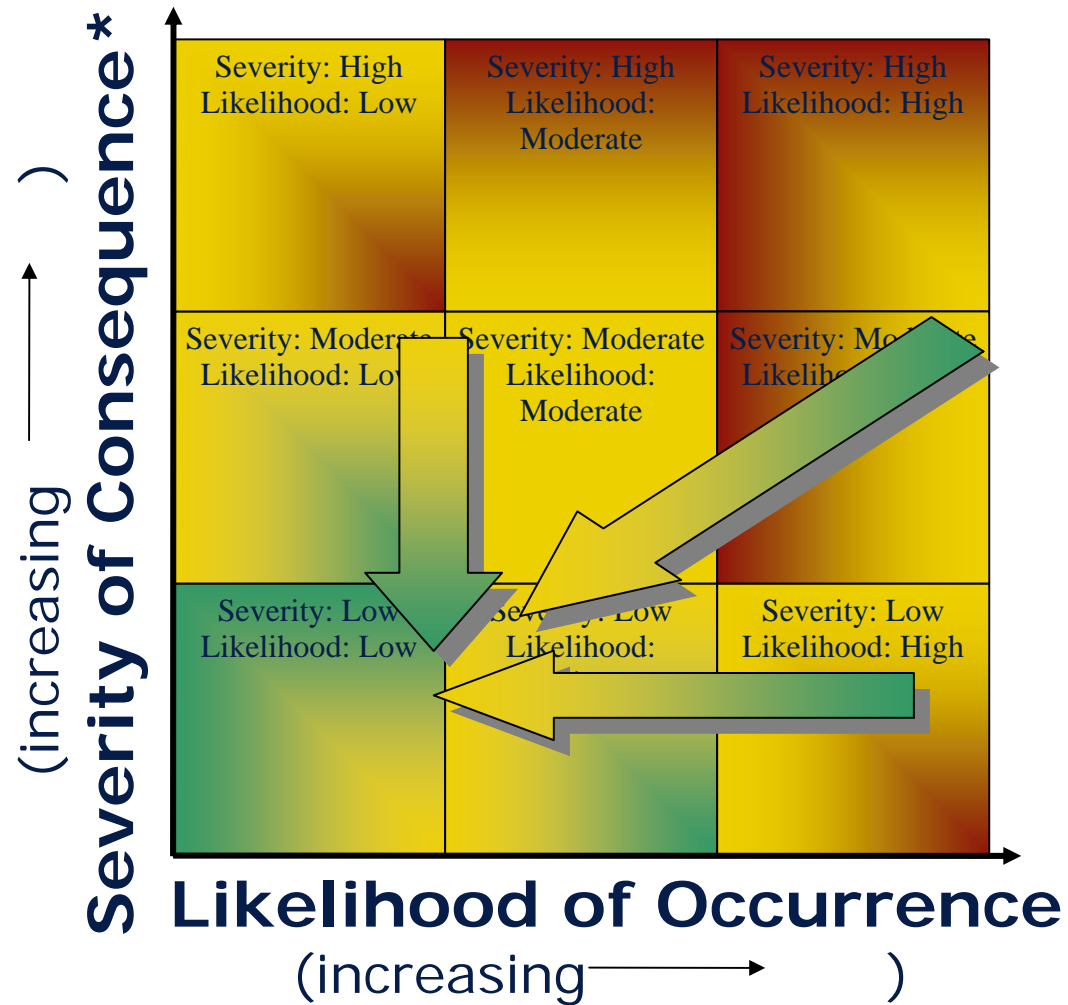
Information Security:

Model, Process and Outputs

Information Security Method


- The problem...
- The solution:
 - Model
 - Process
 - Outputs

Managing Information Risk

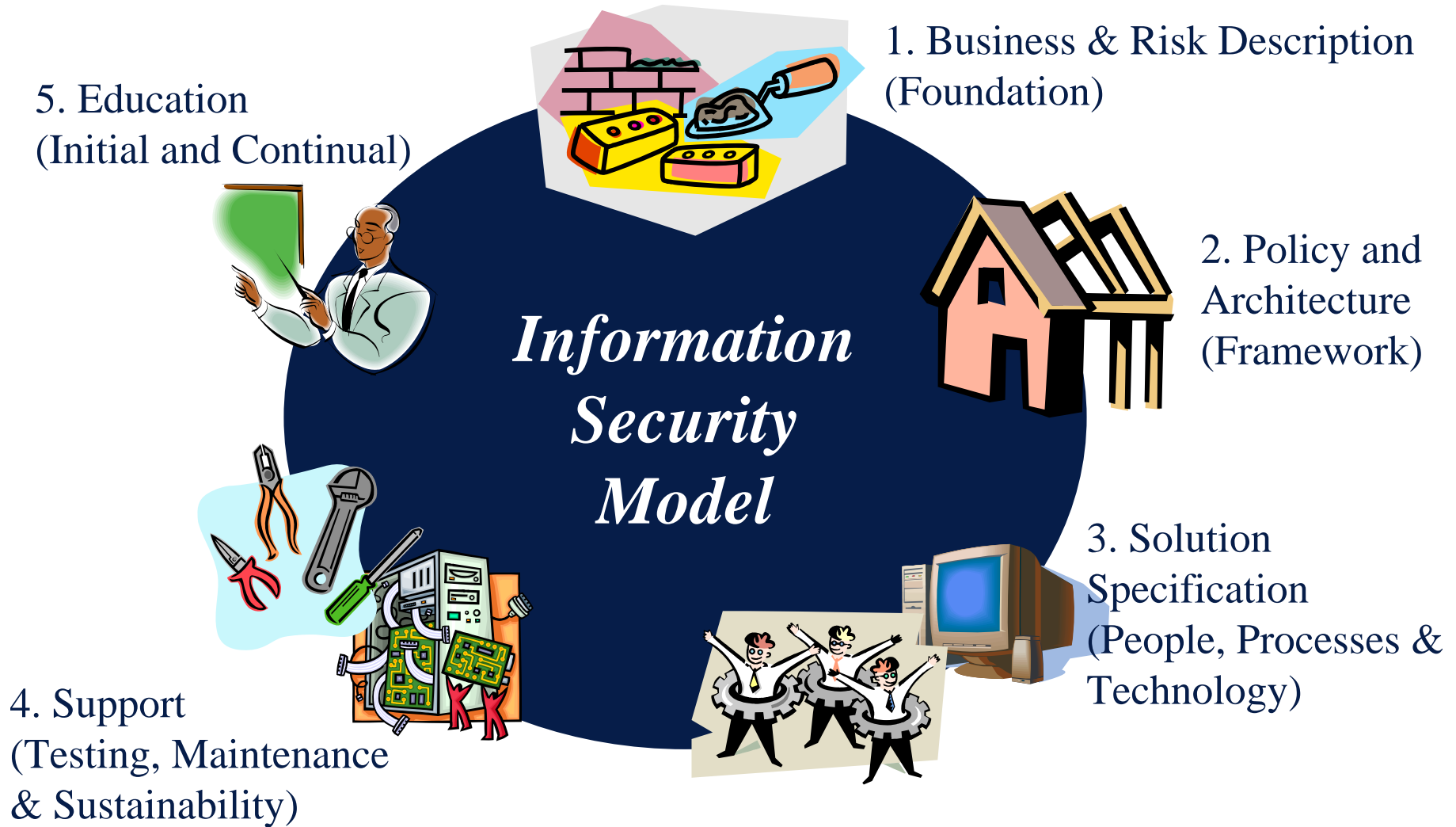


* In some cases, consequence severity may not change. The goal then is to drive "likelihood of occurrence" to zero.

Security Solution: Model / Process / Outputs

- 
- Five component security model
 - Step-by-step security solution development process
 - Ten “must have” outputs for understanding, managing and monitoring your security solution

Information Security Model

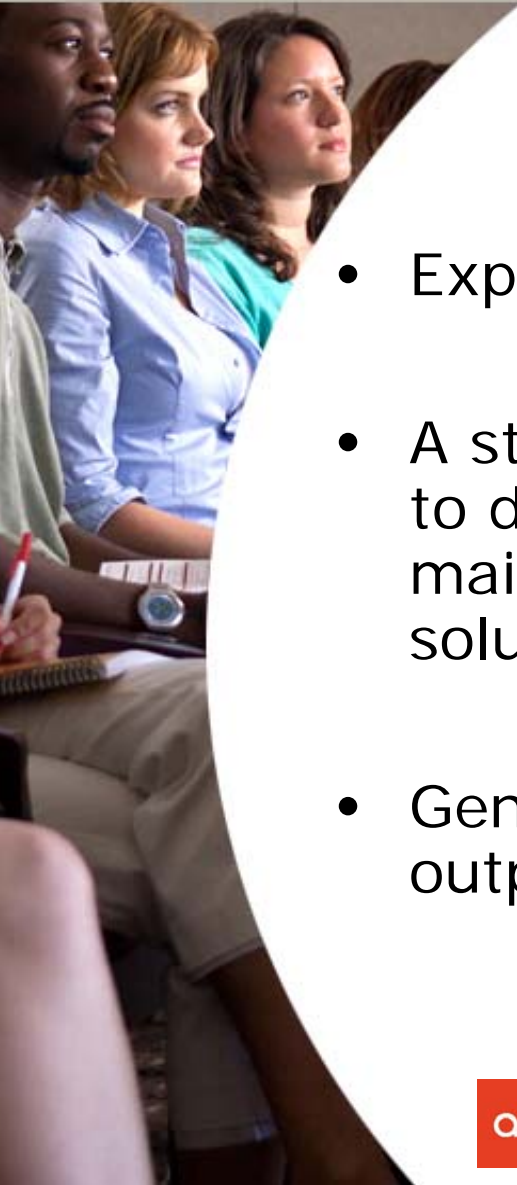


- Business & Risk Description
 - Overall description of business scenario(s)
 - Understanding of information assets, users, and operational environment
 - Identification and summarization of business risks associated with information assets

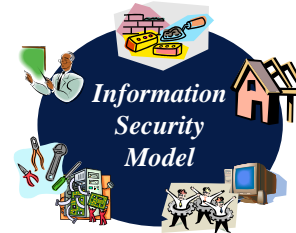
- Framework
 - Definition of an information security policy
 - Major statements (requirements) regarding information security
 - Can be considered the “what is allowed / not allowed” document
 - Definition of an information security architecture
 - The “big picture” that ties together information resources and how they should be protected
 - Identifies the major information systems and the interconnectivity between those systems

- Solution
 - Detailed specifications
 - Technology
 - Procedures
 - Personnel
 - Implementation planning
 - Implementation and test
 - Certification & accreditation
- Support Program
 - Follow-on Testing, Re-certification & Reporting
 - Maintenance & Monitoring
 - Insurance & Contingency Planning
- Awareness Program
 - General security literature
 - Specific “How to...” guides

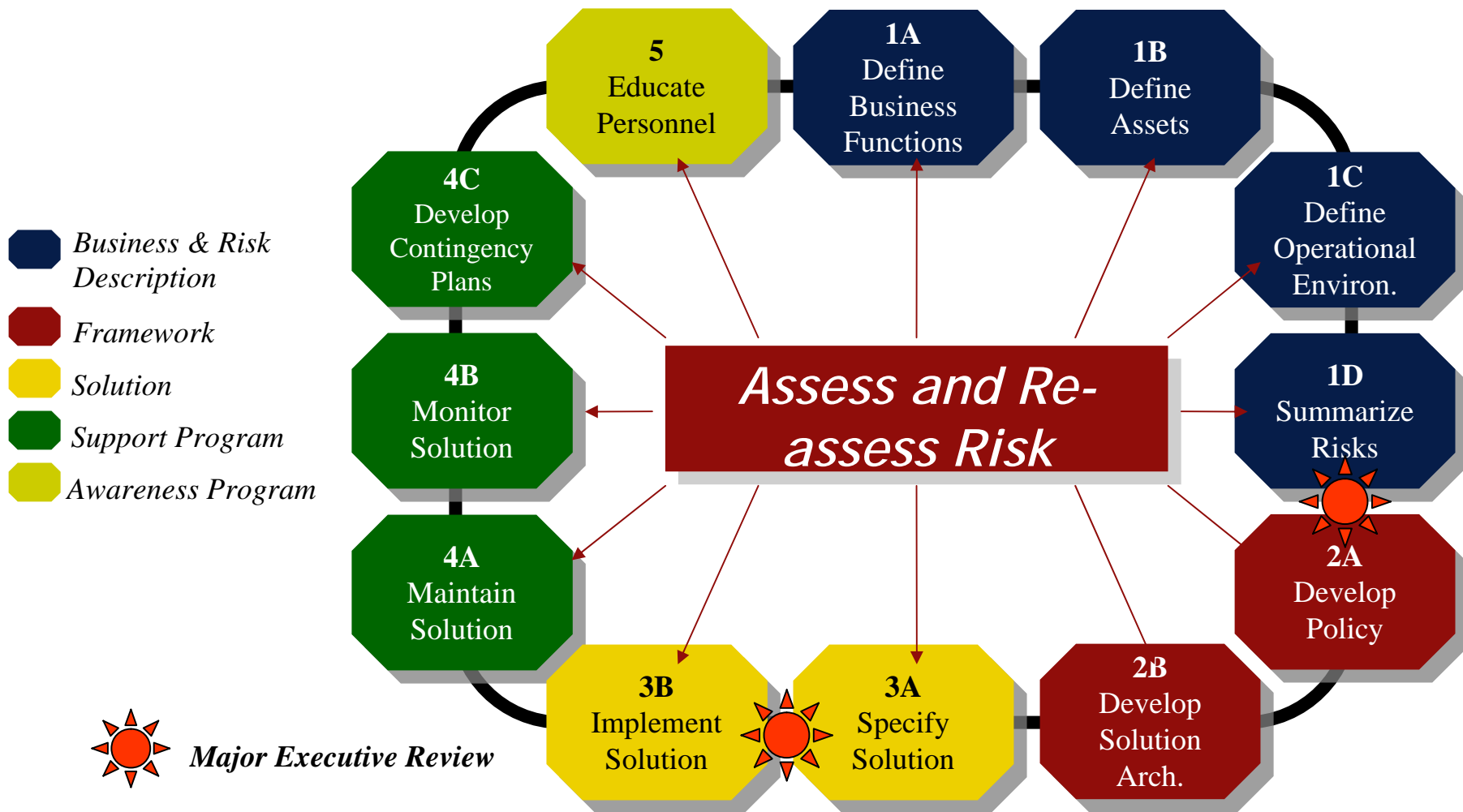
Information Security Process



- Expands on the Model
- A step-by-step, manageable approach to defining, deploying, operating and maintaining an information security solution
- Generates the ten “must have” outputs



Information Security Process (cont.)



The Results

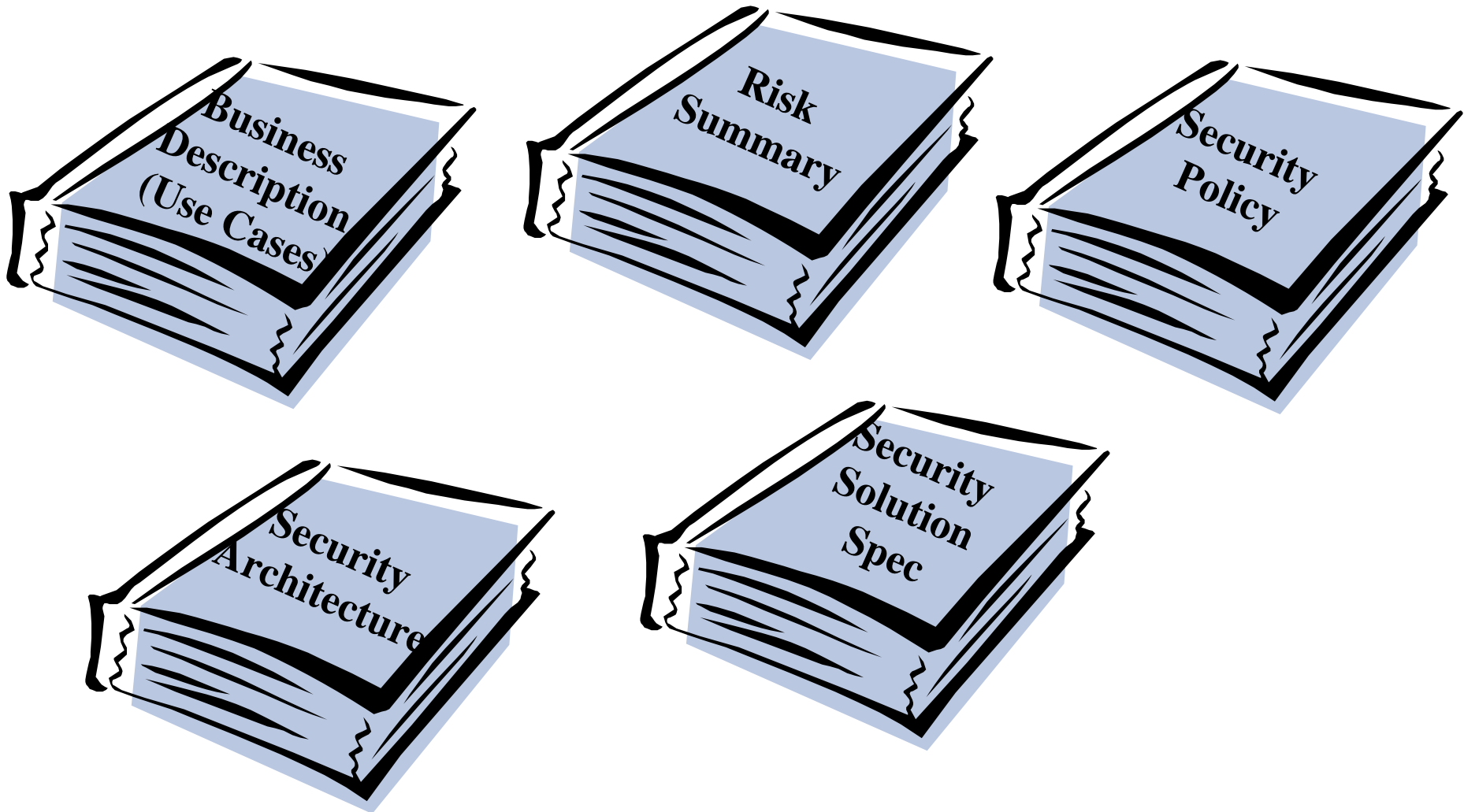


- A security solution:
 - Derived from business requirements
 - Derived from defined business risks
 - Results in appropriate protection of business assets
- Risk management capability
 - Each step after the risk summarization step forces a risk mitigation review for each identified risk
 - What one step cannot address, another step will address
 - The monitoring step ensures that risk management and monitoring always exists

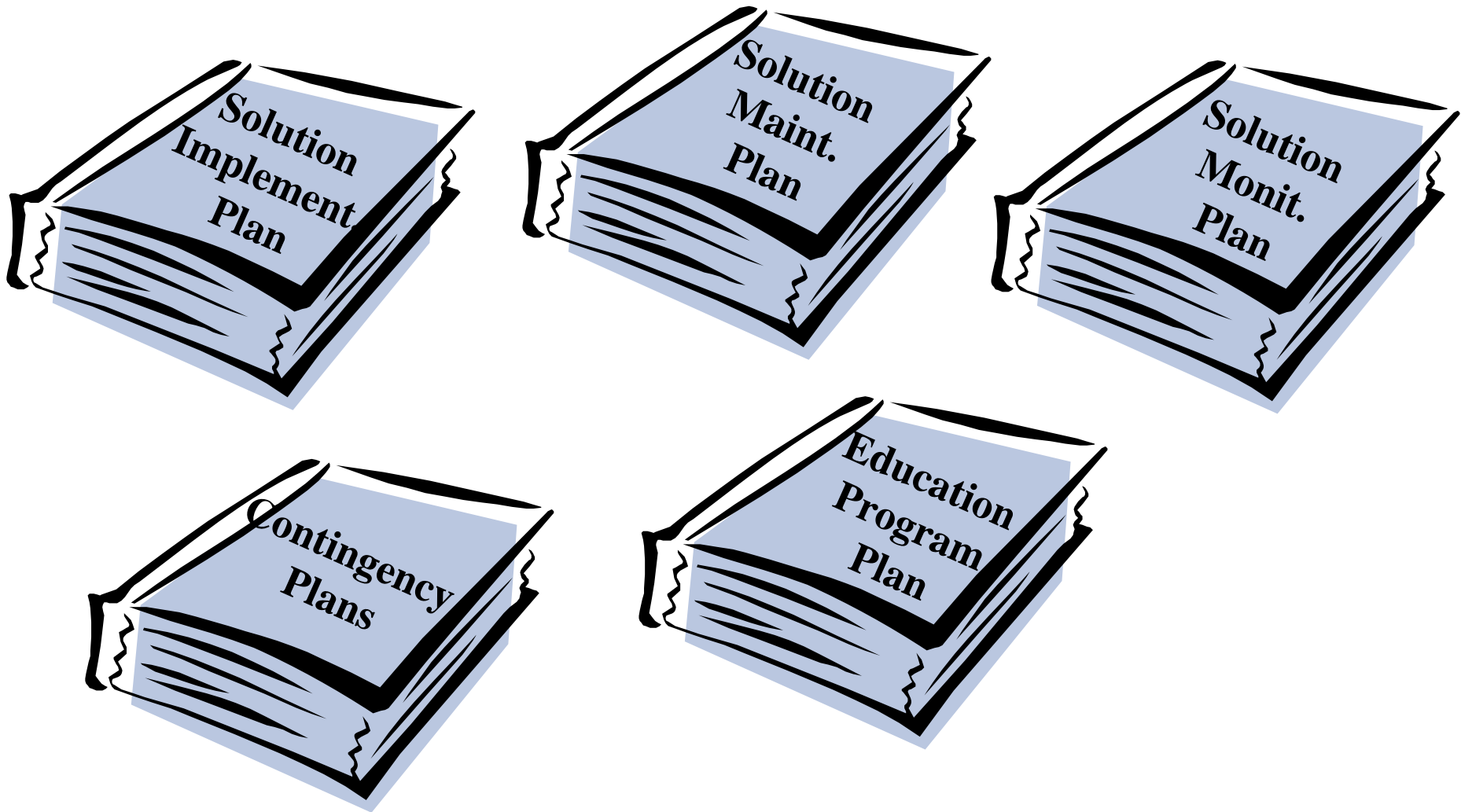
The Results (cont.)

- Documented solution to support:
 - Change control
 - Awareness training
 - Audits and accreditation
- A review process:
 - Two major reviews
 - Risk Summary Review
 - Solution Specification Review
 - Major reviews intended for trade-off analyses
 - Risk mitigation reviews after each step following Risk Summarization Step
 - Other reviews can be performed as needed and in-line with already established corporate review procedures

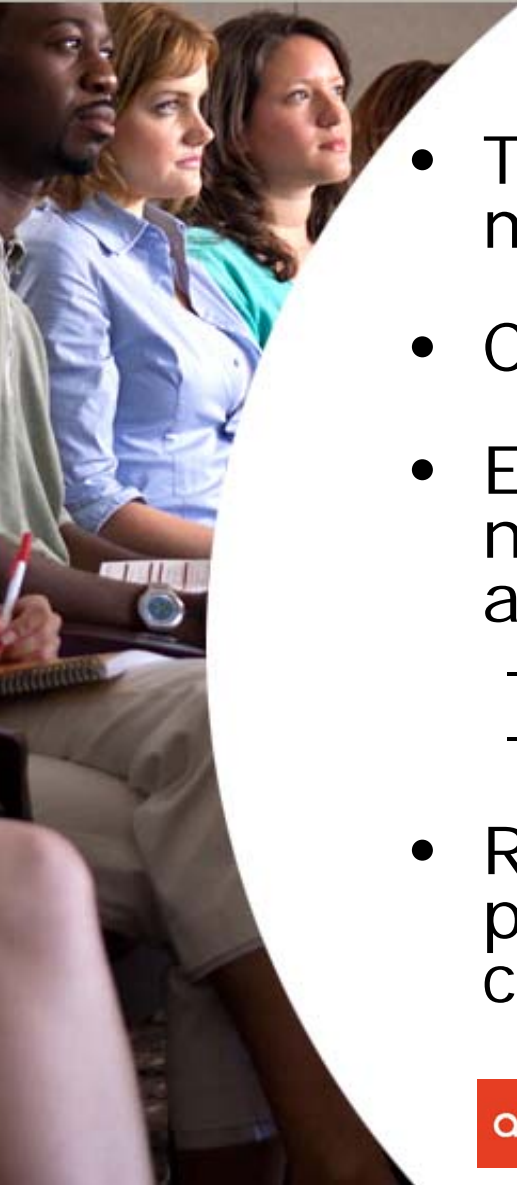
The Results: Ten “Must Have” Outputs



The Results: Ten “Must Have” Outputs



Ongoing Process...

- 
- There is no “one-time” solution to managing information security risks
 - Conditions change → Risks change
 - Each output is a living document that needs to be reviewed for accuracy and relevancy
 - Periodically (i.e., time-driven events)
 - Ad hoc (i.e., event-driven events)
 - Reapply process (or portions of process) as needed based on changing risks



Information Security

John L. Jones

President

Arion Zoe Corp.

813 254-0055

jjones@ArionZoe.com