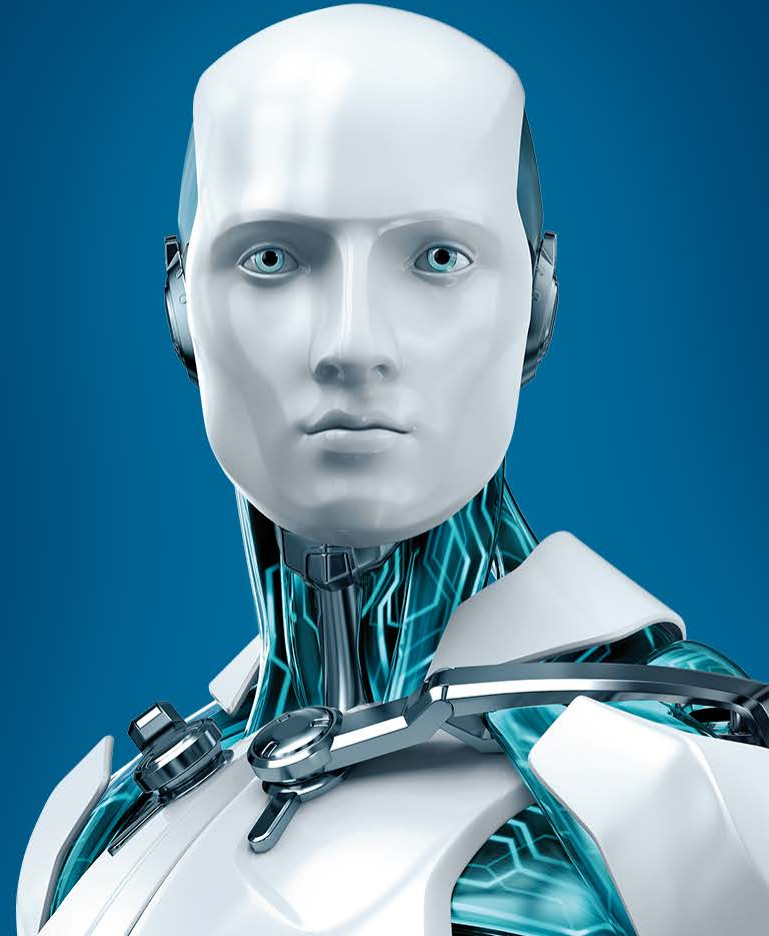




Cybersecurity Risk Management Framework



ENJOY SAFER TECHNOLOGY®



6 Steps


To Building an effective Risk Management Framework



ENJOY SAFER
TECHNOLOGY®



The 6 Steps

1. Categorize
2. Selecting Security Controls
3. Implementation 
4. Assess Controls
5. Authorize
6. Continuous Monitoring



Step 1: Categorize

- Risk Executive (Function)
 - Senior Leadership Buy-in & Support
 - Organizational Support
 - FIPS 199 as a Categorical Roadmap
 - Info Types, Systems & Controls
-



Defining Security Objectives


- Confidentiality
- Integrity
- Availability



- High
- Moderate
- Low

Step 2: Security Controls Selection

Establishing Controls for

-
- Authorized & Unauthorized Devices
 - Authorized & Unauthorized Software
 - Secure Configs for all Devices in Environment
 - Continuous Vuln Testing & Remediation
 - **Controlled Use of Admin Privileges**
 - Maint, Monitoring and Analysis of Audit Logs
 - Email & Web Browser Protections
 - Malware Defenses
 - Control & Limitation of Network Ports
 - Data Recovery Capabilities
 - Secure configurations of Network Devices (Firewalls, Router & Switches)
 - Perimeter & Boundary Defenses
 - Data Protection
- 
- Controlled Access – Permissions Based
 - Wireless Access Control
 - Account Monitoring & Control
 - Security Skills Assessment
 - Security Training & Best Practices
 - Application Software Security
 - Physical Security
 - Incident Response
 - Incident Management
 - Penetration Testing
 - Establishment of “Red Team”
 - Red Team Exercises
 - Middleware, Cloud & Vendor Security Postures

Step 3: Implementation

5 Steps to Robust Implementation

- Step 1 - Identify
- Step 2 - Protect
- Step 3 - Detect
- Step 4 - Respond
- Step 5 - Recover



Step 4: Assess Controls


If it can't be measured, it doesn't exist.....





Step 5: Authorize

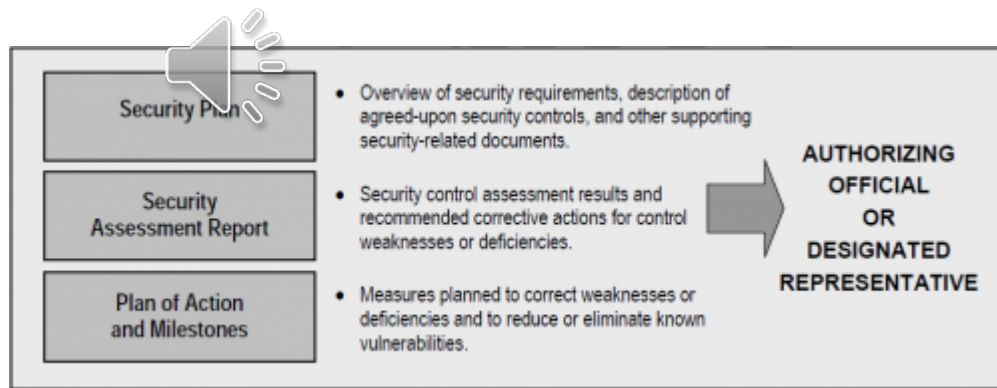
NIST's Definition



Authorize information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the Nation resulting from the operation of the information system and the decision that this risk is acceptable

The Authorization Process

Assembling the Authorization Package



Obtaining Authorization

Date: 01/11/2011

Letter of Authorization

To: AT&T Energy Services

We, _____, the original manufacturer of the _____, hereby authorize _____ at _____ (Town/City) as our authorized distributor in Texas. _____ is authorized to apply for registration and market approval for the following device(s):

Model Number(s):

Name of Manufacturer: _____

Manufacturing address: _____

Country: _____

Name: _____

Title: _____



NIST



Step 6: Monitoring

Active Monitoring, Engagement and Adjustment



The question is not “if” our company will be breached, or even when. It has already happened. The real questions are: is our organization aware of it, and how well are we protected for the future?

Step 6: Monitoring

Accounting for changes in Personnel



Step 6: Monitoring

Accounting for changes to the
hardware/software/firmware



Step 6: Monitoring

Accounting for changes to the
environment



Conclusions & Recommendations

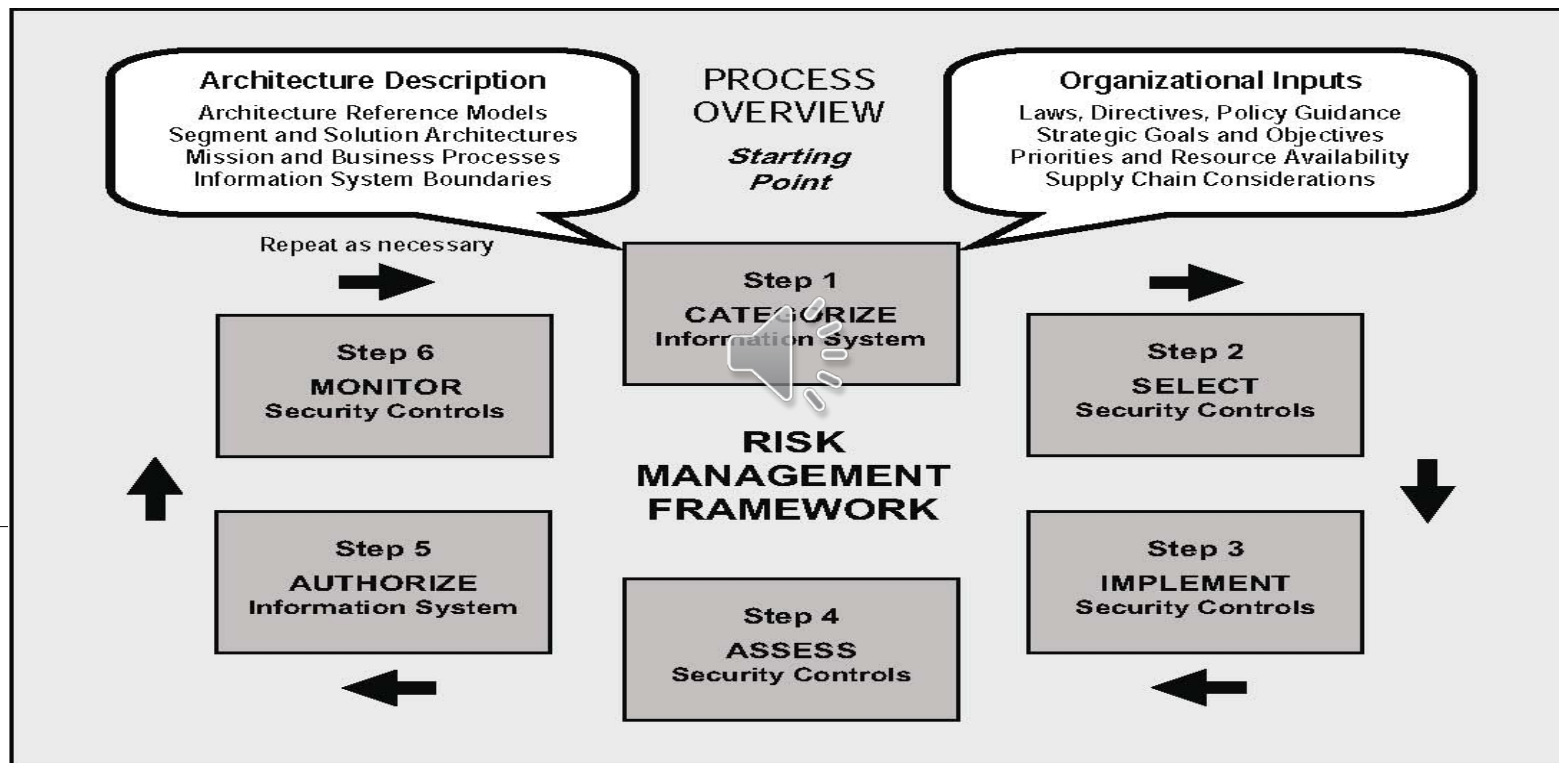


FIGURE 2-2: RISK MANAGEMENT FRAMEWORK



RISK COMPLIANCE

Meeting the requirements, head-on

Q&A Session



ENJOY SAFER
TECHNOLOGY®

Thank You for your time.