Ron Shuck, CISSP, CISM, CISA, CPP, GCIA
Global Computing Security Manager
Spirit AeroSystems

RISK MANAGEMENT

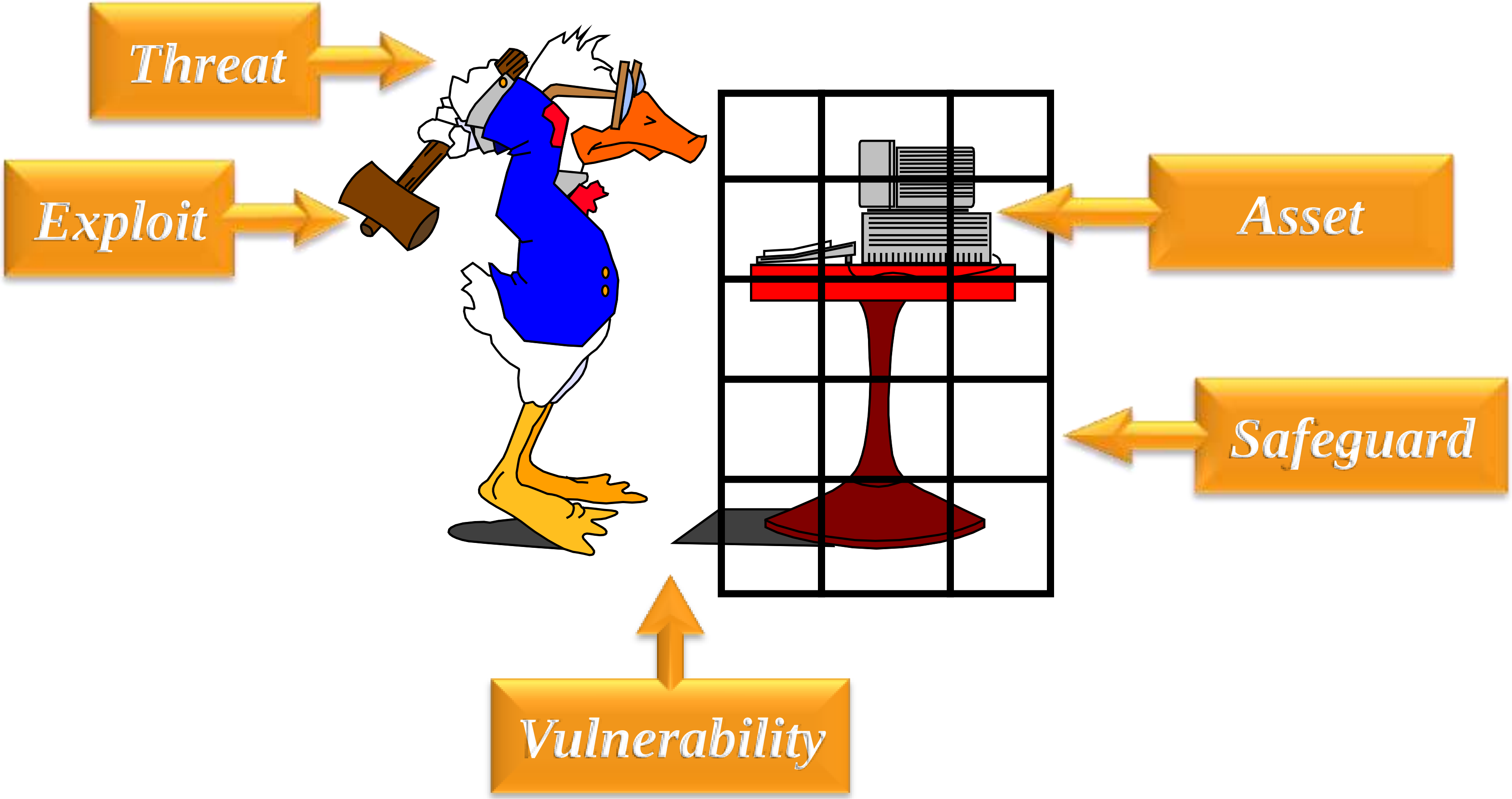
September 2, 2011

ISSA™
Information Systems Security Association
CENTRAL PLAINS CHAPTER

Overview

- What is Risk
- Threats, Vulnerabilities, & Exploits
- Identification of Risk
- Management of Risk
- Risk Management Framework
- Risk Analysis
- Risk Assessment Process

Risk



Identification of Threat

Threat: A force that could negatively impact Spirit's ability to do business. The threat model uses the categories below to classify threats:

Environment

- Man Made Disasters
- Natural Disasters
- Business Environment

People

- Attackers (Internal/External)
- Errors & Omissions
- Espionage (Nations/Companies)

Environmental Threats

Environmental Threats: Forces that are due to interaction with the world around us.

- Frequency rates are usually more accurate then other threat types
- Impact is usually higher then others
- Usually effects a wide geographic area or market sector

Man Made Disaster	Natural Disaster	Business Environment
Crime	Explosions	Law/Regulations
Chemical Release	Fire	Supply Chain Failure
Civil Disturbance	Weather	Economic Downturn
Terrorism	Flooding	Merge / Acquisition
War	Earthquakes	Contractual Obligations
HVAC Failure	Power Surges	Strategic Direction Change
Power Failure	Radio Interference	Technology Advancement

People Threats

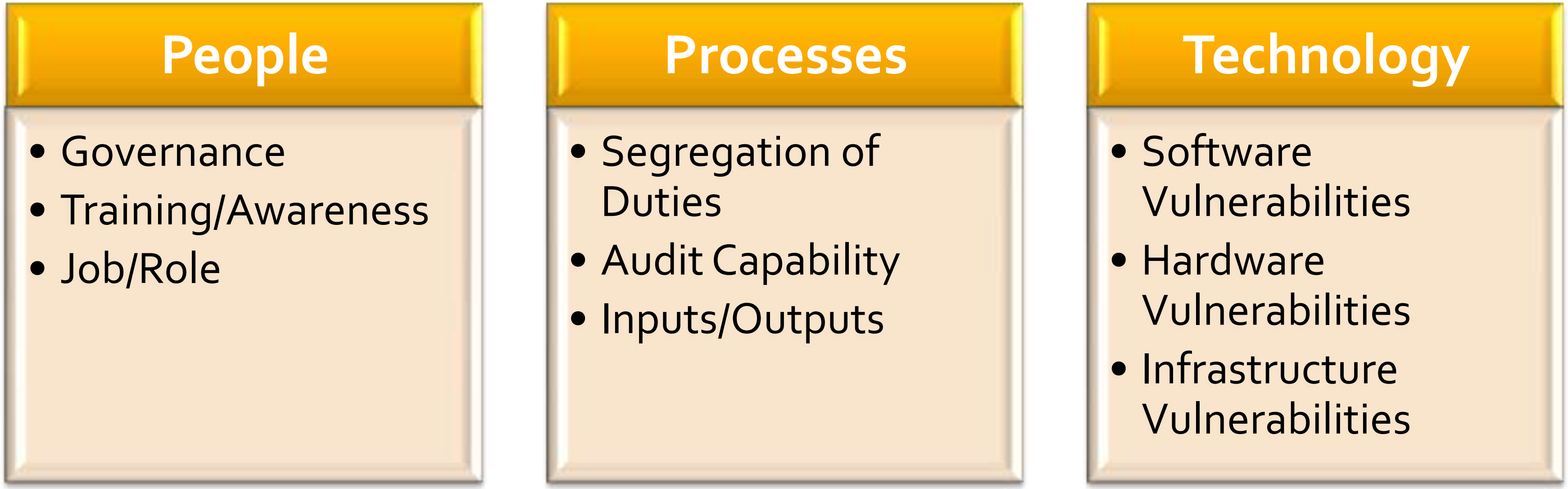
People Threats: Forces that are due to the acts of a person or entity.

- Frequency difficult to estimates
- Usually targeted at a specific company
- More difficult to identify

Attackers	Errors & Omissions	Espionage
Internal Employees	Data Entry Errors	State Sponsored
External Persons	Lack of Security Knowledge	Corporate Sponsored
Contractors	Social Engineering	Sabotage
Vendors	Unintentional Disclosure	Work Stoppage
Malicious Software	Compliance Reporting Failure	
Physical Intrusion	Unqualified Practitioner	
Theft	Contractual Error	

Identification of Vulnerabilities

Vulnerabilities: These are weaknesses that a threat could exploit to cause a compromise of Confidentiality, Integrity, or Availability of an information system.



People

- Governance
- Training/Awareness
- Job/Role

Processes

- Segregation of Duties
- Audit Capability
- Inputs/Outputs

Technology

- Software Vulnerabilities
- Hardware Vulnerabilities
- Infrastructure Vulnerabilities

People Vulnerabilities

People: Vulnerabilities that are introduced directly by the people operating the system. These vulnerabilities can be caused intentionally or unintentionally. Vulnerabilities in these areas tend to have a large impact.

Governance	Training	Job/Role
Information Security Policies	User Security Awareness	Employee Background Checks
Security Program Development	IT Security Training	Separation of Duties
Audit Functions	Roles and Responsibilities	Adequate Skill Set
Regulatory Compliance	Technology Specific Skills	Adequate Resources
Enforcement Activities	Social Engineering	Operational Security

Process Vulnerabilities

Process Vulnerabilities: Weakness in operational and technical processes that can introduce risk into information systems.

Separation of Duties	Audit Capability	Input/Output
Backup Duties	Logs Kept	Data Record Inputs
System Admin	Non-Repudiation	Data Manipulation
Network Admin	Evidence Handling	Output Manipulation
Financial Transaction Authorization	Forensics	Traditional Fraud
Risk Management	Access to Logs	Bounds Checking
Performance Reporting	Audit Functions	Workflow
Job Rotation	Frequency of Audits	Data Verification

Technology Vulnerabilities

Technology Vulnerabilities: Vulnerabilities that are directly introduced by a technical component.

Software	Hardware	Infrastructure
Code Execution	Device Physical Security	HVAC
Privilege Execution	Data Protection	Physical Security
System Configuration	Access Control	Fire Supression
Access Control	Component Failure	Flooding
Administrative Access	Device Hardening	Location
Data Privacy	Hardware Configuration	Weather
Data Integrity	Tamper Resistance	Power
System Interdependence	System Interdependence	System Interdependence

Identification of Exploits

Exploits – Are the tools and conditions conducive for the threat to take advantage of the vulnerability? Does it take an elite PRC hacker to exploit or a janitor?

Knowledge

- Attack Methods
- Intrusion Methodologies
- Operational Knowledge

Tool

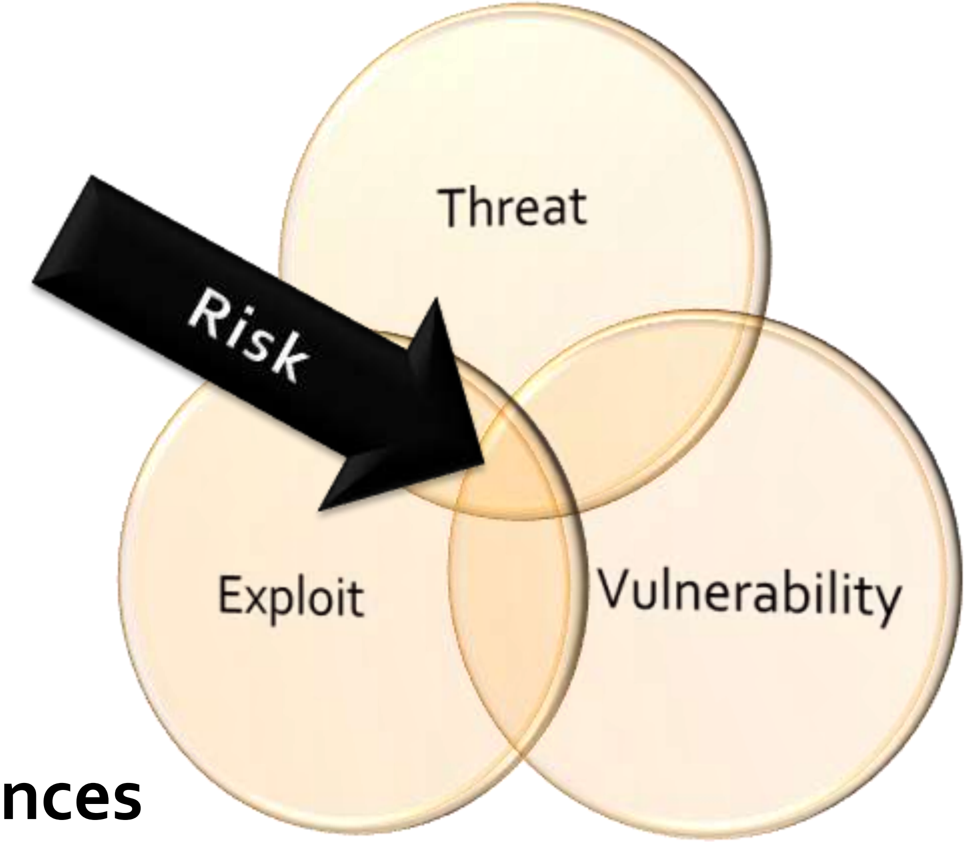
- Pre-built
- Custom Designed
- Easy to Acquire

Opportunity

- Is their a realistic opportunity of exploit?
- Can the threat reach the vulnerability?

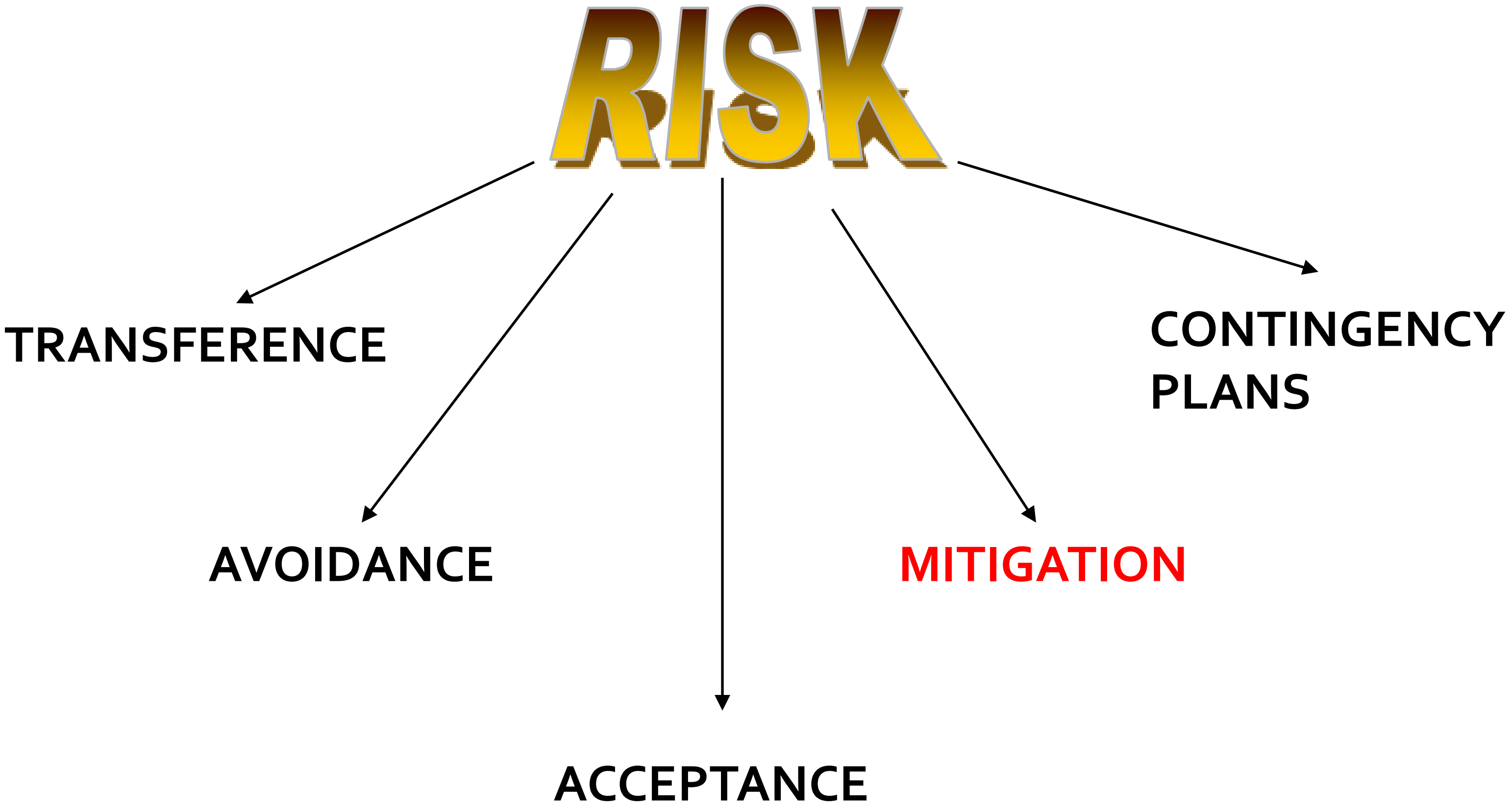
Identification of Risk

RISK: A risk occurs when there is an alignment of a threat, vulnerability, and mechanism to exploit the vulnerability that allows the Confidentiality, Integrity, and/or Availability of an information system to be compromised.



- **Actual Threat**
- **Possible Consequences**
- **Occurrence Frequency of threat**
- **Confidence in occurrence of threat**

Management of Risk



RISK

TRANSFERENCE

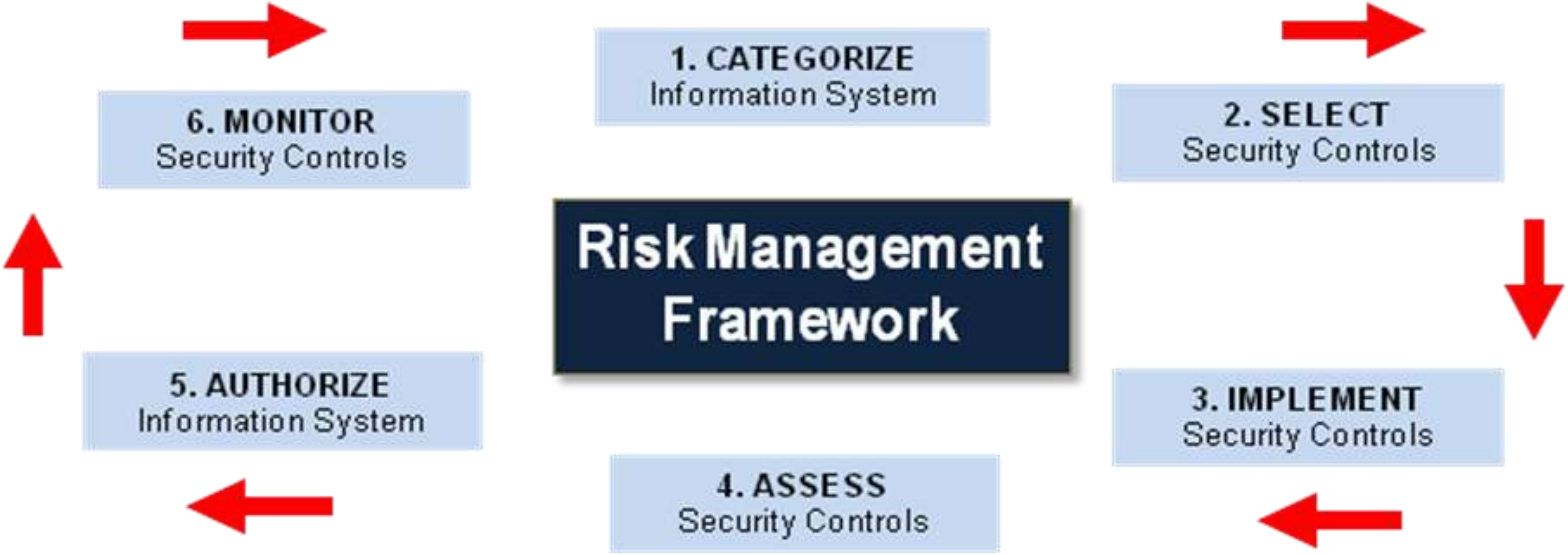
AVOIDANCE

ACCEPTANCE

MITIGATION

CONTINGENCY PLANS

Risk Management Framework



Risk Management Framework

1. CATEGORIZE
Information System

2. SELECT
Security Controls

3. IMPLEMENT
Security Controls

4. ASSESS
Security Controls

5. AUTHORIZE
Information System

6. MONITOR
Security Controls

NIST Special Publication 800-37 rev1 Guide for Applying the Risk Management Framework to Federal Information Systems

Quantitative Risk Analysis

- Independent Objective Numeric Values
- Preliminary Security Examination (PSE)
- Determine Asset Value
- Analyze Potential threats
- Define ALE
  - (Asset Value × EF) × ARO

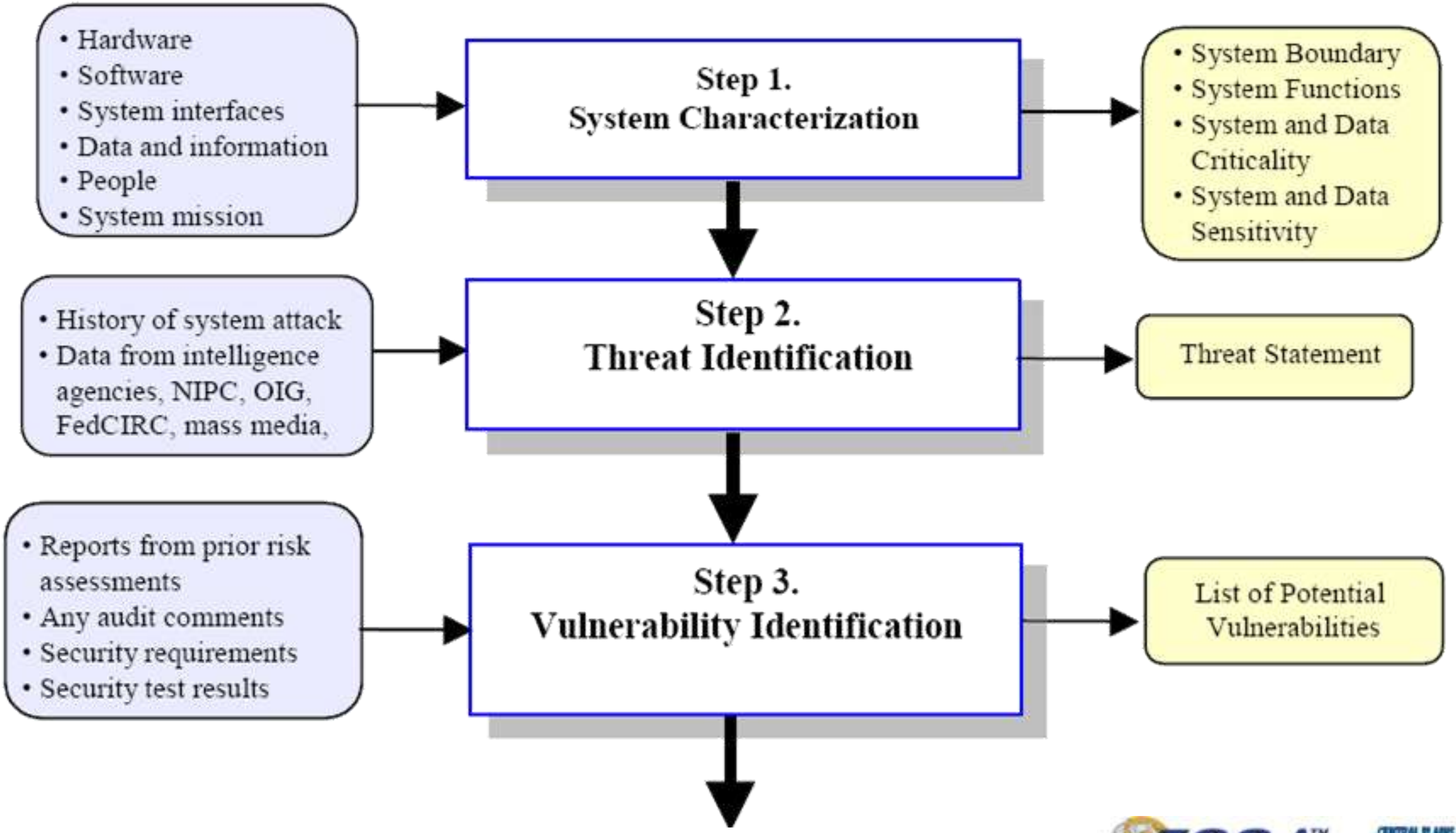
Quantitative Risk Analysis Terms

- Exposure Factor (**EF**)
  - % loss to asset if threat realized
- Single Loss Expectancy (**SLE**)
  - $Asset\ Value \times EF$
- Annualized Rate of Occurrence (**ARO**)
  - Expected frequency of threat
- Annualized Loss Expectancy (**ALE**)
  - $SLE \times ARO$

Qualitative Risk Analysis

- Intangible Value Assessment
- Most Common
- Scenario Procedure
- Asset Valuation Process

Risk Assessment Process



- Hardware
- Software
- System interfaces
- Data and information
- People
- System mission

Step 1.
System Characterization

- System Boundary
- System Functions
- System and Data Criticality
- System and Data Sensitivity

- History of system attack
- Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media,

Step 2.
Threat Identification

Threat Statement

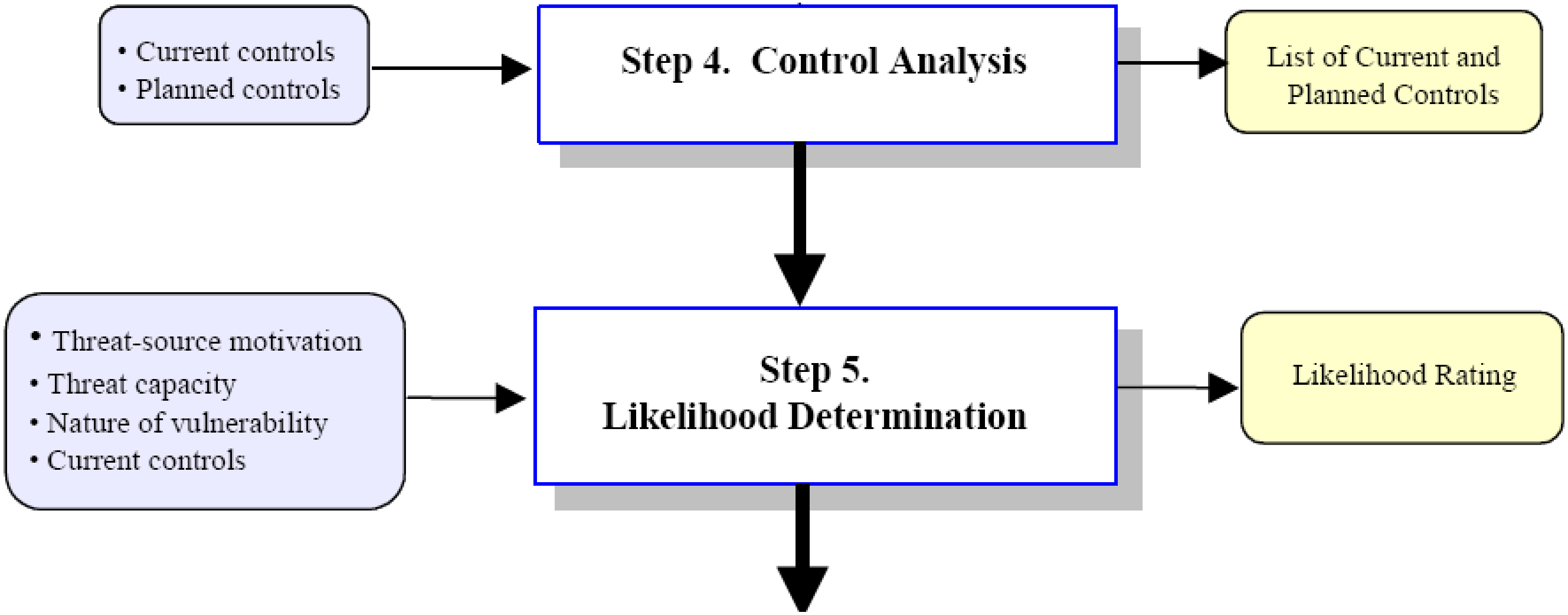
- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test results

Step 3.
Vulnerability Identification

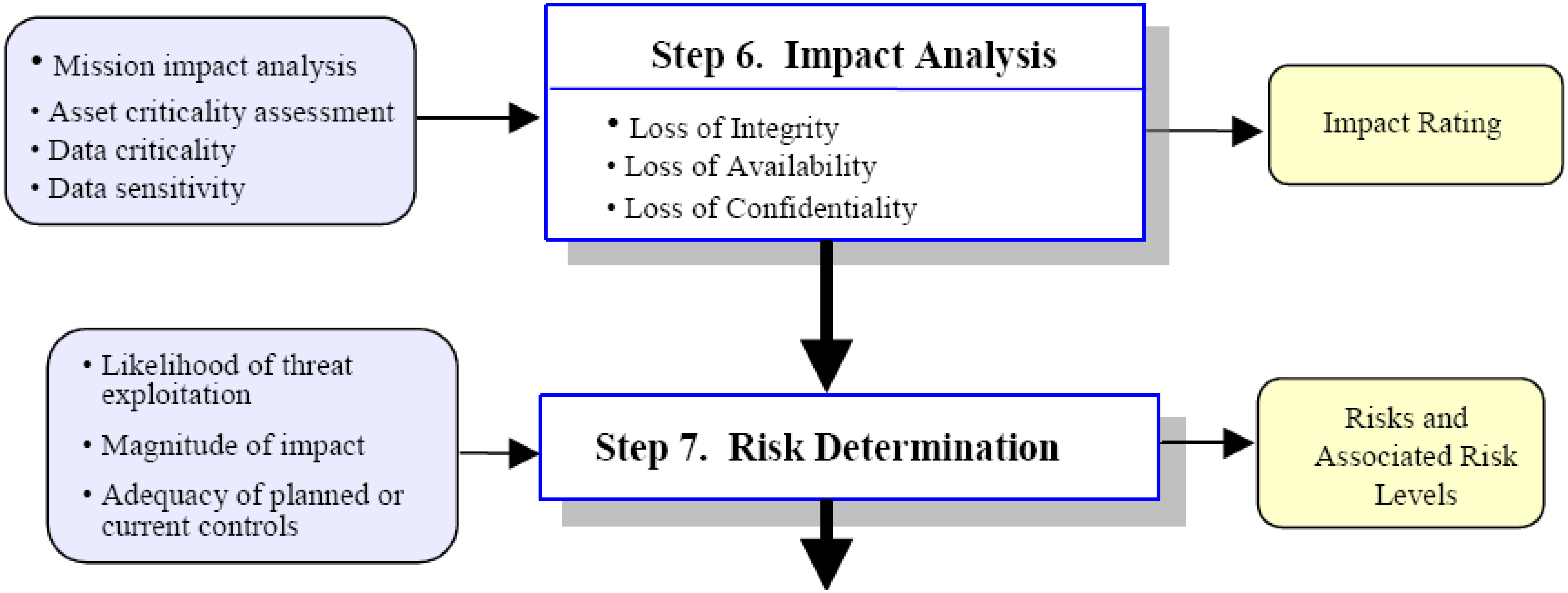
List of Potential Vulnerabilities

NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems

Risk Assessment Process



Risk Assessment Process



- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity

Step 6. Impact Analysis

- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

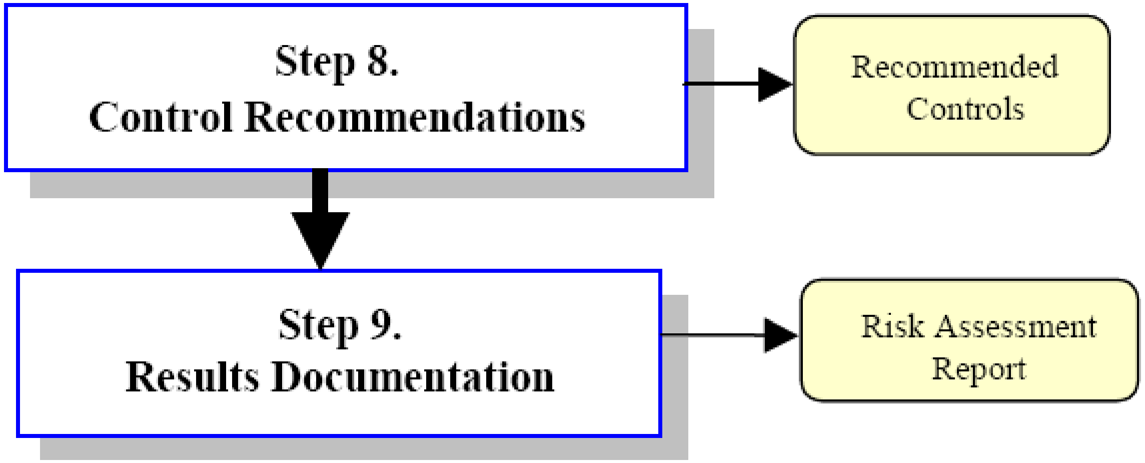
Impact Rating

- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

Step 7. Risk Determination

Risks and Associated Risk Levels

Risk Assessment Process

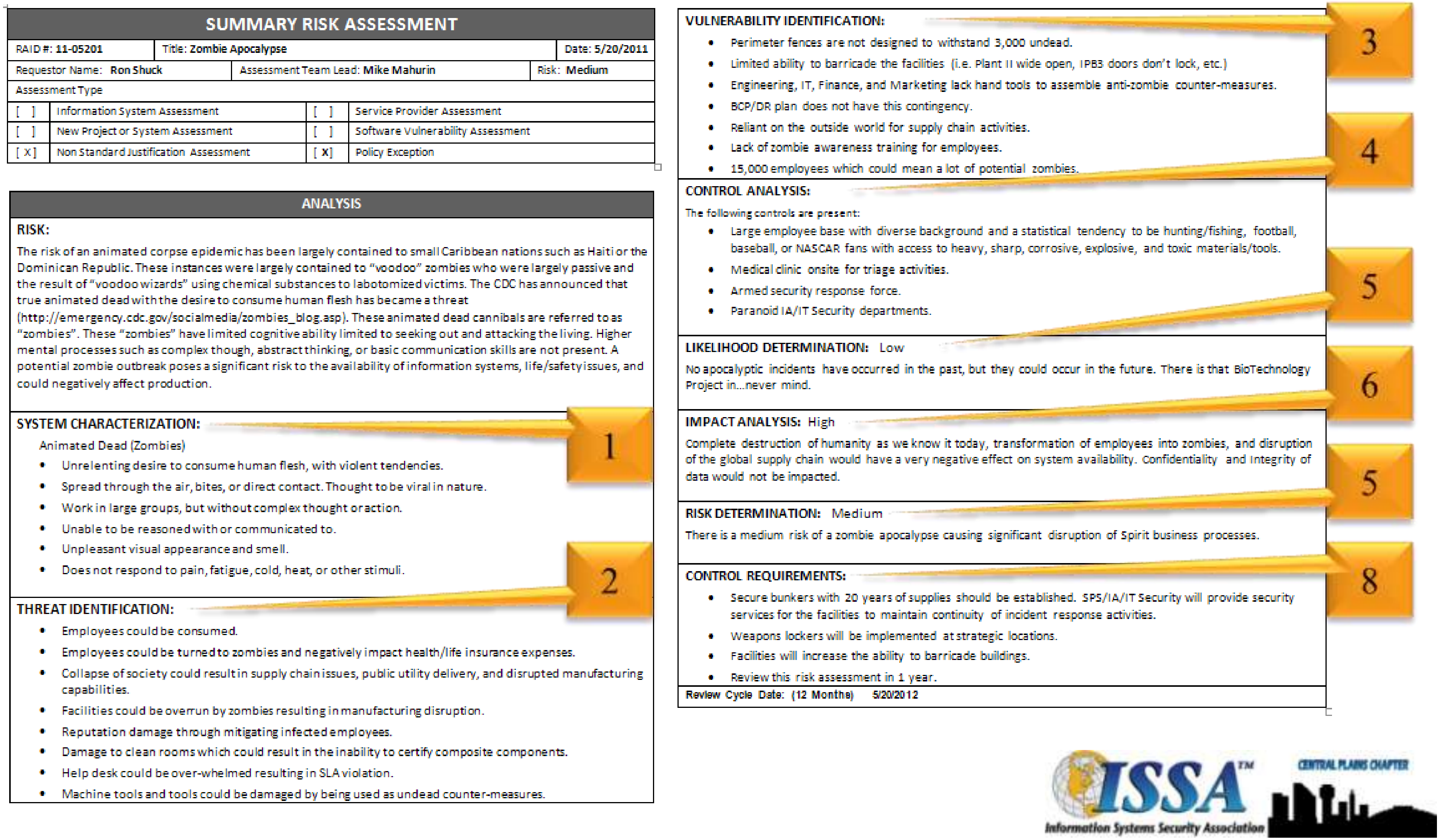

Step 8.
Control Recommendations

Recommended Controls

Step 9.
Results Documentation

Risk Assessment Report

Sample Risk Form



SUMMARY RISK ASSESSMENT

RAID #: 11-05201	Title: Zombie Apocalypse	Date: 5/20/2011
Requestor Name: Ron Shuck	Assessment Team Lead: Mike Mahurin	Risk: Medium

Assessment Type

[ ]	Information System Assessment	[ ]	Service Provider Assessment
[ ]	New Project or System Assessment	[ ]	Software Vulnerability Assessment
[X]	Non Standard Justification Assessment	[X]	Policy Exception

ANALYSIS

RISK:

The risk of an animated corpse epidemic has been largely contained to small Caribbean nations such as Haiti or the Dominican Republic. These instances were largely contained to "voodoo" zombies who were largely passive and the result of "voodoo wizards" using chemical substances to labotomized victims. The CDC has announced that true animated dead with the desire to consume human flesh has became a threat (http://emergency.cdc.gov/socialmedia/zombies_blog.asp). These animated dead cannibals are referred to as "zombies". These "zombies" have limited cognitive ability limited to seeking out and attacking the living. Higher mental processes such as complex though, abstract thinking, or basic communication skills are not present. A potential zombie outbreak poses a significant risk to the availability of information systems, life/safety issues, and could negatively affect production.

SYSTEM CHARACTERIZATION:

Animated Dead (Zombies)

- Unrelenting desire to consume human flesh, with violent tendencies.
- Spread through the air, bites, or direct contact. Thought to be viral in nature.
- Work in large groups, but without complex thought or action.
- Unable to be reasoned with or communicated to.
- Unpleasant visual appearance and smell.
- Does not respond to pain, fatigue, cold, heat, or other stimuli.

THREAT IDENTIFICATION:

- Employees could be consumed.
- Employees could be turned to zombies and negatively impact health/life insurance expenses.
- Collapse of society could result in supply chain issues, public utility delivery, and disrupted manufacturing capabilities.
- Facilities could be overrun by zombies resulting in manufacturing disruption.
- Reputation damage through mitigating infected employees.
- Damage to clean rooms which could result in the inability to certify composite components.
- Help desk could be over-whelmed resulting in SLA violation.
- Machine tools and tools could be damaged by being used as undead counter-measures.

VULNERABILITY IDENTIFICATION:

- Perimeter fences are not designed to withstand 3,000 undead.
- Limited ability to barricade the facilities (i.e. Plant II wide open, IPB3 doors don't lock, etc.)
- Engineering, IT, Finance, and Marketing lack hand tools to assemble anti-zombie counter-measures.
- BCP/DR plan does not have this contingency.
- Reliant on the outside world for supply chain activities.
- Lack of zombie awareness training for employees.
- 15,000 employees which could mean a lot of potential zombies.

CONTROL ANALYSIS:

The following controls are present:

- Large employee base with diverse background and a statistical tendency to be hunting/fishing, football, baseball, or NASCAR fans with access to heavy, sharp, corrosive, explosive, and toxic materials/tools.
- Medical clinic onsite for triage activities.
- Armed security response force.
- Paranoid IA/IT Security departments.

LIKELIHOOD DETERMINATION: Low

No apocalyptic incidents have occurred in the past, but they could occur in the future. There is that BioTechnology Project in...never mind.

IMPACT ANALYSIS: High

Complete destruction of humanity as we know it today, transformation of employees into zombies, and disruption of the global supply chain would have a very negative effect on system availability. Confidentiality and Integrity of data would not be impacted.

RISK DETERMINATION: Medium

There is a medium risk of a zombie apocalypse causing significant disruption of Spirit business processes.

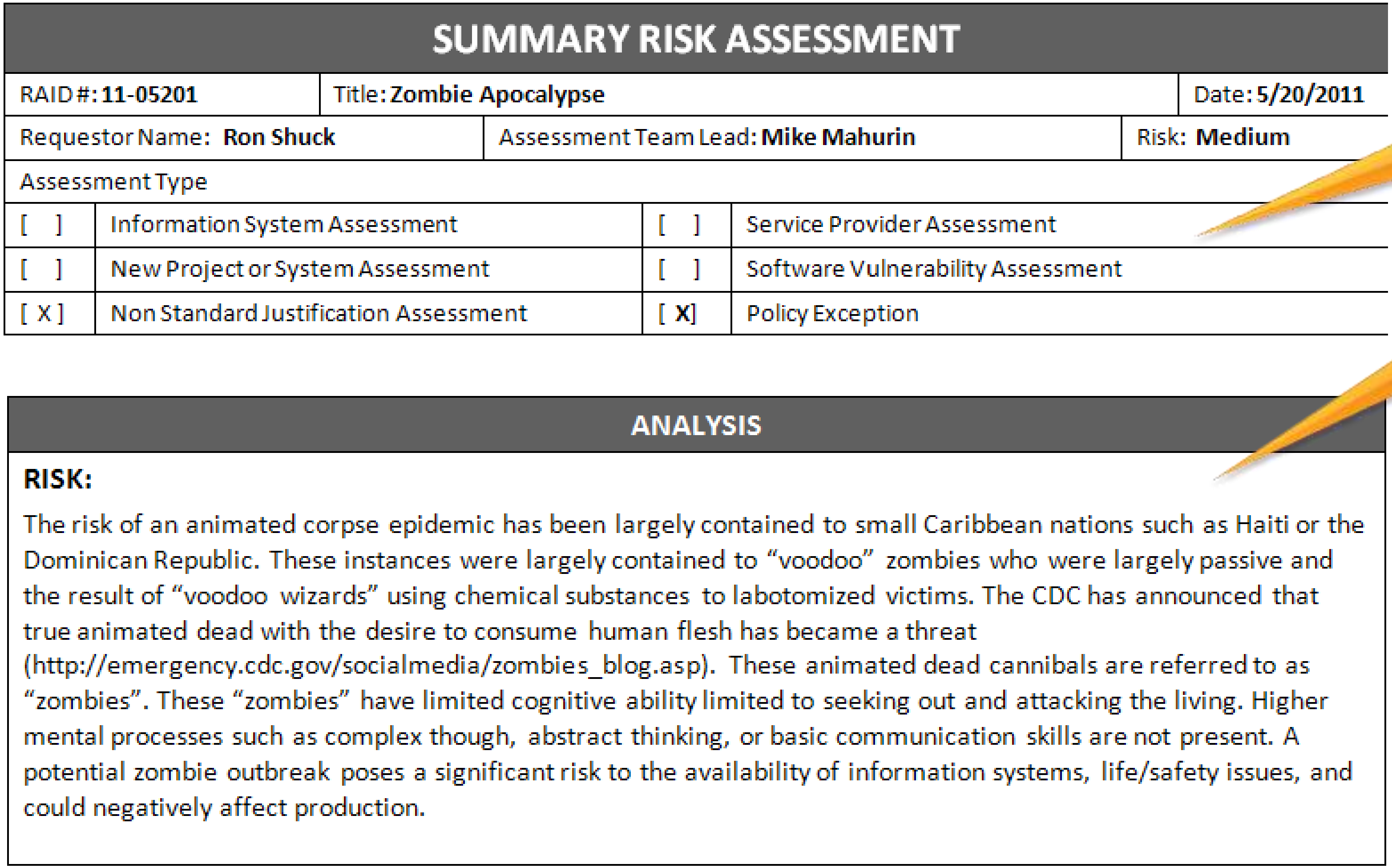
CONTROL REQUIREMENTS:

- Secure bunkers with 20 years of supplies should be established. SPS/IA/IT Security will provide security services for the facilities to maintain continuity of incident response activities.
- Weapons lockers will be implemented at strategic locations.
- Facilities will increase the ability to barricade buildings.
- Review this risk assessment in 1 year.

Review Cycle Date: (12 Months) 5/20/2012

ISSA™ Information Systems Security Association CENTRAL PLAINS CHAPTER

Sample Risk Form Header



SUMMARY RISK ASSESSMENT

RAID #: **11-05201**	Title: **Zombie Apocalypse**	Date: **5/20/2011**
Requestor Name: **Ron Shuck**	Assessment Team Lead: **Mike Mahurin**	Risk: **Medium**
Assessment Type		

[ ]	Information System Assessment	[ ]	Service Provider Assessment
[ ]	New Project or System Assessment	[ ]	Software Vulnerability Assessment
[X]	Non Standard Justification Assessment	[**X**]	Policy Exception

ANALYSIS

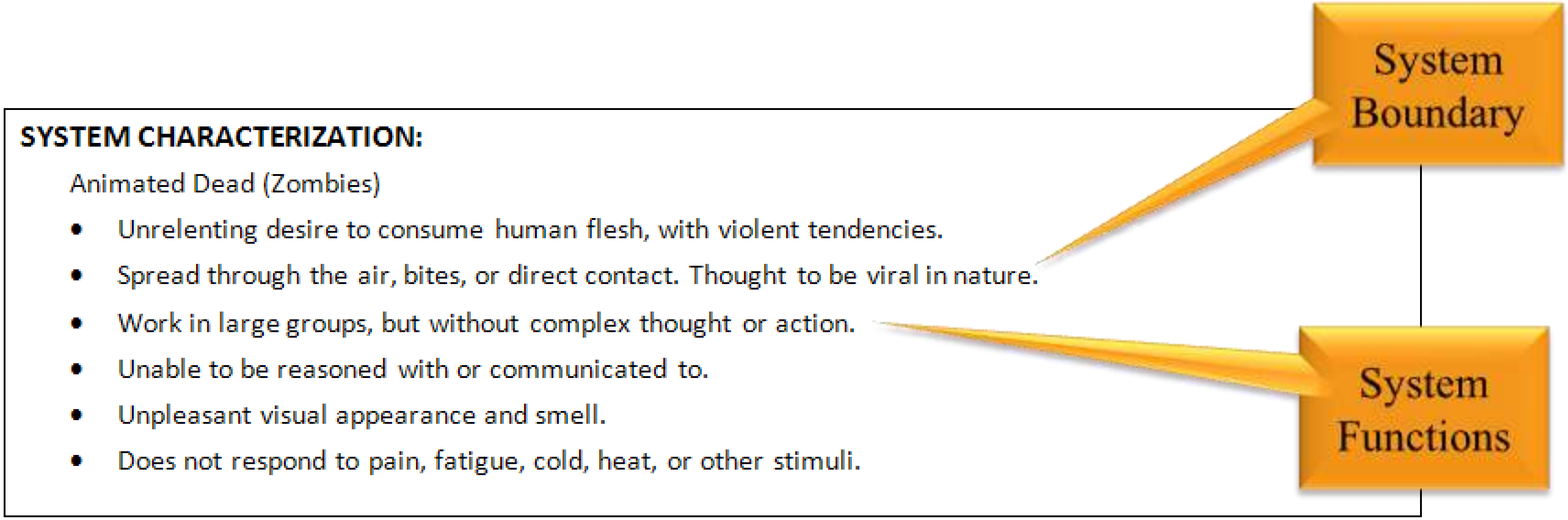
RISK:

The risk of an animated corpse epidemic has been largely contained to small Caribbean nations such as Haiti or the Dominican Republic. These instances were largely contained to "voodoo" zombies who were largely passive and the result of "voodoo wizards" using chemical substances to labotomized victims. The CDC has announced that true animated dead with the desire to consume human flesh has became a threat (http://emergency.cdc.gov/socialmedia/zombies_blog.asp). These animated dead cannibals are referred to as "zombies". These "zombies" have limited cognitive ability limited to seeking out and attacking the living. Higher mental processes such as complex though, abstract thinking, or basic communication skills are not present. A potential zombie outbreak poses a significant risk to the availability of information systems, life/safety issues, and could negatively affect production.

Summary

Description of Risk

Step 1 – System Characterization

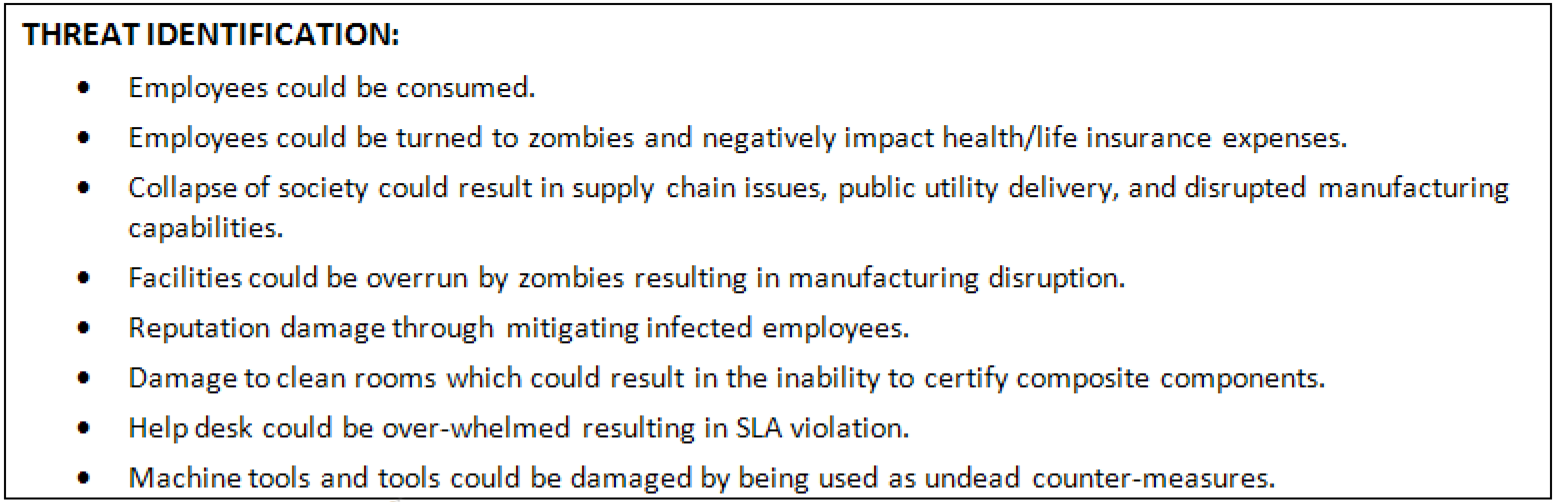


SYSTEM CHARACTERIZATION:

Animated Dead (Zombies)

- Unrelenting desire to consume human flesh, with violent tendencies.
- Spread through the air, bites, or direct contact. Thought to be viral in nature.
- Work in large groups, but without complex thought or action.
- Unable to be reasoned with or communicated to.
- Unpleasant visual appearance and smell.
- Does not respond to pain, fatigue, cold, heat, or other stimuli.

Step 2 – Threat Identification

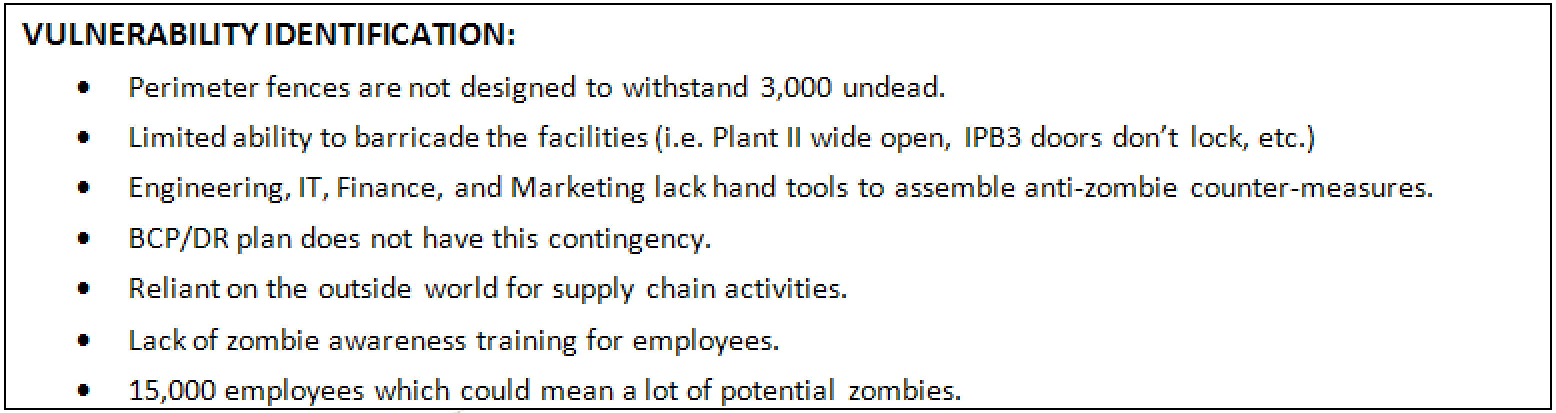


THREAT IDENTIFICATION:

- Employees could be consumed.
- Employees could be turned to zombies and negatively impact health/life insurance expenses.
- Collapse of society could result in supply chain issues, public utility delivery, and disrupted manufacturing capabilities.
- Facilities could be overrun by zombies resulting in manufacturing disruption.
- Reputation damage through mitigating infected employees.
- Damage to clean rooms which could result in the inability to certify composite components.
- Help desk could be over-whelmed resulting in SLA violation.
- Machine tools and tools could be damaged by being used as undead counter-measures.

Threat Statements

Step 3 – Vulnerability Identification

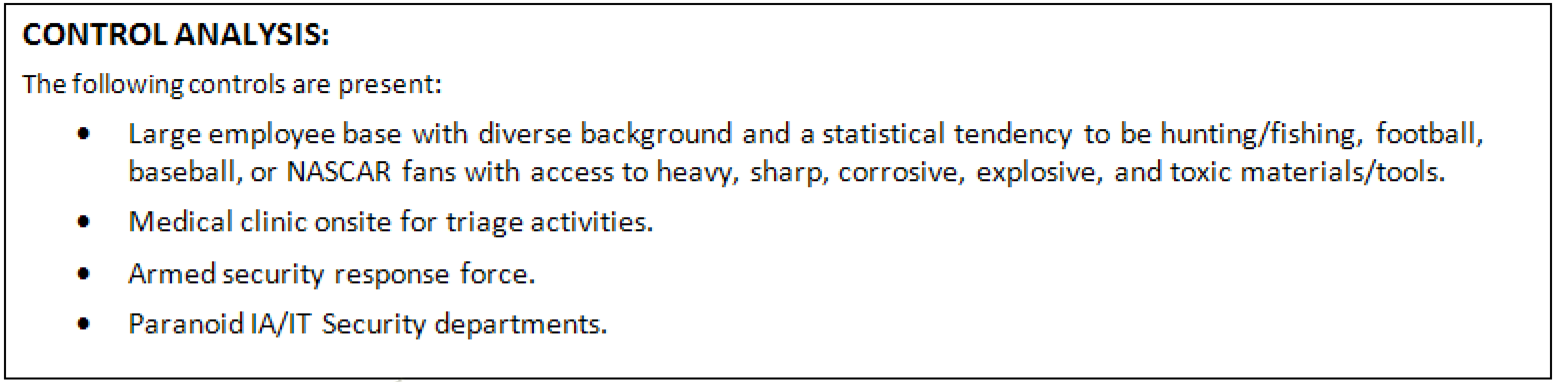


VULNERABILITY IDENTIFICATION:

- Perimeter fences are not designed to withstand 3,000 undead.
- Limited ability to barricade the facilities (i.e. Plant II wide open, IPB3 doors don't lock, etc.)
- Engineering, IT, Finance, and Marketing lack hand tools to assemble anti-zombie counter-measures.
- BCP/DR plan does not have this contingency.
- Reliant on the outside world for supply chain activities.
- Lack of zombie awareness training for employees.
- 15,000 employees which could mean a lot of potential zombies.

List of Vulnerabilities

Step 4 – Control Analysis



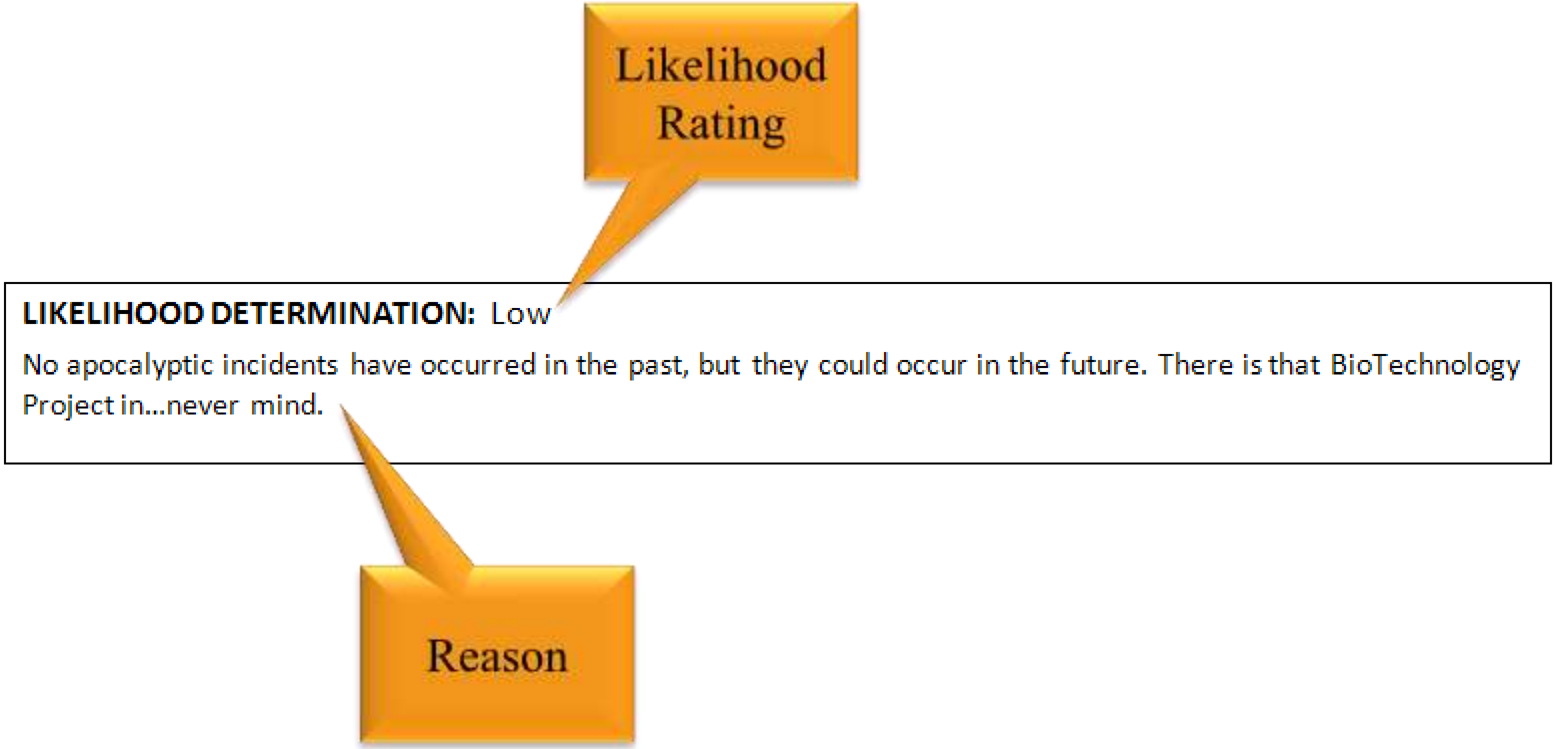
CONTROL ANALYSIS:

The following controls are present:

- Large employee base with diverse background and a statistical tendency to be hunting/fishing, football, baseball, or NASCAR fans with access to heavy, sharp, corrosive, explosive, and toxic materials/tools.
- Medical clinic onsite for triage activities.
- Armed security response force.
- Paranoid IA/IT Security departments.

List of Current Controls

Step 5 – Likelihood Determination



Likelihood Rating

LIKELIHOOD DETERMINATION: Low

No apocalyptic incidents have occurred in the past, but they could occur in the future. There is that BioTechnology Project in…never mind.

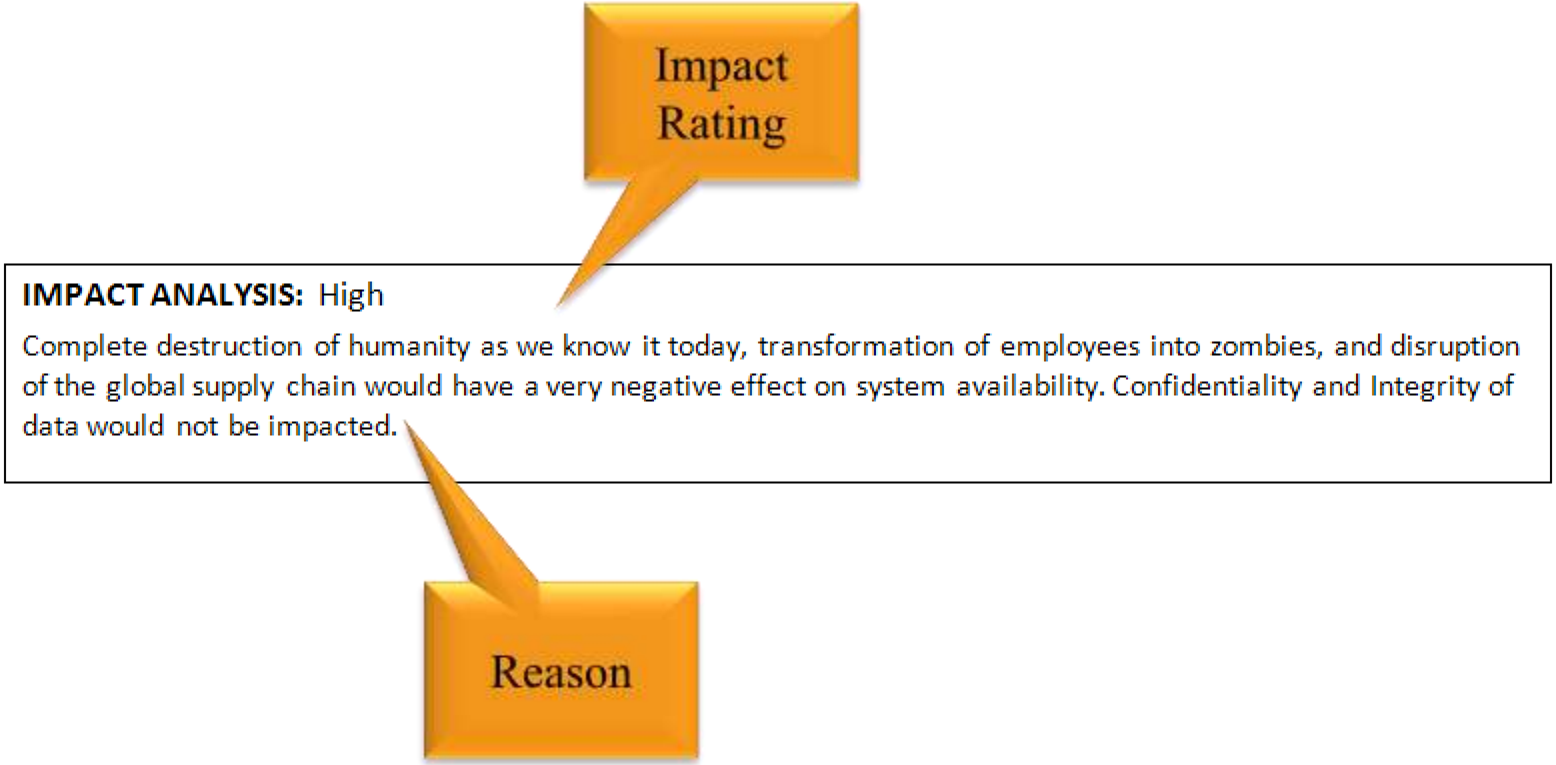
Reason

Likelihood Determination

The level of likelihood is a judgment based decision based on experience, technical analysis, and judgment. Criteria to develop this can range from CVE ratings, vendor ratings, or opinion. Must have valid data to support your position.

Irrelevant	Low	Medium	High
• Low level that doesn't warrant consideration	• Theoretical • Extremely Complex • Seen 1 in 10 years or more	• Practical • Moderately Complex • Seen 1 in 5 years	• Common • Simple to execute • Seen more then once in 1- 4 years

Step 6 – Impact Analysis



Impact Rating

IMPACT ANALYSIS: High

Complete destruction of humanity as we know it today, transformation of employees into zombies, and disruption of the global supply chain would have a very negative effect on system availability. Confidentiality and Integrity of data would not be impacted.

Reason

Impact Analysis

The impact of this risk describes the negative effect realizing the risk would have on Spirit business operations. These can be derived from discussions with the business group, industry research, professional opinion, and judgment.

Irrelevant

- Impact does no damage to Spirit

Low

- Minimal impact of less then $1,000
- Minimal chance of significant business impact

Medium

- Moderate impact of less then $100,000 to the business
- Moderate business impact

High

- Impact of greater then $100,000
- Life/Safety issues

Step 7 – Risk Determination

Risk Rating

RISK DETERMINATION: Medium

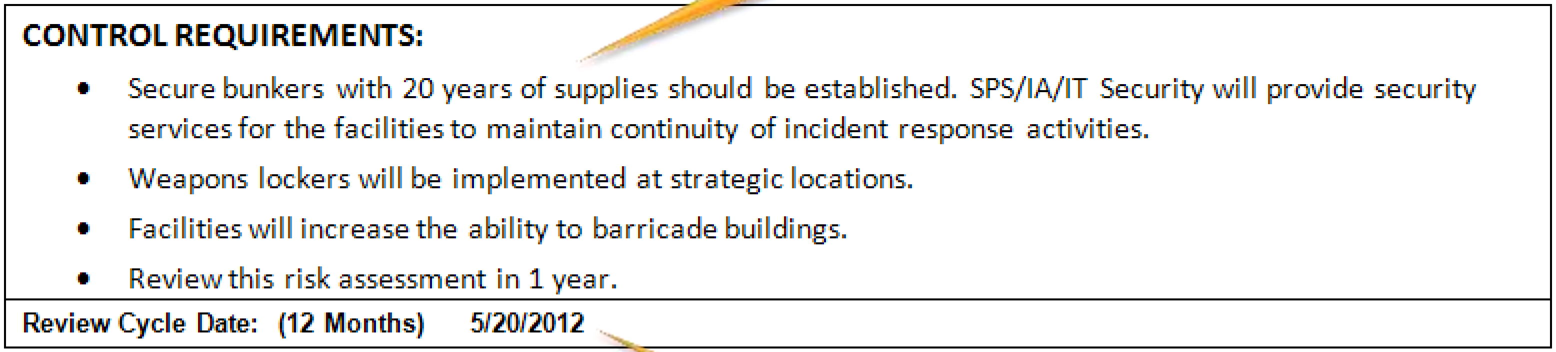
There is a medium risk of a zombie apocalypse causing significant disruption of Spirit business processes.

Reason

Impact	**High**	**Medium**	**High**	**Critical**
	Medium	**Low**	**Medium**	**High**
	Low	**Low**	**Low**	**Medium**
		Low	**Medium**	**High**
			Likelihood	

Step 8 – Control Requirements

Control Requirements



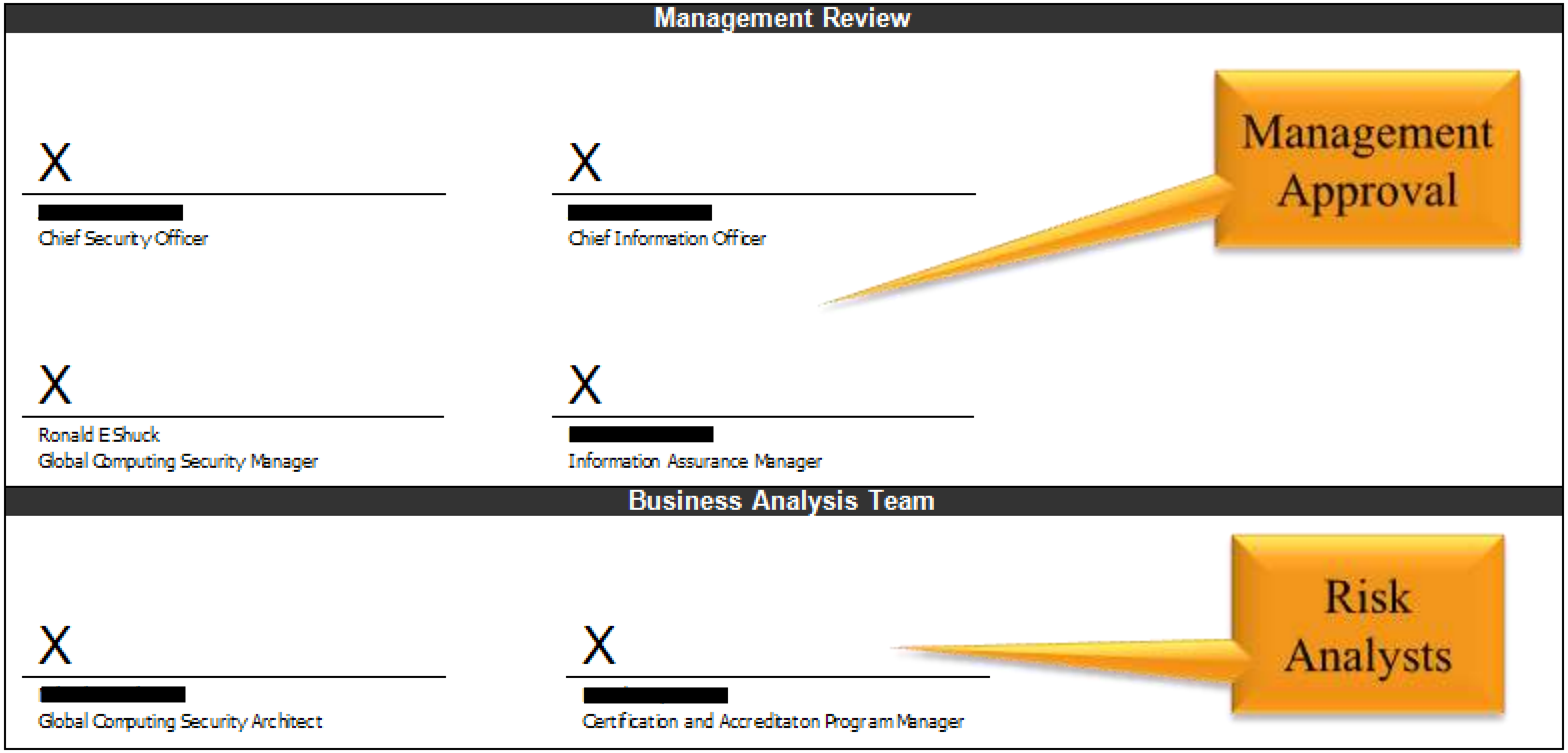
CONTROL REQUIREMENTS:

- Secure bunkers with 20 years of supplies should be established. SPS/IA/IT Security will provide security services for the facilities to maintain continuity of incident response activities.
- Weapons lockers will be implemented at strategic locations.
- Facilities will increase the ability to barricade buildings.
- Review this risk assessment in 1 year.

Review Cycle Date: (12 Months) 5/20/2012

Review Period

Step 9 – Risk Report



Management Review

X

[redacted]
Chief Security Officer

X

[redacted]
Chief Information Officer

X

Ronald E Shuck
Global Computing Security Manager

X

[redacted]
Information Assurance Manager

Business Analysis Team

X

[redacted]
Global Computing Security Architect

X

[redacted]
Certfication and Accreditaton Program Manager

Management Approval

Risk Analysts

Step 10 – Risk Tracking

- Consider Share Point
  - Use workflows
- Use Spreadsheet

Risk Management

Questions