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

RISK MANAGEMENT

ERM & eGRC Tools

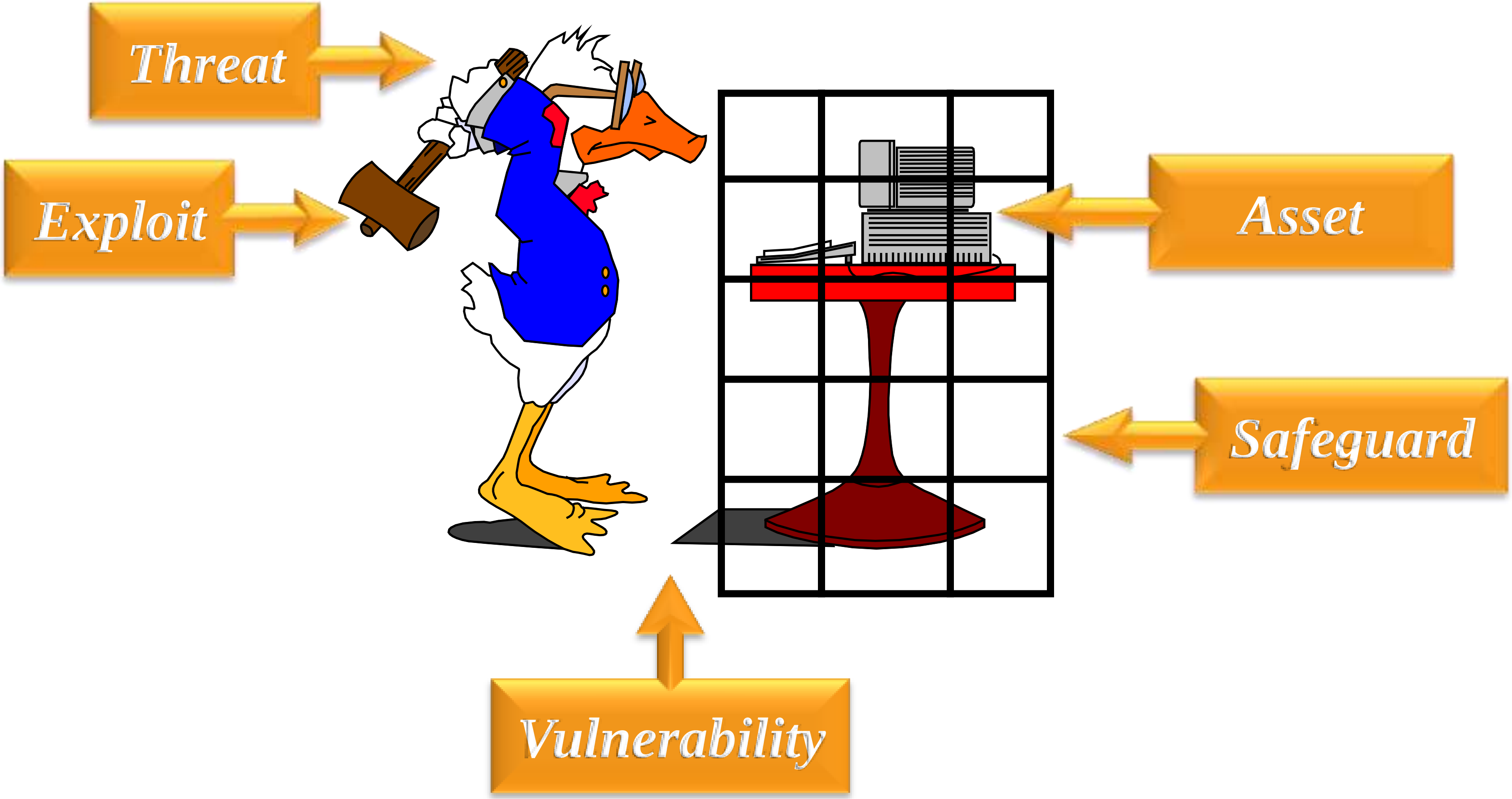
December 2, 2011

ISSA™
Information Systems Security Association
CENTRAL PLAINS CHAPTER

Overview

- What is Risk
- Threats, Vulnerabilities, & Exploits
- Identification of Risk
- Management of Risk
- Business Risk
- ERM Development
- eGRC Tool Deployment

Risk



Threat

Exploit

Asset

Safeguard

Vulnerability

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)

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

ISSA™ Information Systems Security Association CENTRAL PLAINS CHAPTER

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 Knowledg

Tool

- Pre-built
- Custom Designed
- Easy to Acquire

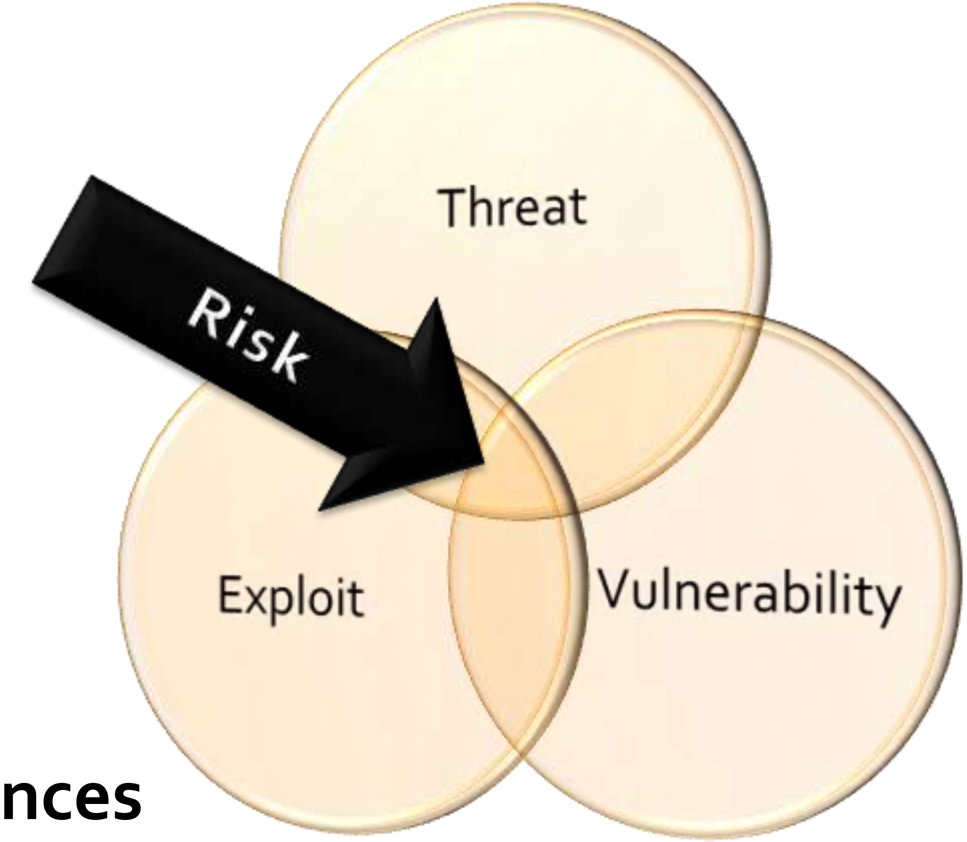
Opportunity

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

ISSA™ Information Systems Security Association CENTRAL PLAINS CHAPTER

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**

Business Risk

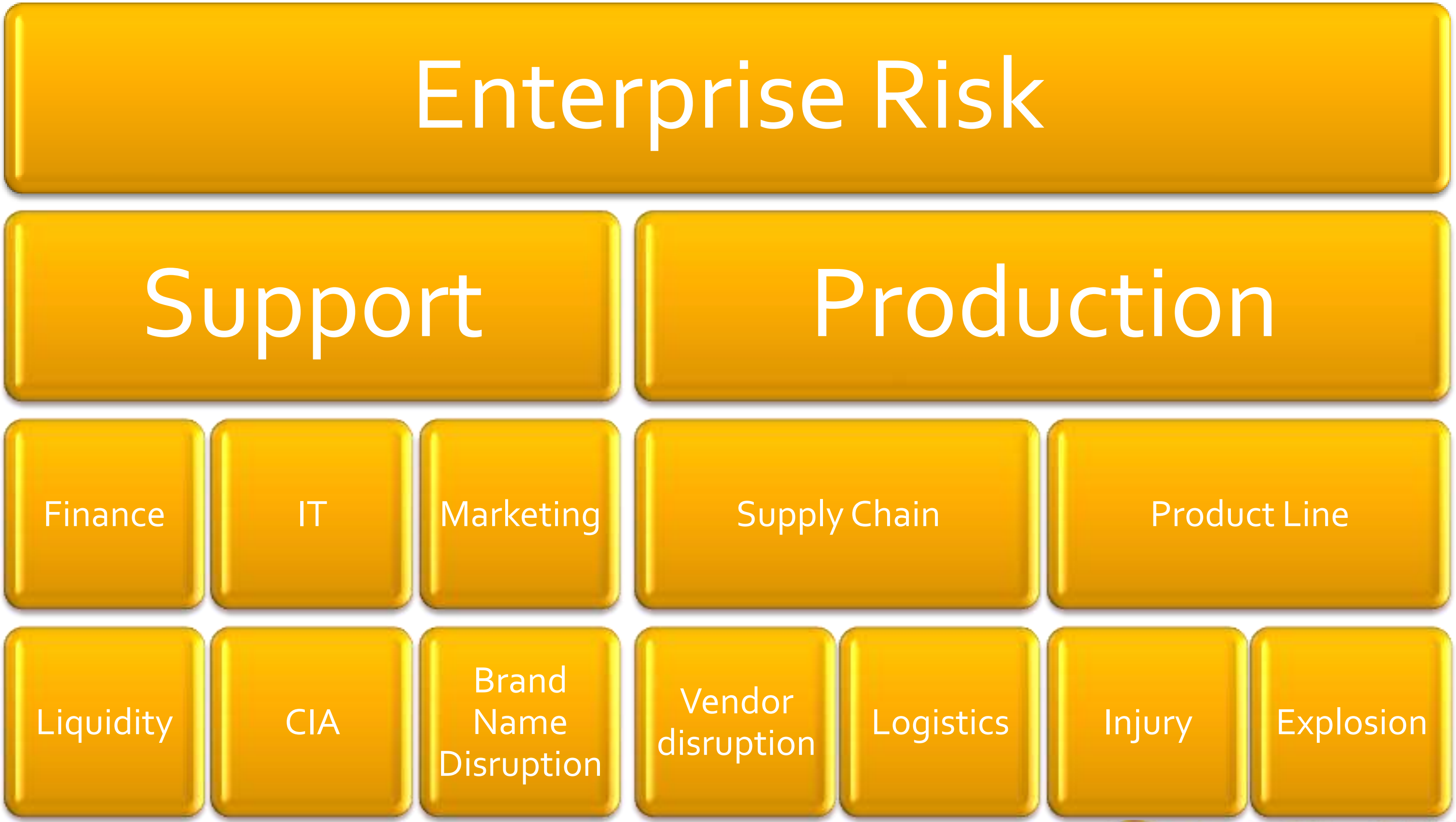
- **Business Risk**
  - An uncertain event that could have a positive or negative impact to the company.
  - Actions can be taken to influence the outcome of the event.
- **Positive**
  - Acquiring company X will allow us to bring in Y revenue, but it could also fail costing us Z.
- **Negative**
  - Failing to apply a patch to the server could result in compromise which would cost us X, but patching the server will cause an outage that costs Y.

Goal

Develop ways for the business to assess and manage risk.

- **Risk Assessment**
  - Identifying risks
  - Measuring risks
  - Reporting risks
- **Risk Management**
  - Facilitate decision making with tools to take action to maximize profitability.
  - Facilitate the use of risk management tools: avoid, accept, mitigate, transfer, or ignore.
  - Report outcomes of risk management decision's.

Risks in Enterprise



Enterprise Risk

- Support
  - Finance
    - Liquidity
  - IT
    - CIA
  - Marketing
    - Brand Name Disruption
- Production
  - Supply Chain
    - Vendor disruption
    - Logistics
  - Product Line
    - Injury
    - Explosion

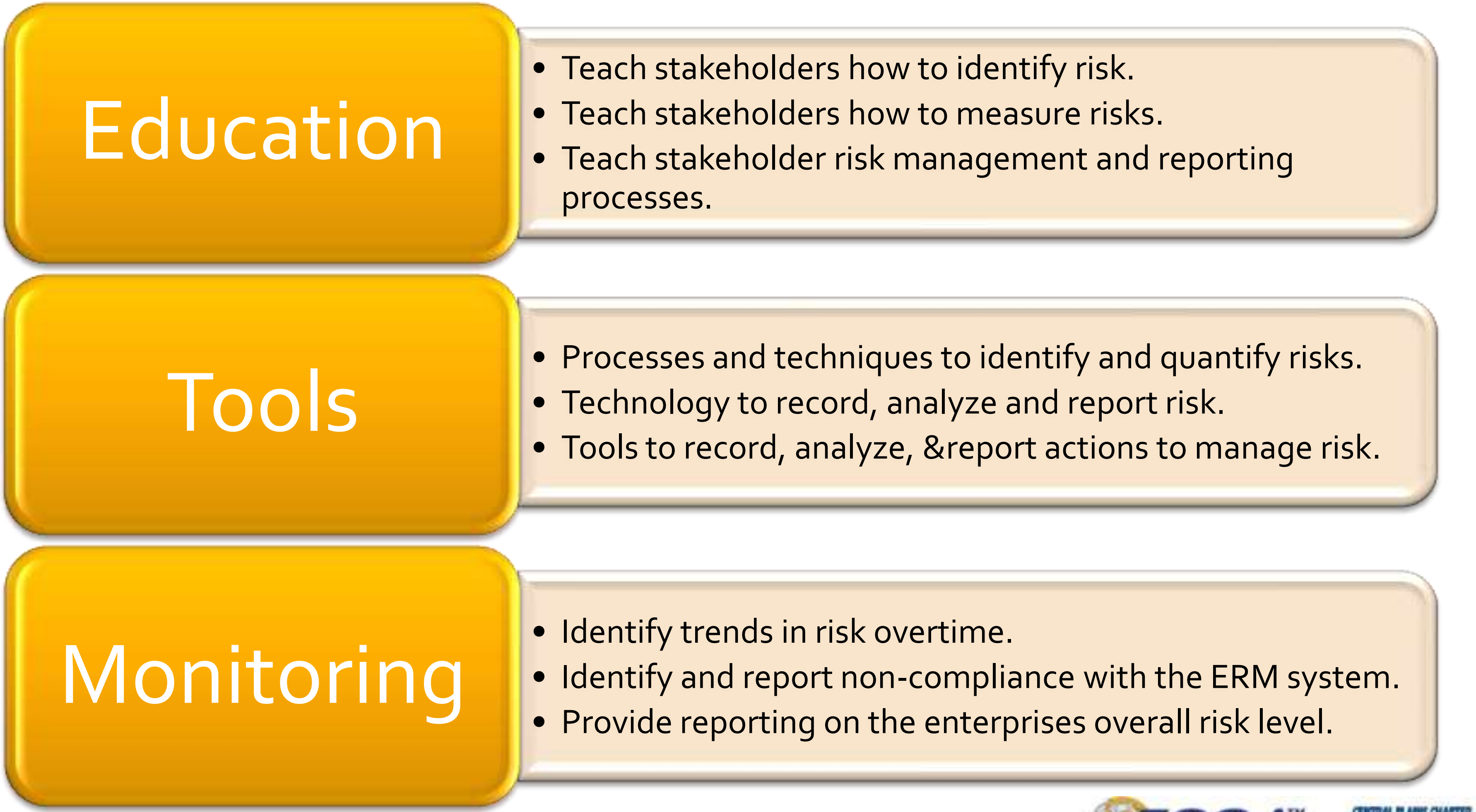
Place of IT Risk

- **IT Security**
  - Lower level risk
  - Very few businesses would be knocked out of business due to an IT Security incident.
- **Example**
  - Name 1 company that has been taken out of business due to an IT Security Incident. HBGary is still operational…
  - Name 3 companies that have been taken out of business due to accounting fraud.

Place of IT Risk

- **IT Security Value Proposition**
  - Reduction of risk to enhance business profitability and increase business opportunities.
  - Support availability of production assets.
  - Protect intellectual property.
- **Creating Value**
  - Implementing a counter fraud software into SAP to reduce vendor fraud by 20% saving $1 million.
  - Enabling a company to provide secure Internet based partner connection saving 30% versus dedicated circuits.
- **Destroying Value**
  - Putting excessive controls in place for low risk threats.
  - Mis-representing risk and avoiding potentially profitable business opportunities.

IT Role



Education

- Teach stakeholders how to identify risk.
- Teach stakeholders how to measure risks.
- Teach stakeholder risk management and reporting processes.

Tools

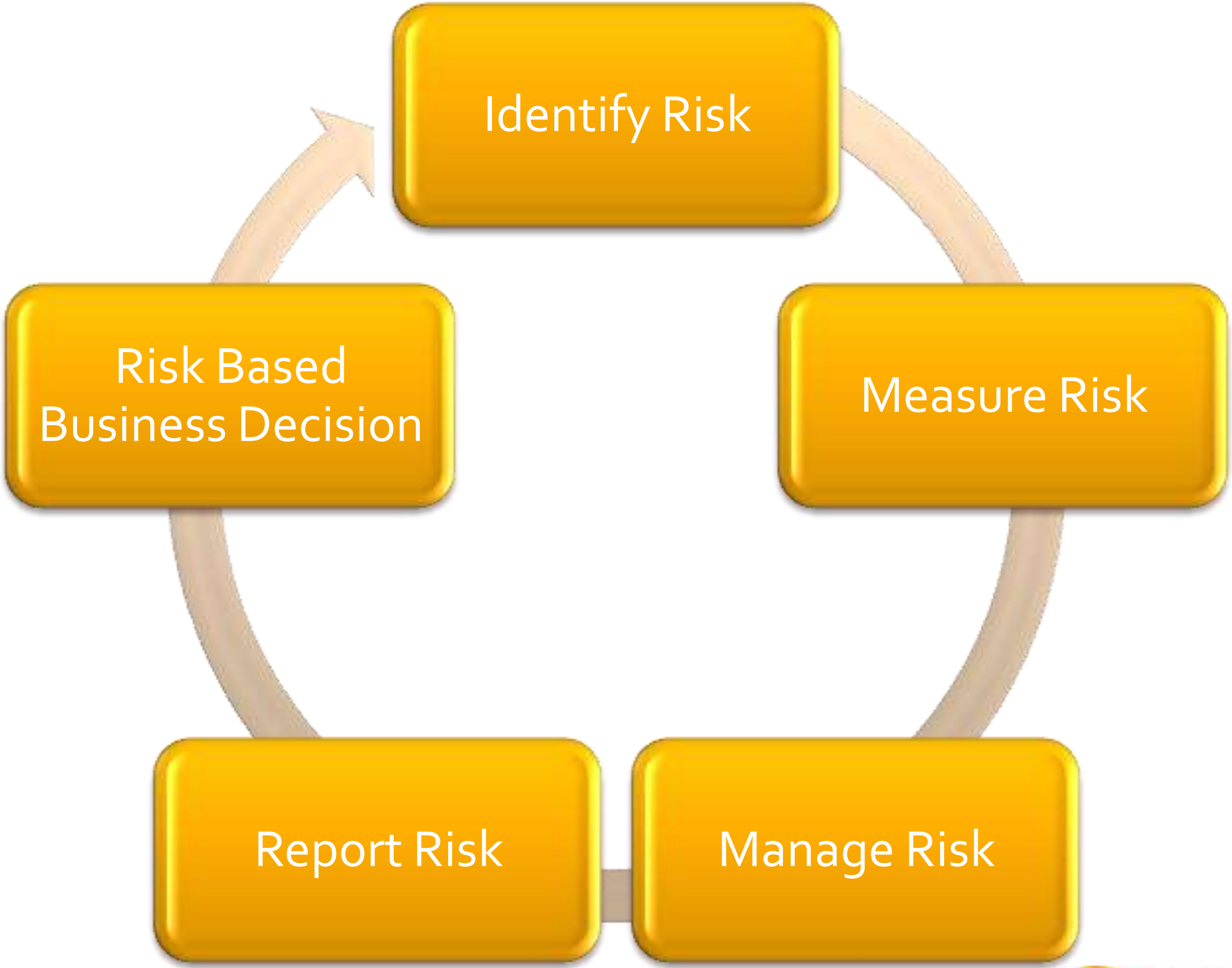
- Processes and techniques to identify and quantify risks.
- Technology to record, analyze and report risk.
- Tools to record, analyze, &report actions to manage risk.

Monitoring

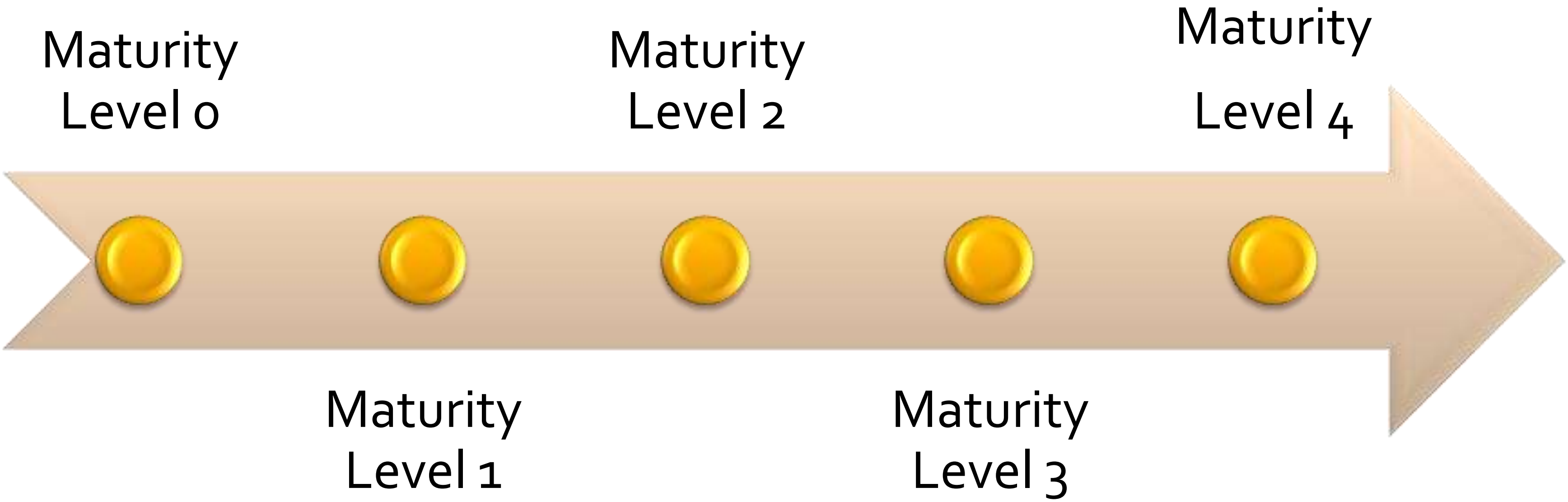
- Identify trends in risk overtime.
- Identify and report non-compliance with the ERM system.
- Provide reporting on the enterprises overall risk level.

ISSA™ Information Systems Security Association CENTRAL PLAINS CHAPTER

Enterprise Risk Management (ERM)



ERM Development



Maturity Level 0

Maturity Level 1

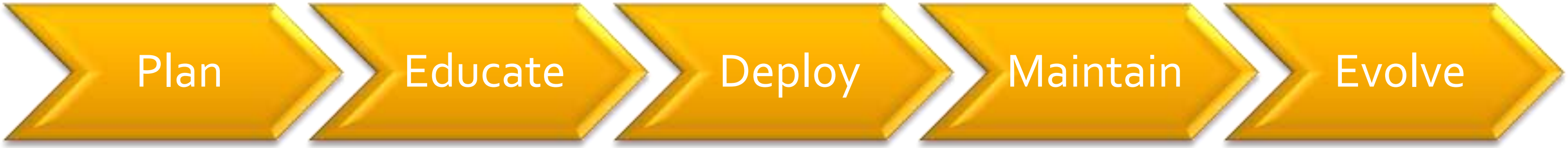
Maturity Level 2

Maturity Level 3

Maturity Level 4

Overall ERM Process

To raise the maturity level we must go through each of these phases for each level of maturity.



Plan

Educate

Deploy

Maintain

Evolve

Plan

- **Define Objectives**
  - Which business units can benefit from risk management.
  - Understand the business and develop business drivers.
- **Develop ERM Strategy**
  - Establish management support
  - Identify current maturity level
  - Determine key stakeholders
- **Develop ERM Plan**
  - What tools need to be used?
  - Who will be the business owner?
  - Order of business units adopting (1 or 2 at a time)

Educate

Risk

- What is risk?
- Why does it need to be managed?
- How do me get the best business value?

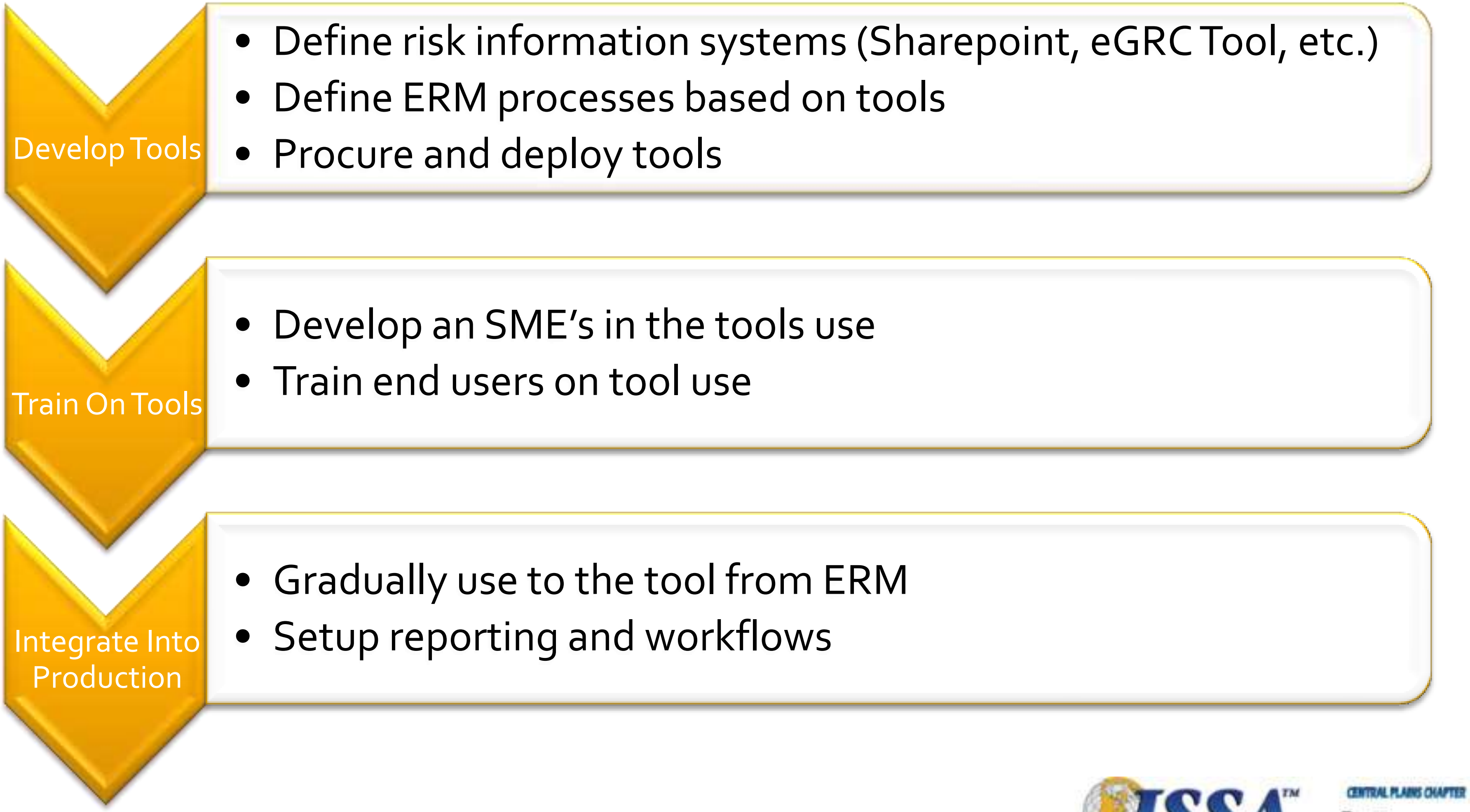
Risk Assessment

- How is risk identified?
- How is measure risk measured?
- How is risk reported?

Risk Management

- Who decides what to do?
- What are the options to deal with the risk?
- How do you track compliance?

Deploy



Develop Tools

- Define risk information systems (Sharepoint, eGRC Tool, etc.)
- Define ERM processes based on tools
- Procure and deploy tools

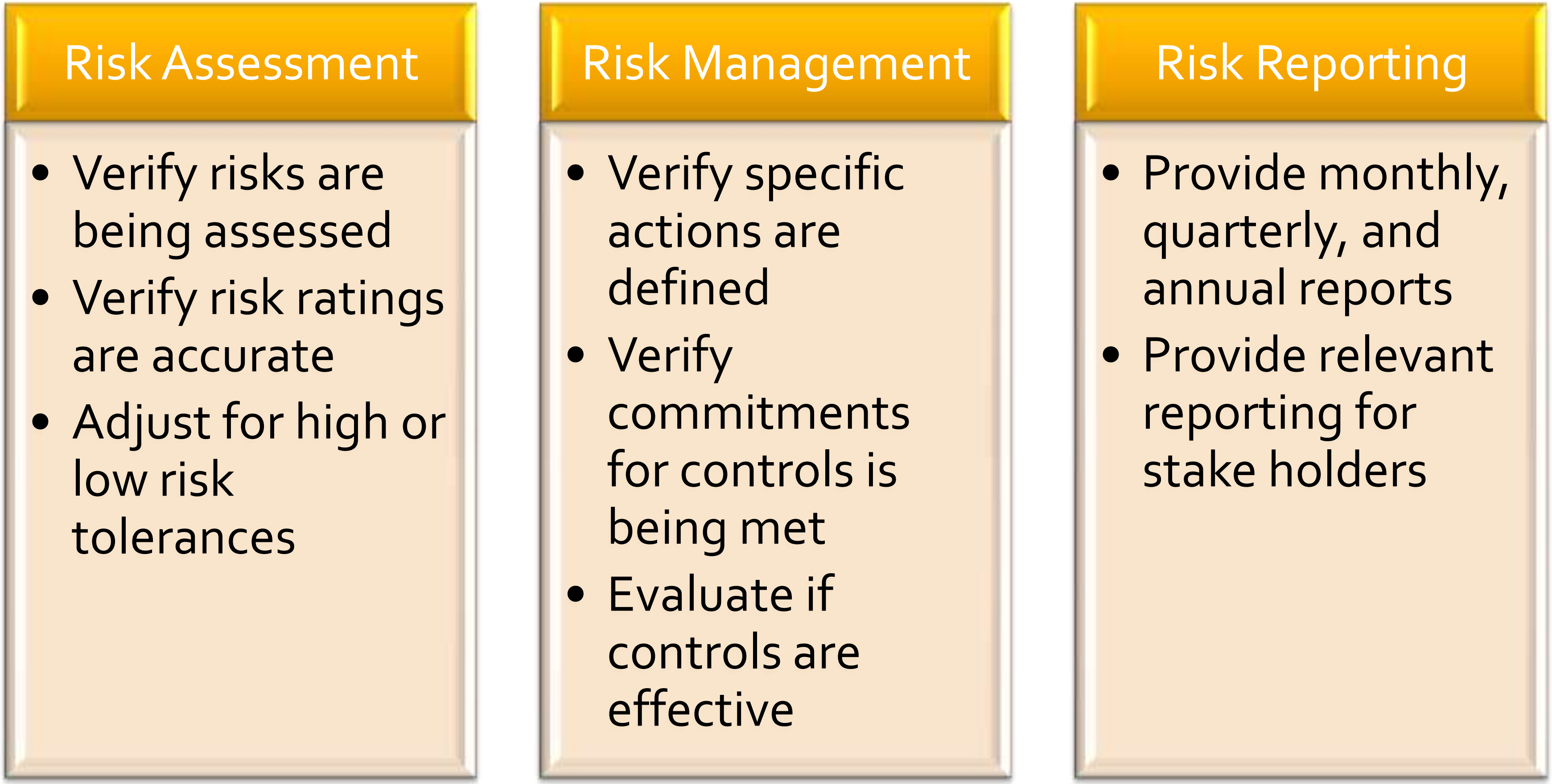
Train On Tools

- Develop an SME’s in the tools use
- Train end users on tool use

Integrate Into Production

- Gradually use to the tool from ERM
- Setup reporting and workflows

Maintain



Risk Assessment

- Verify risks are being assessed
- Verify risk ratings are accurate
- Adjust for high or low risk tolerances

Risk Management

- Verify specific actions are defined
- Verify commitments for controls is being met
- Evaluate if controls are effective

Risk Reporting

- Provide monthly, quarterly, and annual reports
- Provide relevant reporting for stake holders

Evolve

- **Maturity Level**
  - Does increasing the maturity level make business sense?
  - Quantify the benefit in financial terms.
- **Streamline Process**
  - Identify ways to increase efficiency.
  - Determine if the ERM program should expand.
  - Evaluate technologies to facilitate streamlining.

eGRC Tools

Enterprise Governance Risk & Compliance

- **eGRC Tool Provides**
  - Standardized risk models with consistent threat, vulnerability, likelihood, and impact ratings.
  - Scoring model that defines risk classification.
  - Records/reports risks, actions taken to manage risks, and summarizes organizations risk levels.
- **eGRC Does Not**
  - Automatically measure risk.
  - Does not remediate risks.
  - Does not manage risks.

When Needed

- **Enhance and Existing ERM Program**
  - The organization (not just IT) should have a commitment to ERM.
  - Cannot be forced on departments.
  - Does not provide risk assessment and management skills.
- **Complex Environments**
  - Large organization.
  - Numerous business units.

Tool Selection

- **Review Product Capabilities**
  - Get list of Gartner, Forester, or ISACA list of prominent vendors.
  - Review capabilities of at least three products.
- **Define Product Requirements**
  - Determine what features meet you ERM needs.
  - Work through a multi-business unit evaluation team.
  - Just because it meets IT requirements does not mean it will meet business needs.

Tool Implementation

- **Education on Tool**
  - SME level skills on the tool are required before deployment.
  - Poor setup or support skills will quickly make the tool untrusted in the organization.
- **Phased Approach**
  - Do not implement all features at once.
  - Do not start by adding automatic feeds from security tools.

Tool Implementation

- **User Driven Questionnaires**
  - Move to questionnaire with analyst review.
  - Develop for the various assessment types.
  - Develop instruction for completing assessments.
  - Develop risk management reporting procedure.
- **Integrate with other processes**
  - Certification and Accreditation.
  - Incident Response.

Tool Implementation

- **Develop dashboards and reports**
  - Develop automated report distribution settings.
  - Develop efficiency metrics.

Risk Management

Questions