

FoRMA: An Open Framework of Risk Management & Analysis for Information Security

Kris Kahn,
January 17, 2007

Agenda

- Introduction
- Audience
- Objectives
- Overview of FoRMA
- Benefits of FoRMA
- Questions & Answers
- References

Introduction

- About the author
 - **Kris Kahn, CISSP,-ISSAP,-ISSMP, CISA, OPSA**
 - **Sr Governance Analyst, Seagate Technology LLC**
- About the model
 - **Three years in development**
 - **Based on author's security and audit experience**
- About this presentation
 - **Balancing Risk Management in Information Security**

Audience

- Responsibilities may include
 - Information Security
 - Operations Security
 - Risk Managers
 - Company Officers
- Experience and knowledge may include
 - Familiarity with Security Best Practices
 - Understanding of Risk Management Concepts

Objectives

- **Big Picture:** FoRMA will help to provide a holistic vision and strategic understanding of the relationships of many of our current and familiar security models.
- **Technology independent:** FoRMA is flexible and can be applied to information security, physical security, even medical risk management.
- **Business Focused:** FoRMA will demonstrate how to achieve business objectives by controlling risk to acceptable levels, not by maximizing security.

Overview

- A new model focusing on balance and appropriate control
- An Open Framework for integrating industry standard models, such as CIA*, STRIDE* and others
- Addresses Risk and Control elements:
 - **Risk**
 - Threat
 - Vulnerability
 - **Control**
 - Technology
 - Process

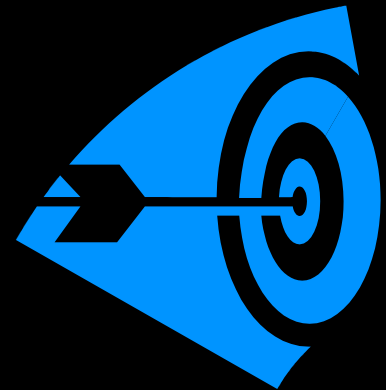
*: See references at the end of the presentation material

FoRMA Goal: Risk Mitigation

- **Control risks within acceptable limits to support business objectives**

Establish Your Boundaries

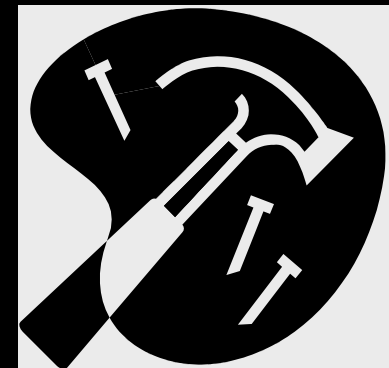
- Define relevant **policies**, standards and best-practices
- Protect assets and resources in accordance with **policy**
- Detect **policy** violations
- Assure **policy** compliance



Build your foundation

Start from the ground level and work your way up!

- Construct a strong security foundation to build your security policies, standards and best-practices. Use industry established security methodologies and codes of best practice to guide your standards and practices.
- A security foundation supporting all IT layers (including information, infrastructure, application, etc), and addressing each security implementation phase (Awareness, Protection, Detection, and Assurance).



Build your foundation: Leverage your security models

Methodology	Model	Subject
Threat Management	STRIDE*	Threat
Security Architecture	APAIN*	Technology
Security Management	RIVET*	Process
Asset/Resource Management	CIA*	Vulnerability

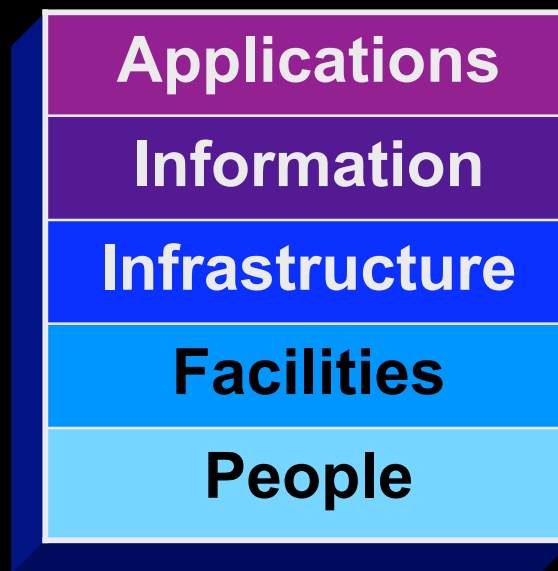
Use **Methodology** with **Model** to evaluate **Subject**

*: See references at the end of the presentation material

Build your foundation:

Identify your scope

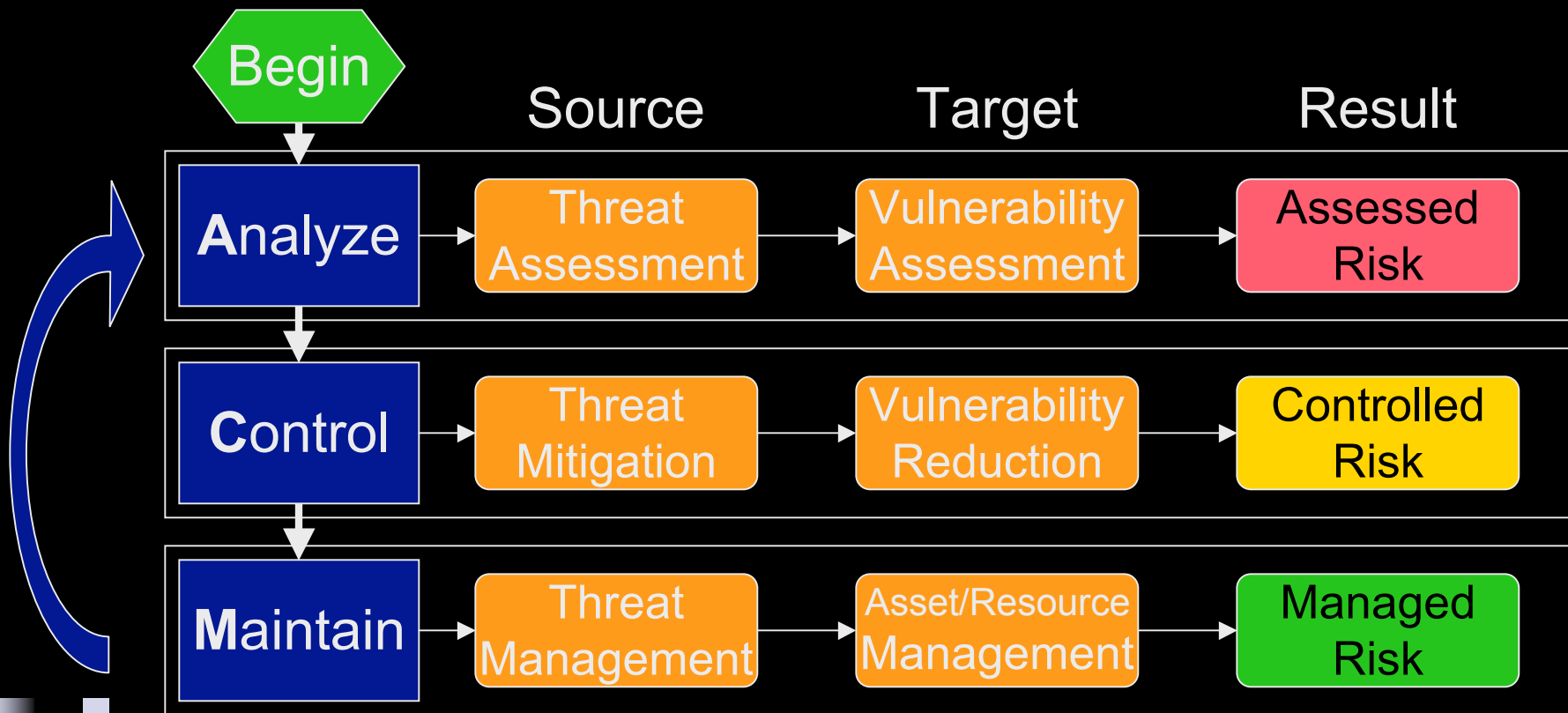
- This is a layered model based on the COBIT IT Resource model* which identifies five (of the original seven) layers of critical assets and resources we want to protect for Information Security.



*: See references at the end of the presentation material

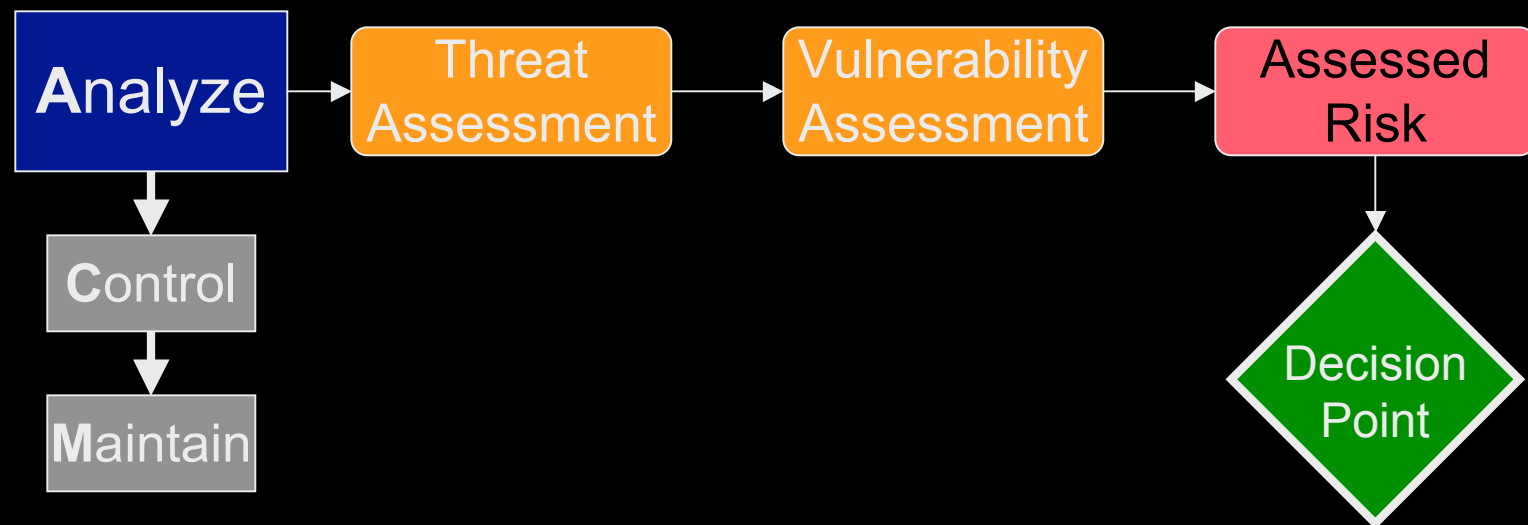
Risk Mitigation Cycle

- Analyze, Control, Maintain, repeat.
- This process life cycle will guide you through the security model to the appropriate security resolution.



Risk Mitigation Cycle: Analyze

- First, to determine the risk, you must understand the threat of attack and the vulnerability of the asset or resource. We measure and analyze these items to determine the corresponding risk.
- FoRMA is flexible to support a Qualitative or Quantitative Analysis



Risk Mitigation Cycle: Analyze

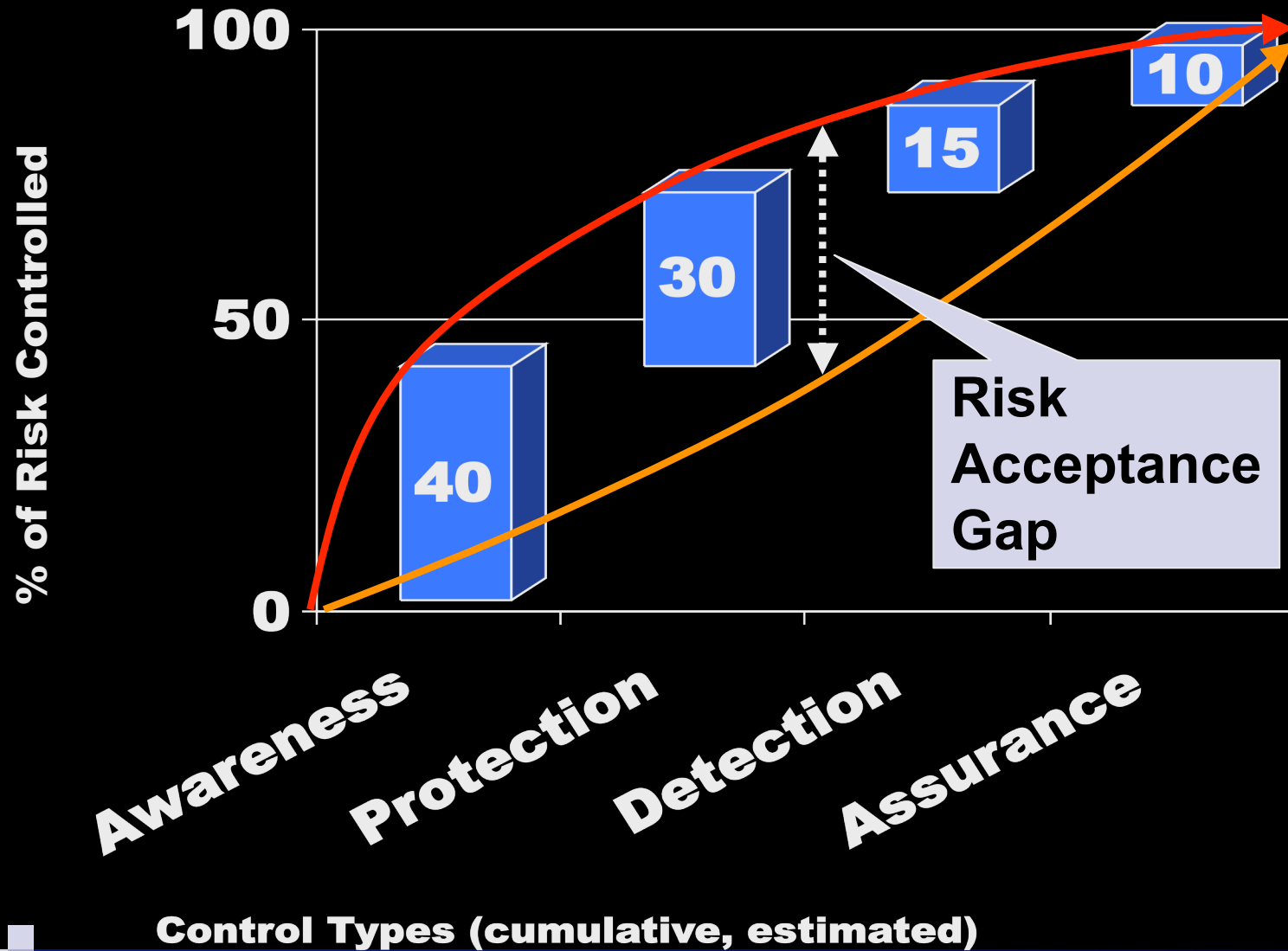


- Decision point
 - **Determine if there is necessity to proceed with implementation of controls to reduce Risk Acceptance Gap**

- Risk Level vs. Value of Asset/Resource
 - **Evaluate findings to determine level of acceptable risk**
 - **Consider recovery/replacement costs**
 - **Consider if existing controls would detect or prevent the risk**

- Risk Acceptance Gap
 - **The difference between existing risk and the level of acceptable risk**

Acceptable Level of Risk



Control Cost in % of Risk Impact

Risk Mitigation Cycle: Analyze

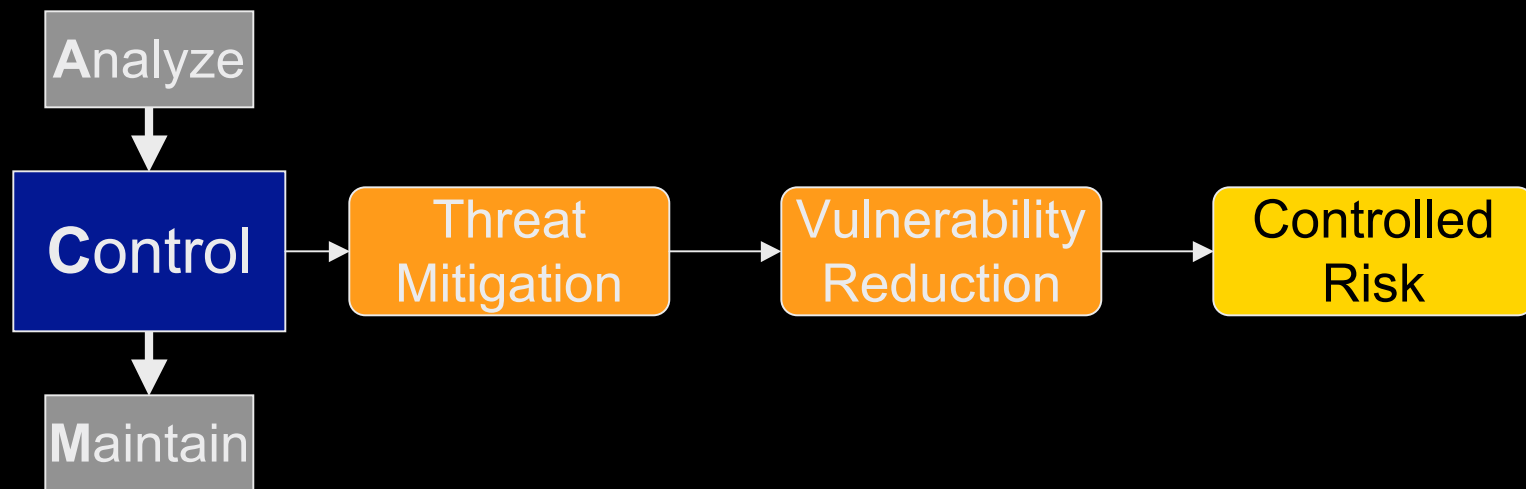
- Qualitative Analysis Tools
 - **The STRIDE* model can be used to help identify key Threats.**
 - **The CIA* model can be used to help identify key Vulnerabilities.**

- Quantitative Analysis Tools
 - **A Failure-Mode Effects Analysis* (FMEA) can be used to generate a more specific Risk Priority score for identified scenarios**
 - **Use with Annual Loss Expectancy* (ALE) to determine likelihood of Business impact**

*: See references at the end of the presentation material

Risk Mitigation Cycle: Control

- Apply counter-measures and control-mechanisms together to mitigate the threat or reduce the vulnerability.
- Once controls are implemented, compare against the level of acceptable risk to ensure appropriate coverage.



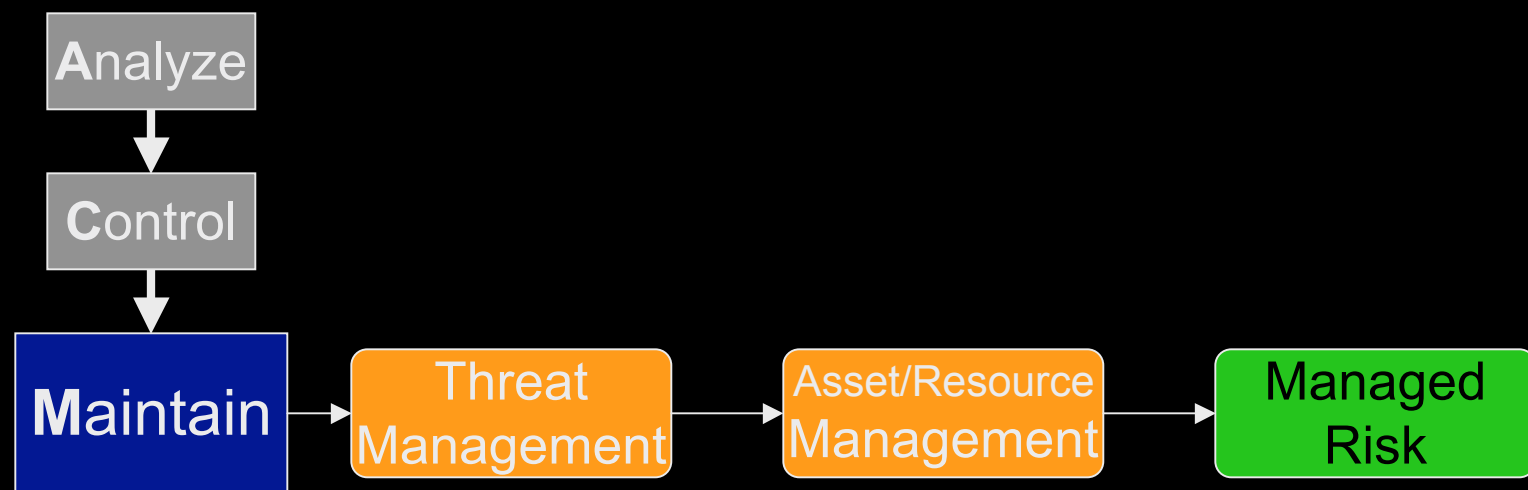
Risk Mitigation Cycle: Control

- Qualitative Analysis Tools
 - **The RIVET* model can be used to help identify key process solutions.**
 - **The APAIN* model can be used to help identify technology solutions.**
- Quantitative Analysis Tools
 - **Compare results of the FMEA to a Maturity Assessment as used by COBIT or Carnegie Mellon Capability Maturity Model**

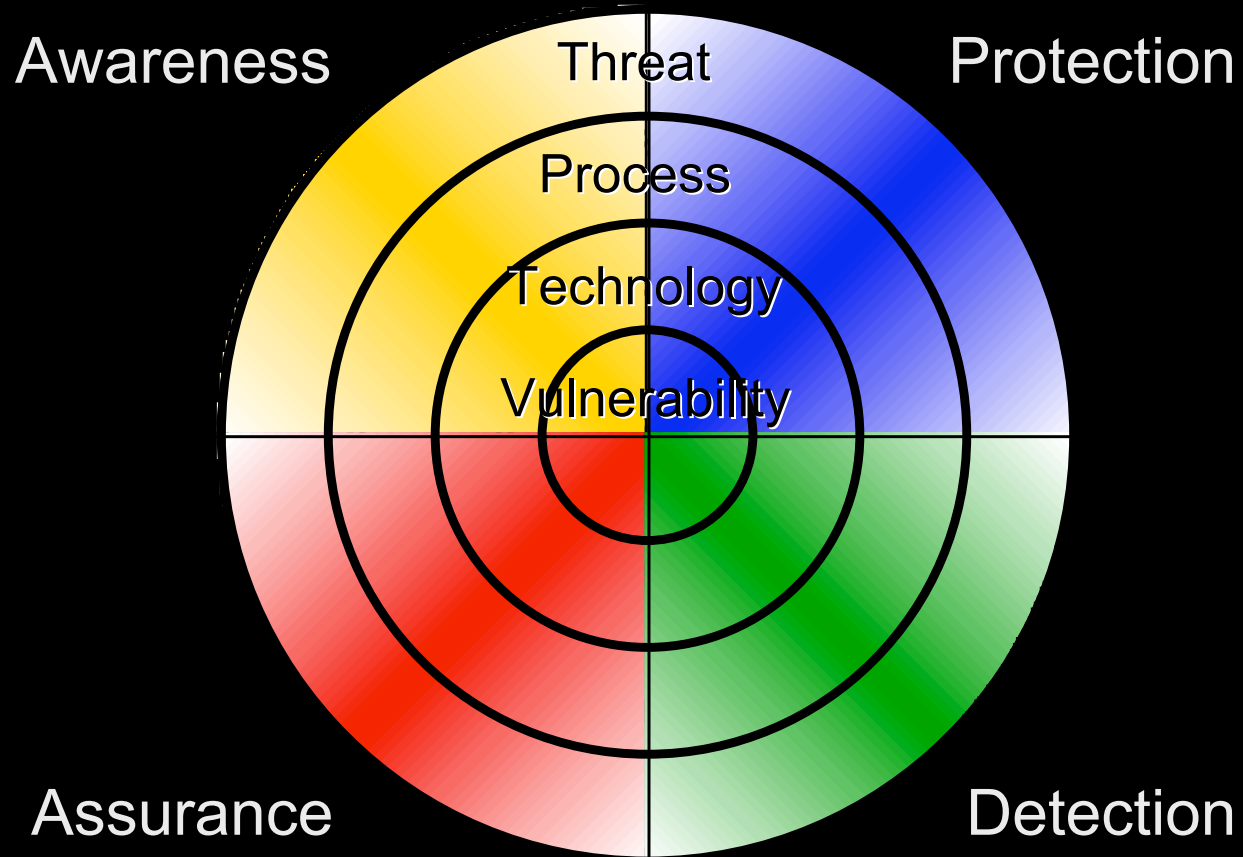
*: See references at the end of the presentation material

Risk Mitigation Cycle: Maintain

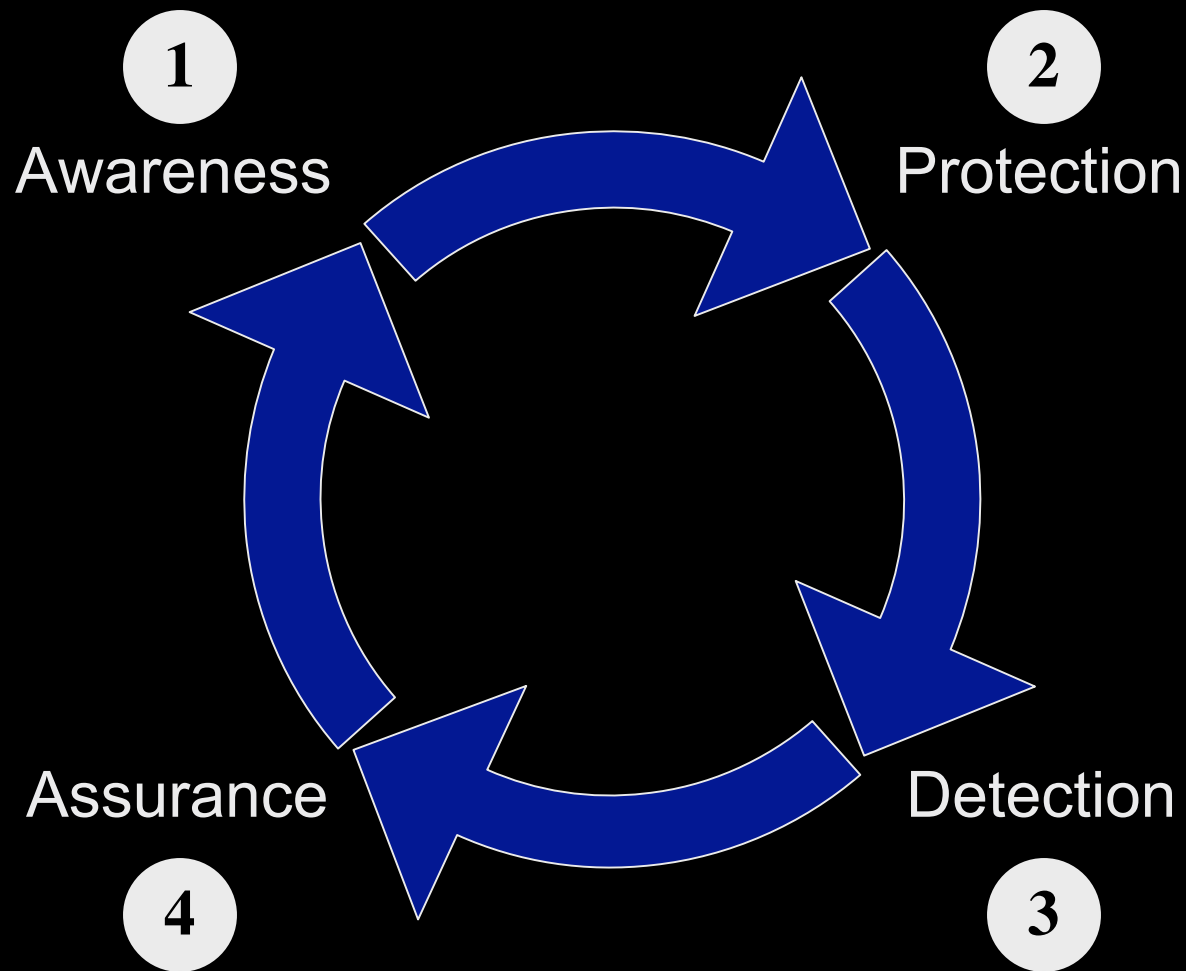
- Once a control is implemented, establish a maintenance life-cycle to regularly re-evaluate the effectiveness of the controls to ensure they meet the level of acceptable risk.
- Implement change control and regular audit processes to verify when an aspect of the risk-control balance has changed.



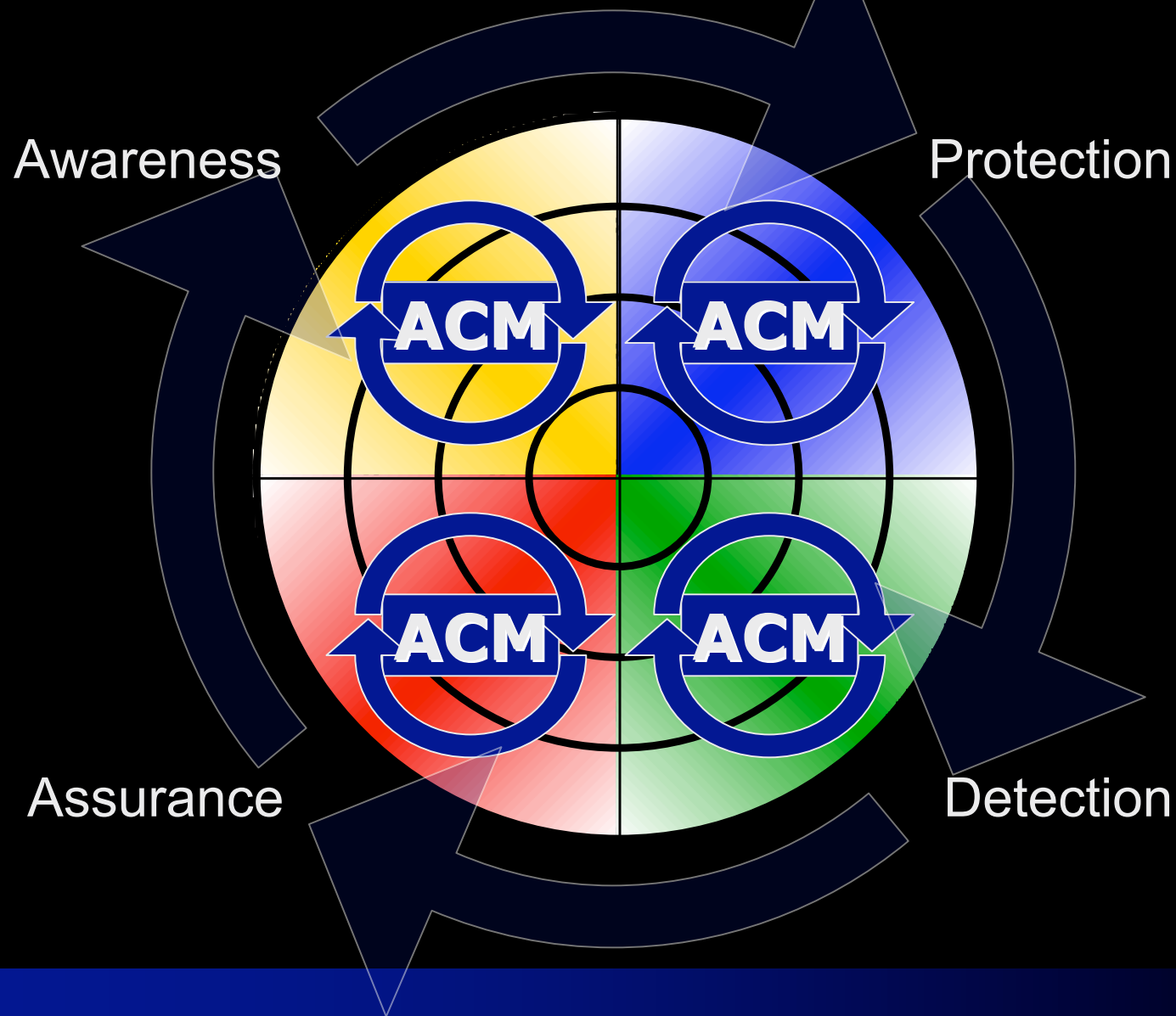
FoRMA Overview



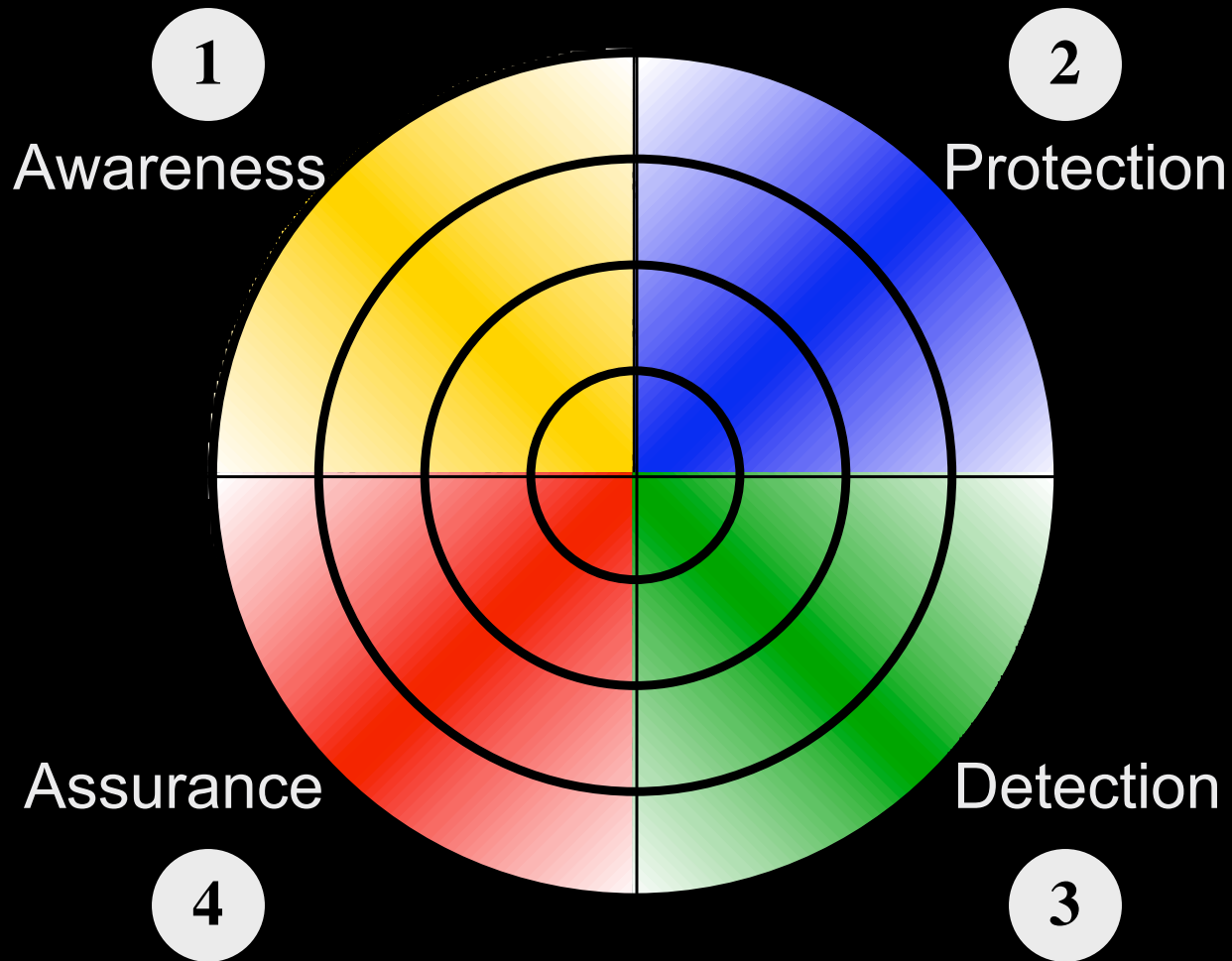
Implementation: Phases



FoRMA Process: Phases & RM Cycle

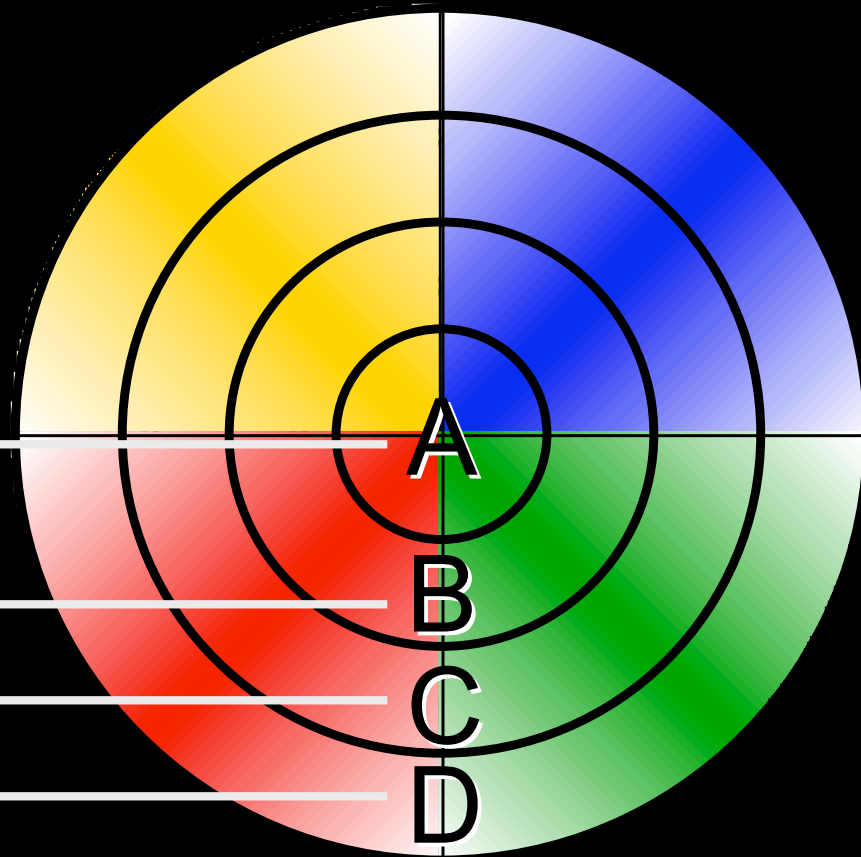


Overview of elements, Quadrants

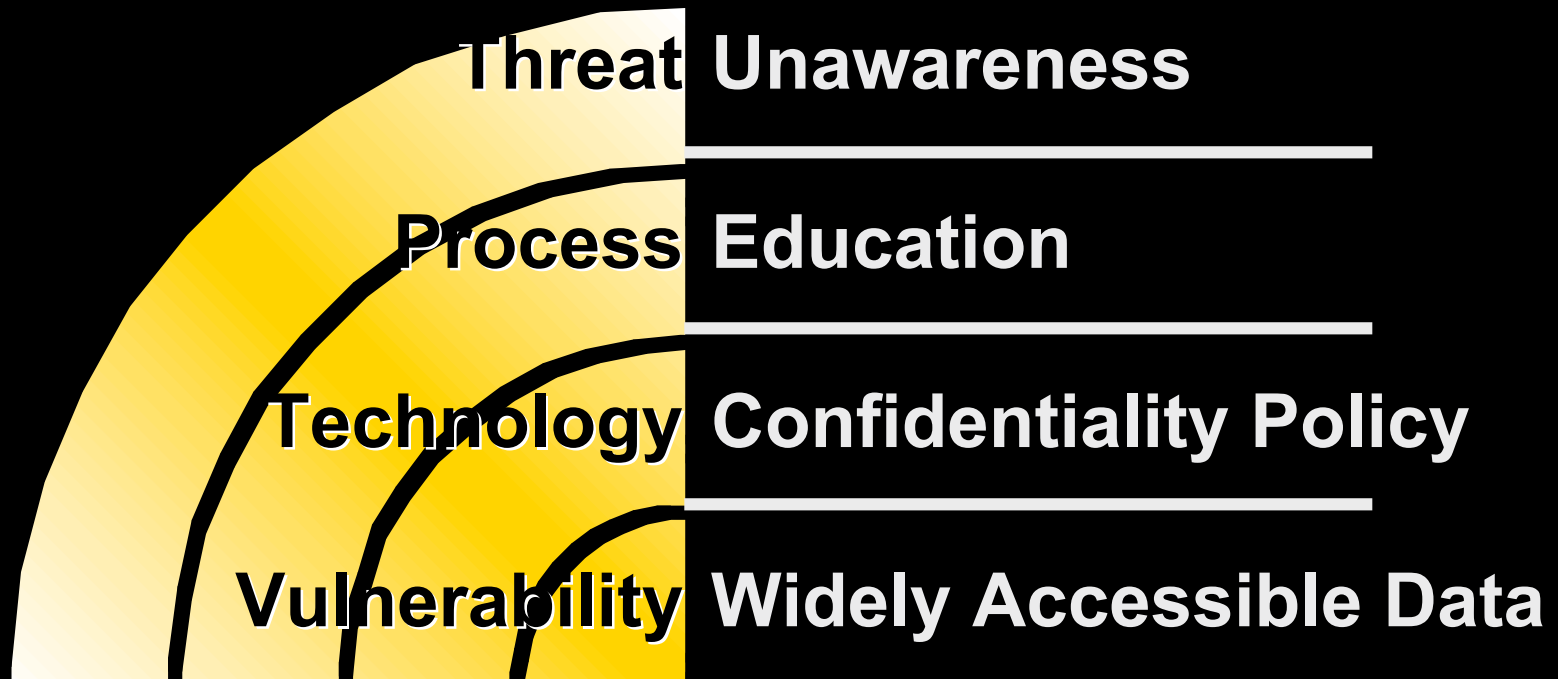


Overview of elements, Rings

- Vulnerabilities **Of Assets & Resources**
- Technology
- Process
- Threats



Quadrant 1, Awareness example



Quadrant 2, Protection example

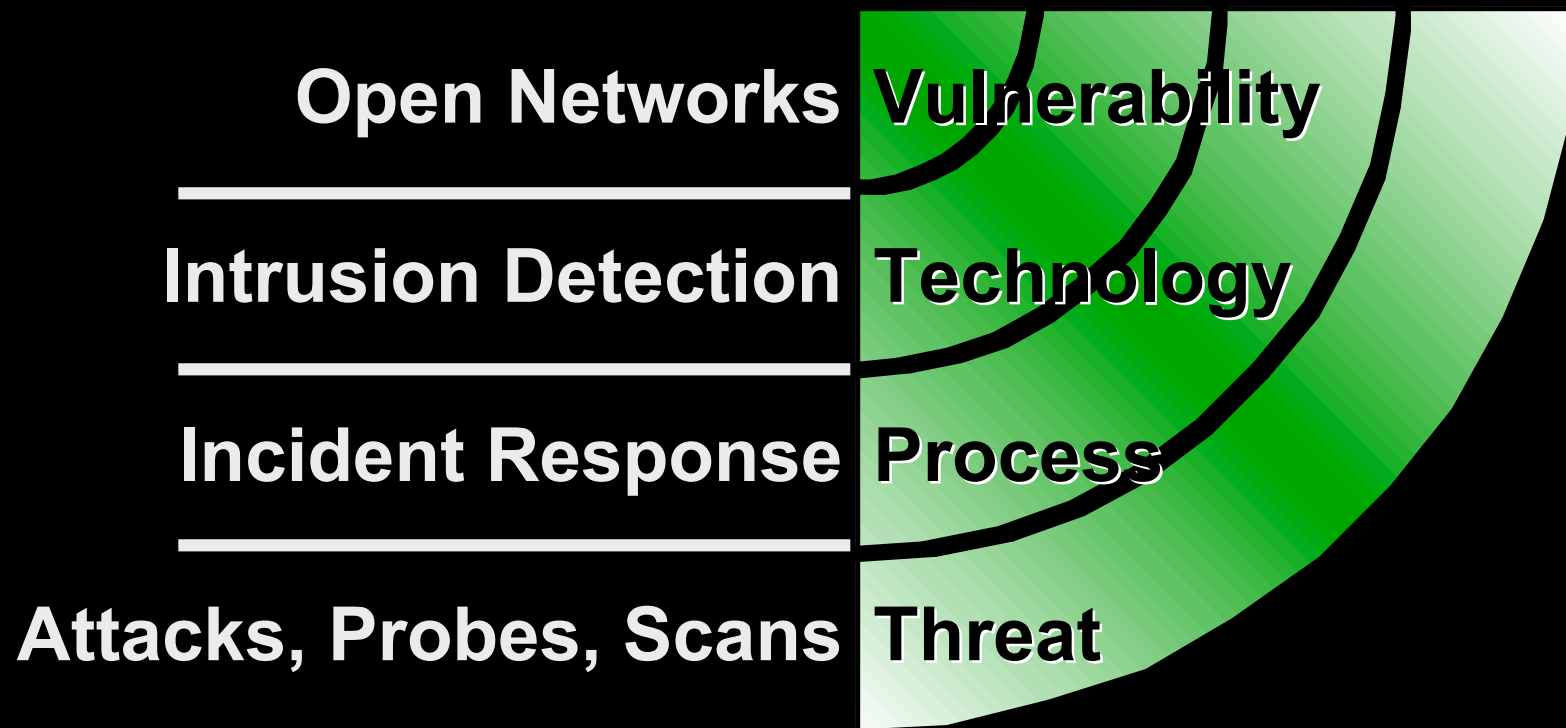
Hack Default Exploits **Threat**

Reinforce Process **Process**

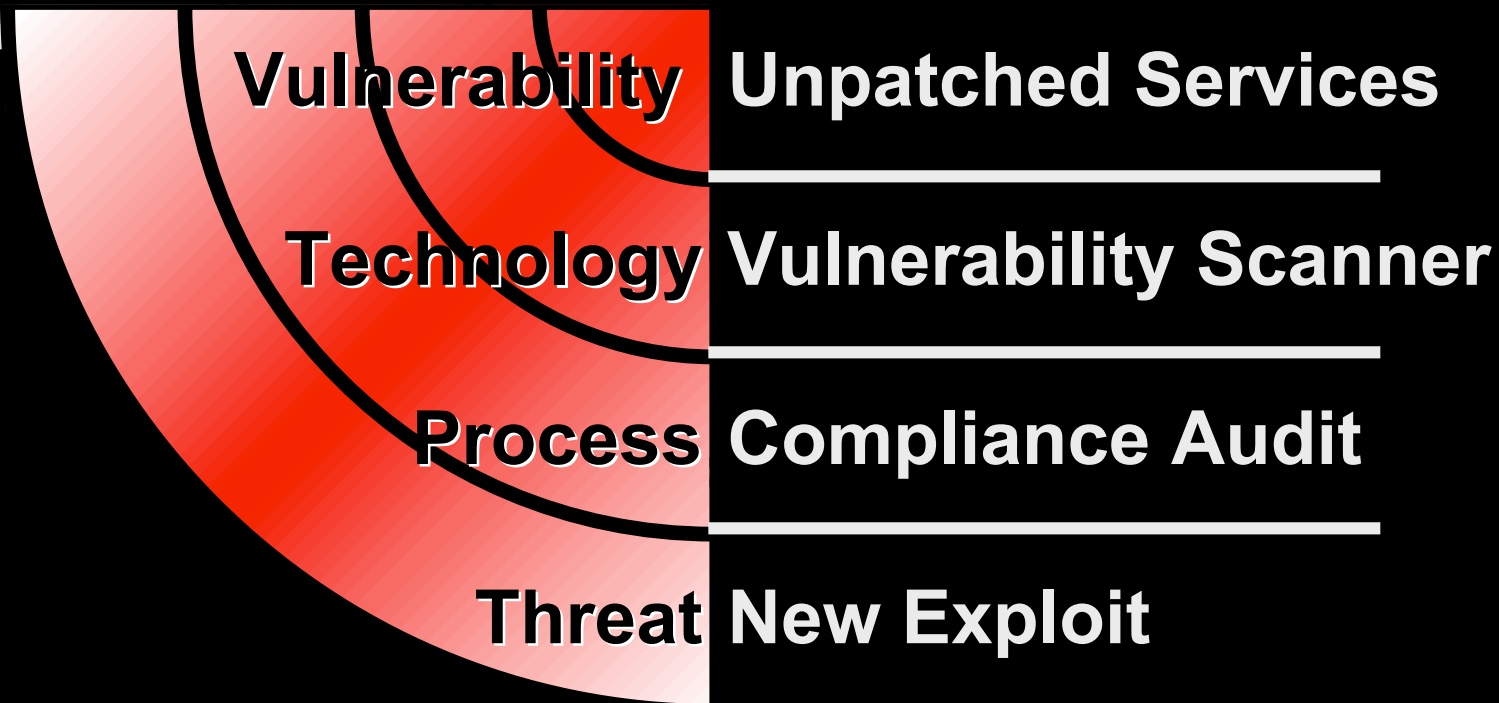
Harden Technology **Technology**

Unpatched Systems **Vulnerability**

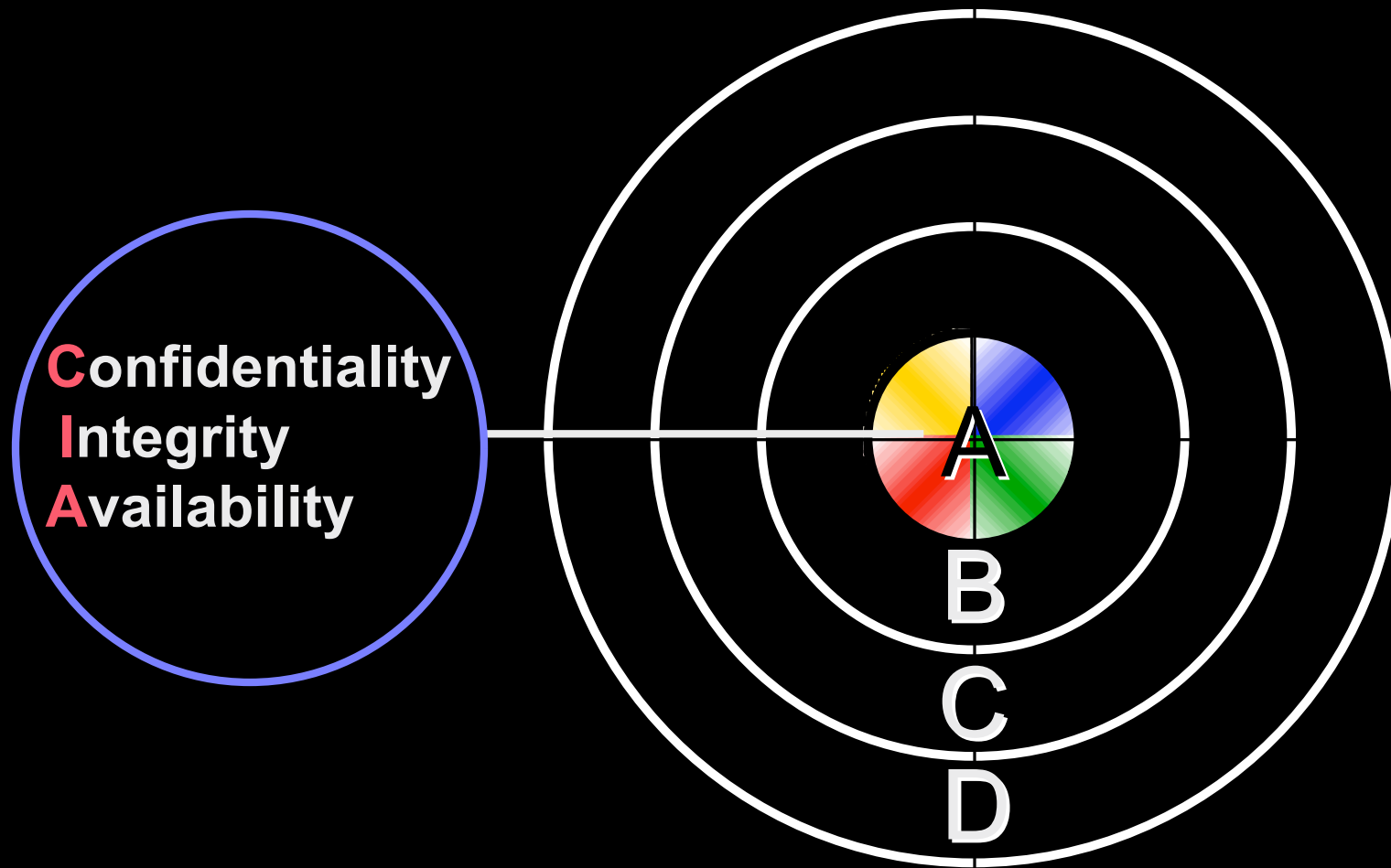
Quadrant 3, Detection example



Quadrant 4, Assurance example



Ring A, Vulnerability Mgmt Model



Confidentiality
Integrity
Availability

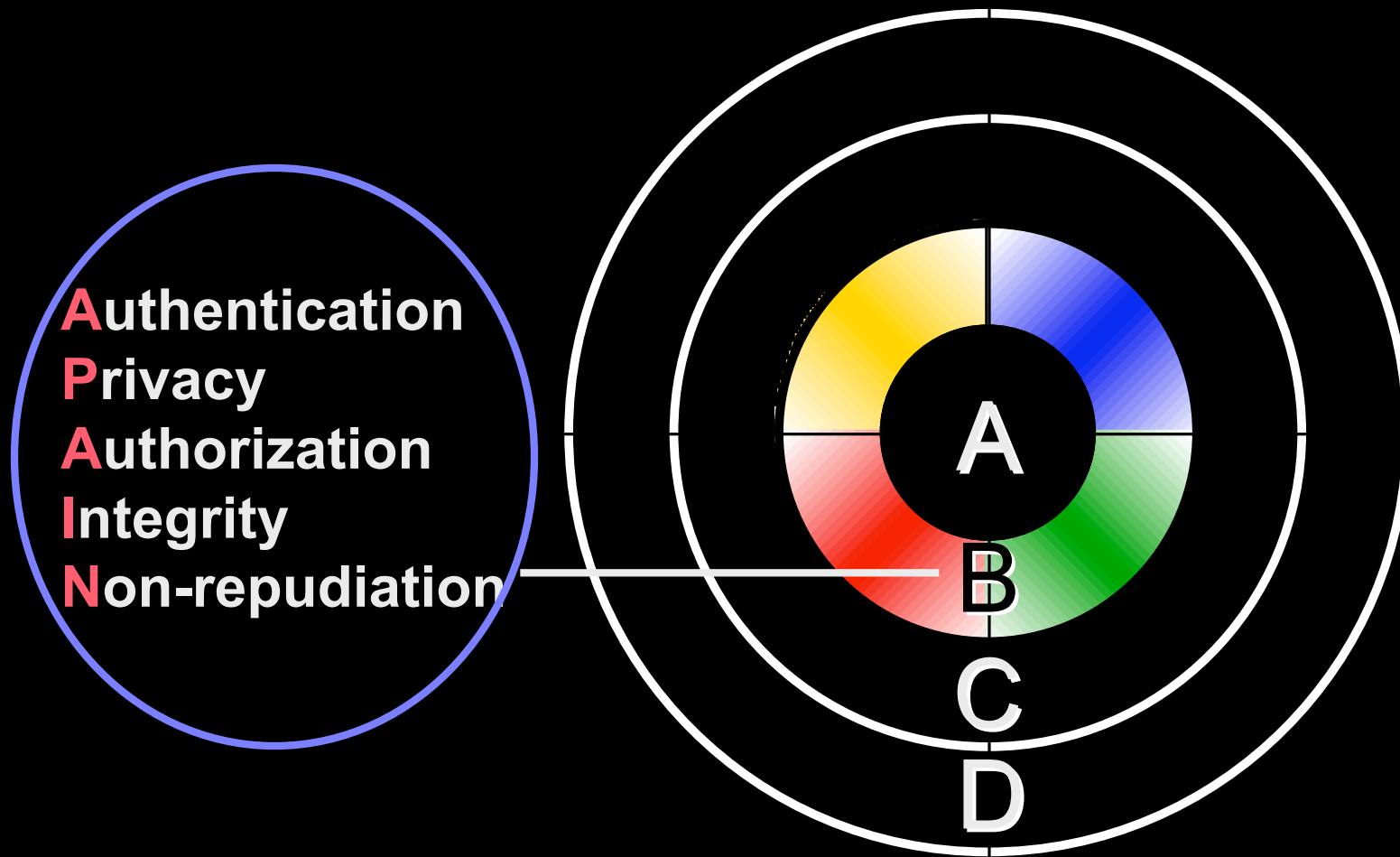
A

B

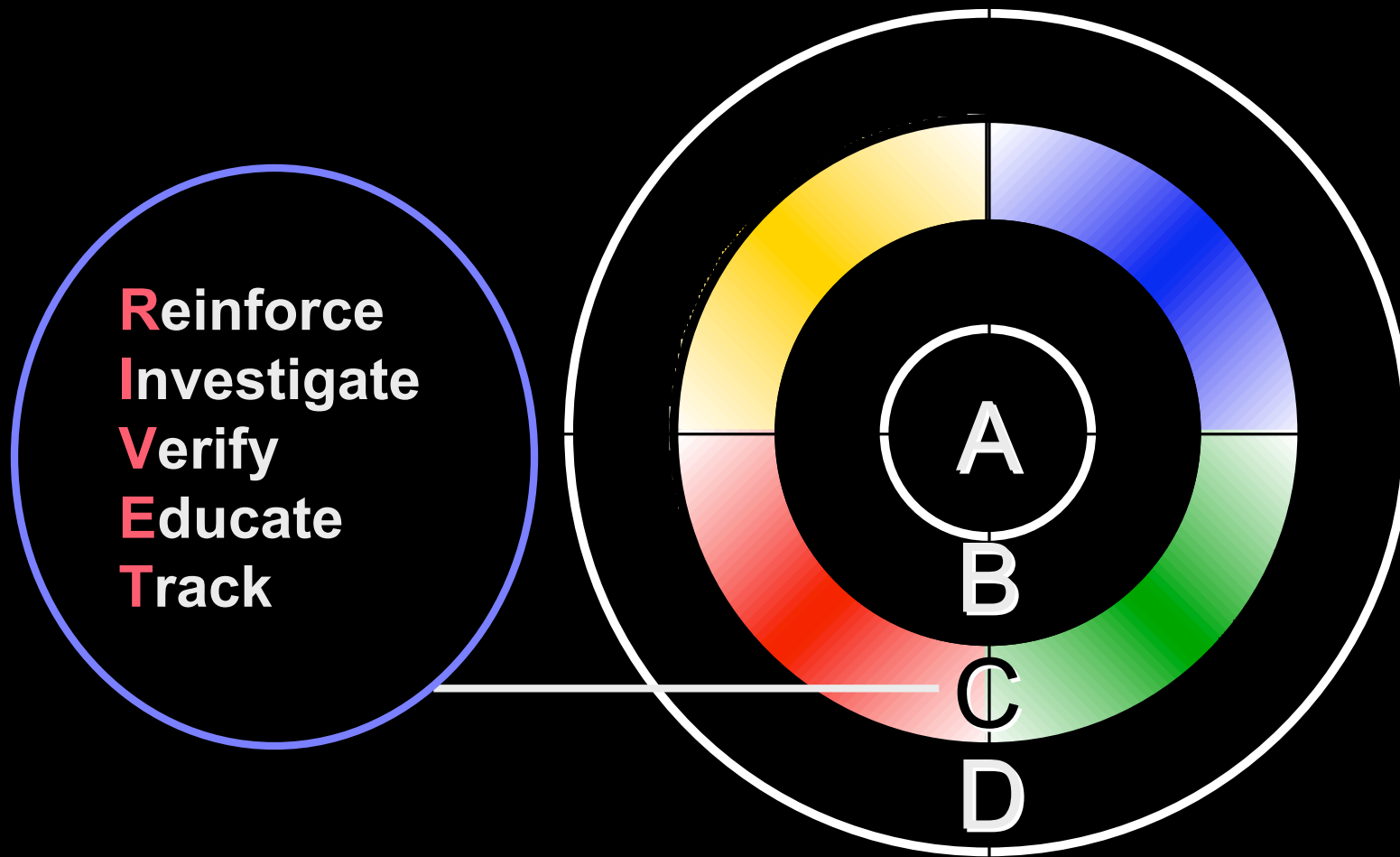
C

D

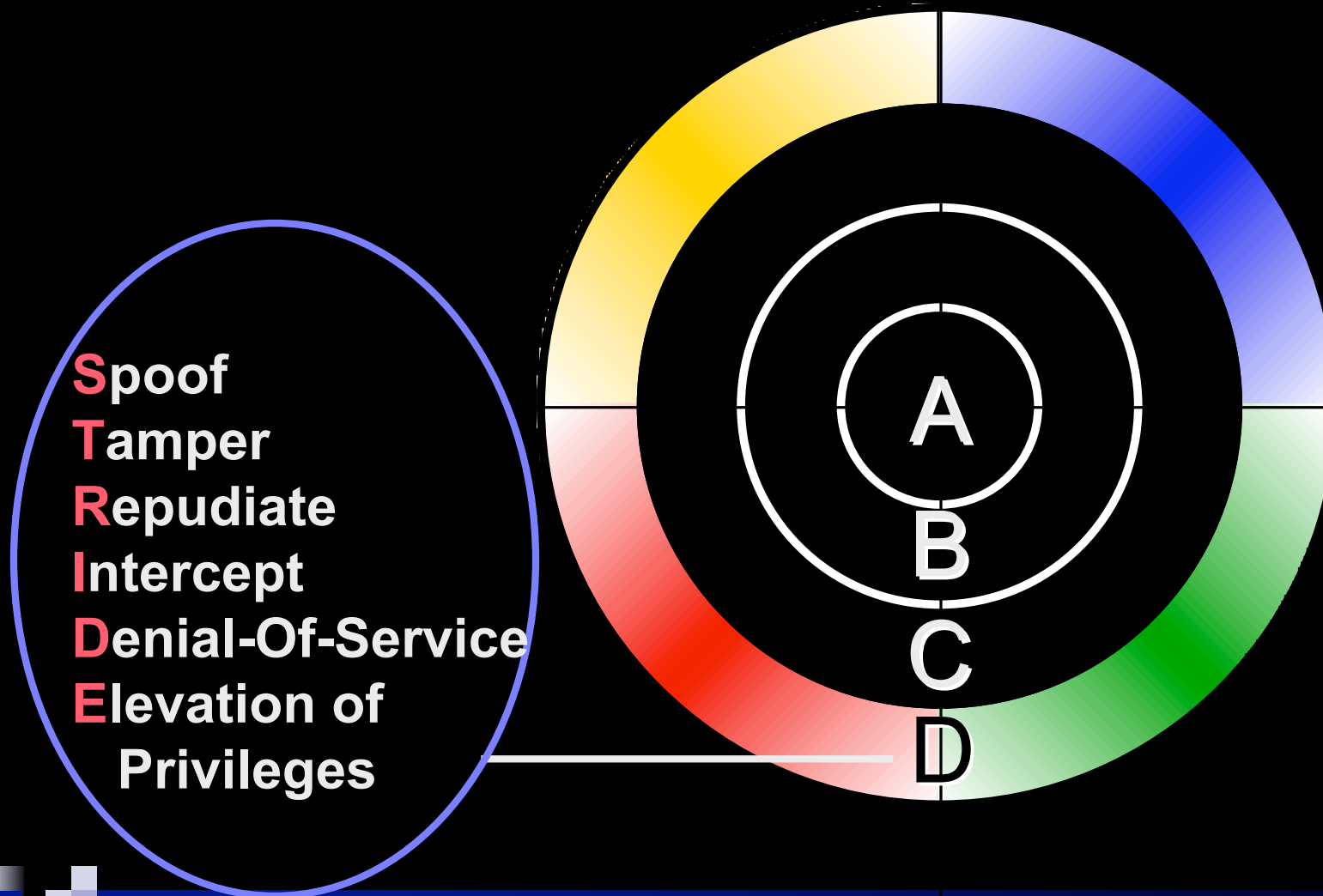
Ring B, Security Technology Model



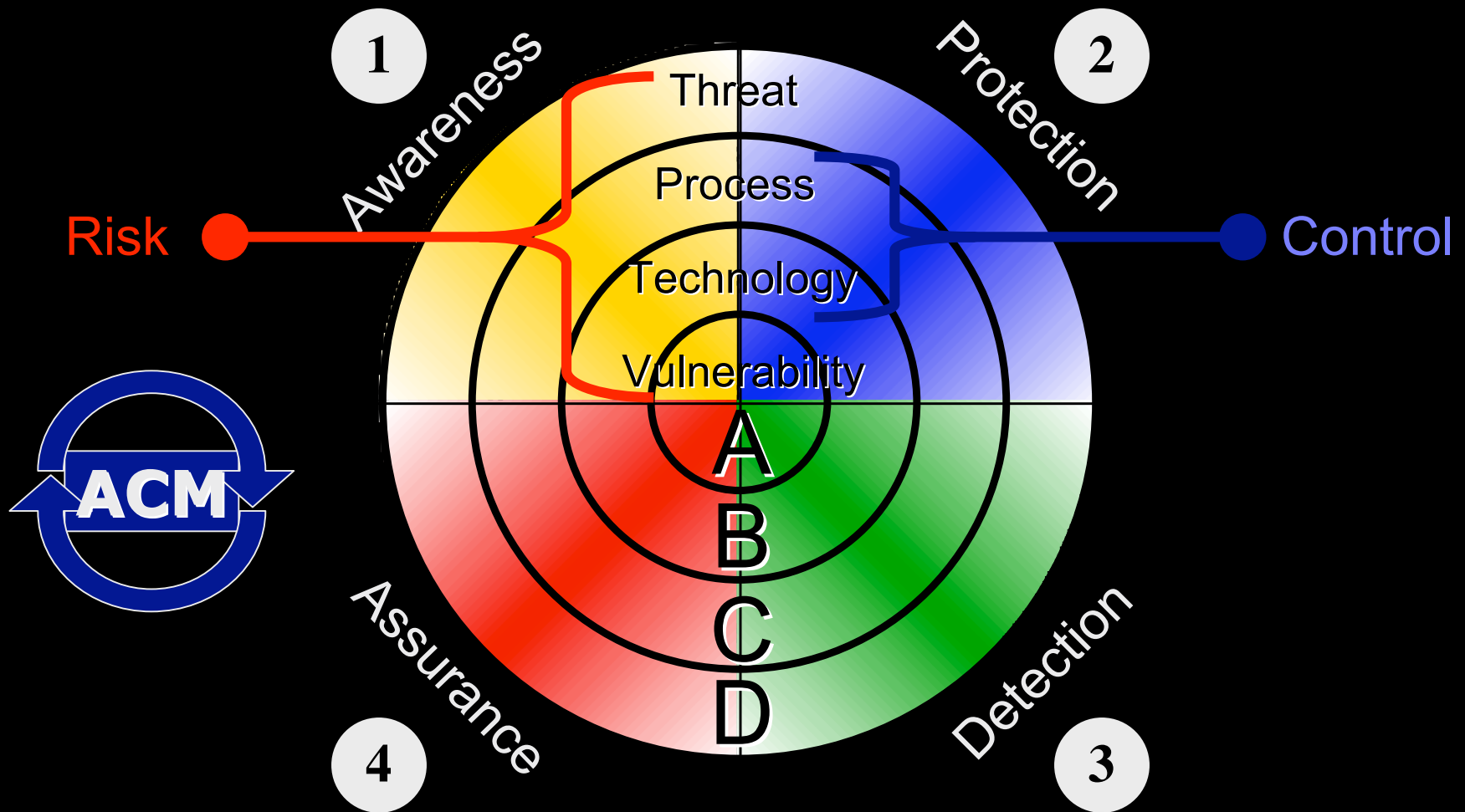
Ring C, Security Process Model



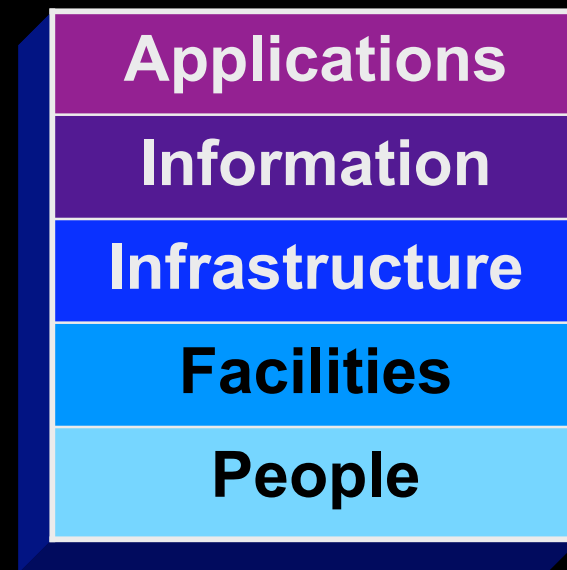
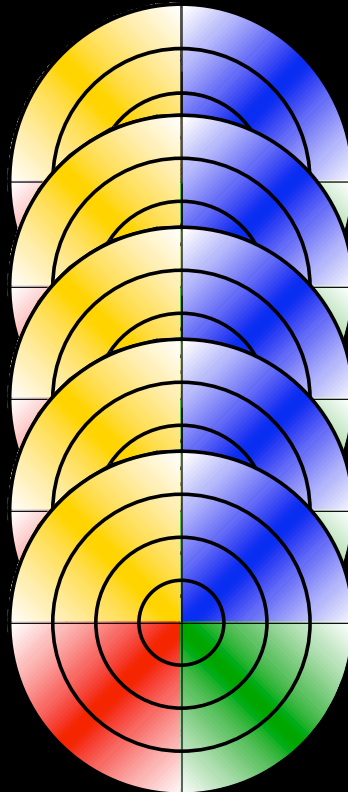
Ring D, Threat Management Model



FoRMA Overview



Applied to the 5 Layer model*



*: See references at the end of the presentation material

Results

- Applying the FoRMA model to your current environment will provide a security benefit in the following areas:
 - **Successful Vision & Strategy**
 - **Balanced Technology & Operations**
 - **Performing Security Gap Analysis & Audits**
 - **Demonstrating Reduced and Acceptable Risk**
 - **Trouble Shooting Security Process problems**

Wrap-Up, Lessons Learned

- Use FoRMA to help make decisions on what controls to implement to mitigate the risk
- It is more important to raise the level of control than to impact the business objectives
- Clearly understand your Risk Acceptance Gaps
- Establish controls that are primarily process-based, assisted with technology
- Regularly review your risk and control levels
- Use FoRMA to identify the controls necessary to support the long term business strategy

Questions?

- Feedback & Comments are welcome.
- Contact information:
 - **Kris.Kahn@mac.com**
 - **831-419-1256**

References (*)

- **Control Objectives for IT and Related Technology (COBIT)** trademarked by the IT Governance Institute (ITGI)
- **Open System Interconnection (OSI) reference model** was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered the primary architectural model for intercomputer communications.
- **STRIDE** Threat Model, conceived, built upon, and evangelized at Microsoft by Loren Hohnfelder, Praerit Garg, Jason Garms, and Michael Howard. Explained further in “Writing Secure Code, 2nd Ed” (ISBN 0-7356-1722-8), pages 83-86.
- **CIA Security Model**, author unknown, taught as part of the Common Body of Knowledge for CISSP curriculum.
- **APAIN** Acronym for Security Architecture, developed by Curtis Coleman in 2001.
- **RIVET** Acronym for Security Management, developed by Kris Kahn 2004.
- **Failure Mode and Effects Analysis (FMEA)** evolved as a process tool used by the United States military as early as 1949 and is currently part of the SixSigma curriculum.
- **Capability Maturity Model (CMM)** is a trademark of Carnegie Mellon University.