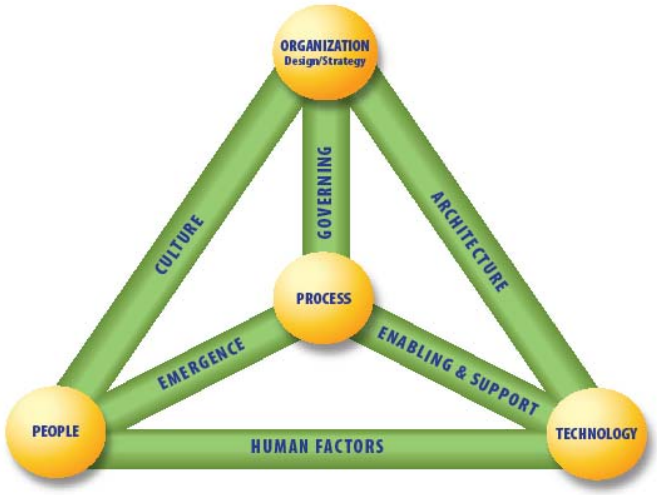
A Business Model for Information Security



© 2009, ISACA. All Rights Reserved.

Session Goals



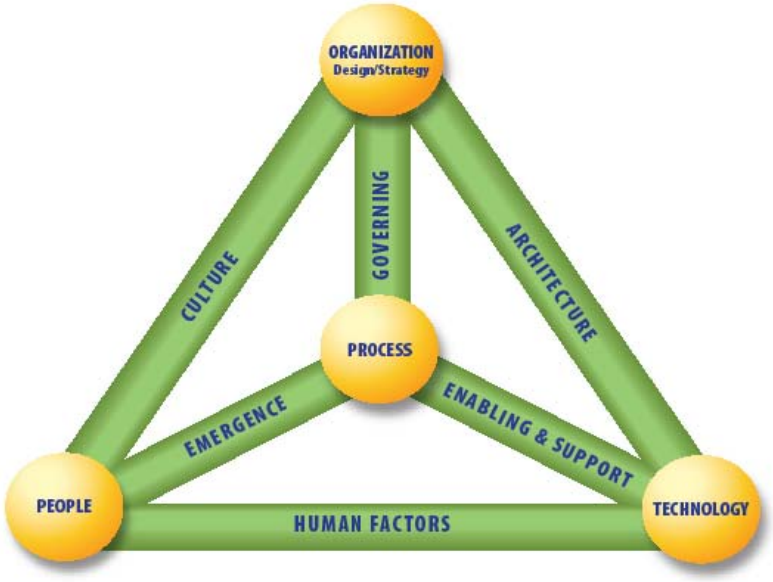
- Consider the business challenges that organizational leaders and security managers need to confront
- Evaluate traditional approaches and Models used to address these challenges
- Introduce systemic thinking as a better way of thinking about information protection solutions
- Review the concepts contained within the Business Model for Information Security Management as a suitable solution
- Have a mutually beneficial exchange of ideas

ISACA® Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

Business Model for Information Security

The Business Model for Information Security was developed to address the complexity of security. It is a business orientated Model that promotes a balance between protection and business.



Elements

- Organization Design and Strategy
- People
- Process
- Technology

Dynamic Interconnections

- Culture
- Architecture
- Governing
- Emergence
- Enabling and Support
- Human Factors

ISACA Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

Why is a Model Required?



Most significant challenges confronting information security managers

- Senior Management commitment to information security initiatives
- Management understanding of information security issues
- Information security planning prior to implementation of new technologies
- Integration between business and information security
- Alignment of information security with the organization's objectives
- Executive and line management ownership and accountability for implementing, monitoring, and reporting on information security

Source: Critical Elements of Information Security Program Success, ISACA, 2005

ISACA Serving IT Governance Professionals 40th Anniversary

© 2009, ISACA. All Rights Reserved.

Challenges



- Information security problems are complex and involve multiple parties
- Many problems appear not to have been solved regardless of past actions taken
- Cause and effect thinking is not effective
- Continuous fire fighting mode results in little time for innovation
- Organization silos reduce opportunities for strategic solutions
- Over-reliance on technology to solve problems

ISACA Serving IT Governance Professionals 40 Anniversary

© 2009, ISACA. All Rights Reserved.

Thinking About Information Security



Security must be understood as a quality improvement process in an organization, aiming at continuous improvement of organizational performance

Security is a chain with many weak links. The dynamics of security is crucial: Compliance erodes, vulnerabilities develop, risk perceptions change, time delays and misperceptions fool people. The interplay of human behaviour, organizational aspects, technology, tasks and environment in security settings is necessarily a system characterized by feedback, temporal change (nonlinear dynamics), time delays, soft factors, and interdisciplinary aspects. Clearly, the ultimate practical reason for studying such systems is to achieve desired goals and to prevent undesired performance. In other words, security systems need to be managed. All this makes **System Dynamics** a promising methodology to confront the many outstanding and ever growing challenges in security.

Dr Jose Gonzalez

Agder University College
Faculty of Engineering and Science
Security and Quality in Organizations
Grooseveien 36
NO-4876 Grimstad
Norway

ISACA Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

Information Security Program Models



An information security program model should:

- Clearly articulate what is part of a security program and what is not
- Provide a means for understanding how components of a program function
- Predict the end result that will be achieved when change is introduced
- Enhance communications among individuals and groups who provide or benefit from information security program activities

Existing security models while valuable do not answer each of these criteria.

ISACA® Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.



Existing Information Security Models

© 2009, ISACA. All Rights Reserved.

Traditional Information Security Models



- Bell-La Padula - state machine model for access control
- Clark-Wilson - integrity model
- Graham – Denning Model - creation and deletion of objects
- Take – Grant Protection Model - system safety
- Brewer and Nash Model - controls to mitigate conflict of interest
- Harrison, Ruzzo, Ullman Model – integrity of access rights
- ISM3

© 2009, ISACA. All Rights Reserved.

Traditional Information Security Models



- Pros
  - ✓ Allow for access control
  - ✓ Provide guidance for defense in depth solutions
  - ✓ May assist with compliance
  - ✓ Provide a tool to manage situational security
- Cons
  - ✓ Static in nature
  - ✓ Process oriented
  - ✓ Not risk based
  - ✓ Do not consider external factors
  - ✓ Do not consider culture
  - ✓ Do not plan for unpredictable situations

ISACA® 40th ANNIVERSARY SINCE 1969
Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

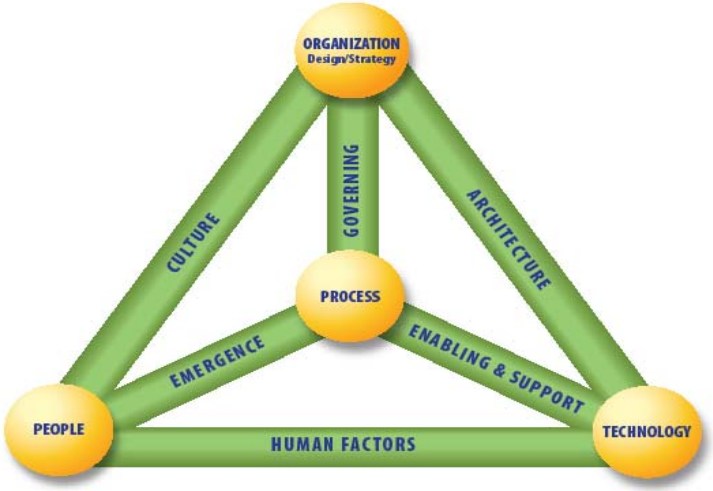
The Business Model for Information Security

© 2009, ISACA. All Rights Reserved.

Business Model for Information Security

BMIS was developed to address the complexity of security.

It is a business orientated Model that promotes a balance between protection and business.



Elements

- Organization Design and Strategy
- People
- Process
- Technology

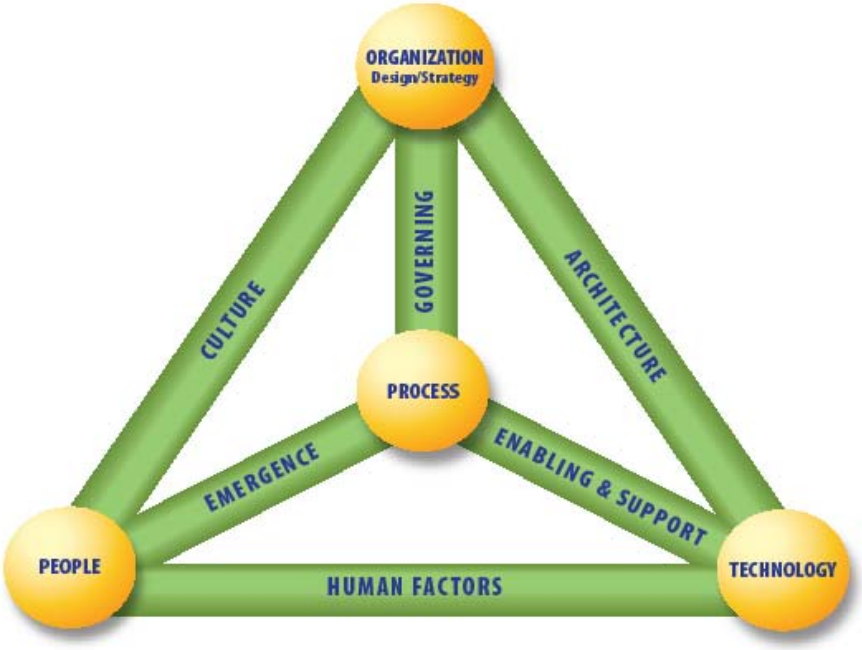
Dynamic Interconnections

- Culture
- Architecture
- Governing
- Emergence
- Enabling and Support
- Human Factors

ISACA Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

Core Concept



BMIS can be viewed as a three dimensional Model best visualized as a pyramid. All aspects of the Model interact with each other. If any one part of the Model is changed, not addressed, or managed inappropriately, it will distort the balance of the Model.

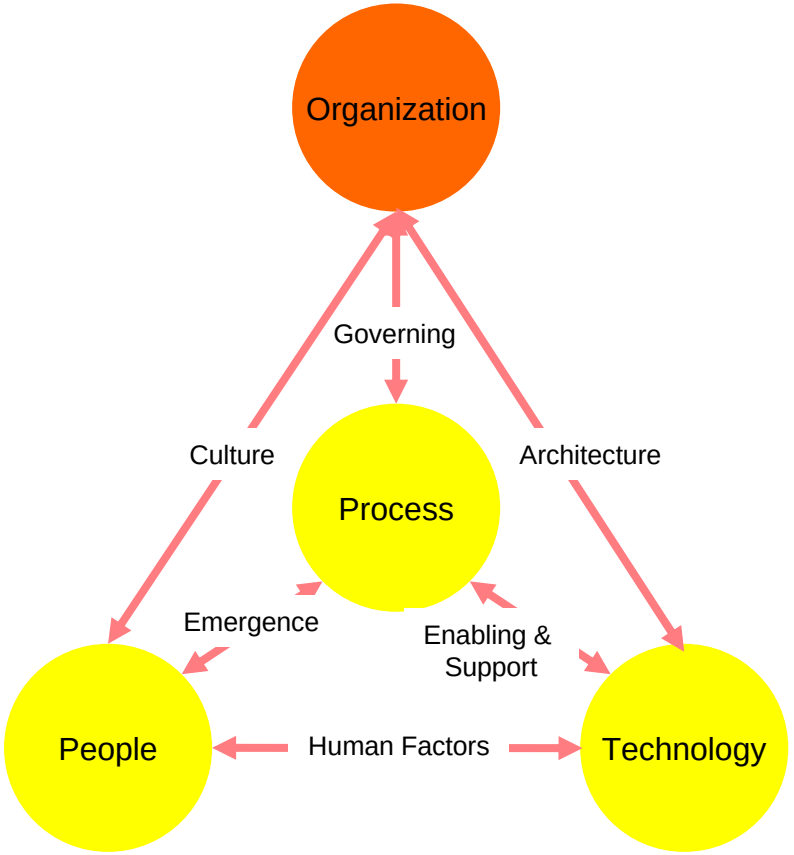
ISACA
Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

Organization Design & Strategy Element



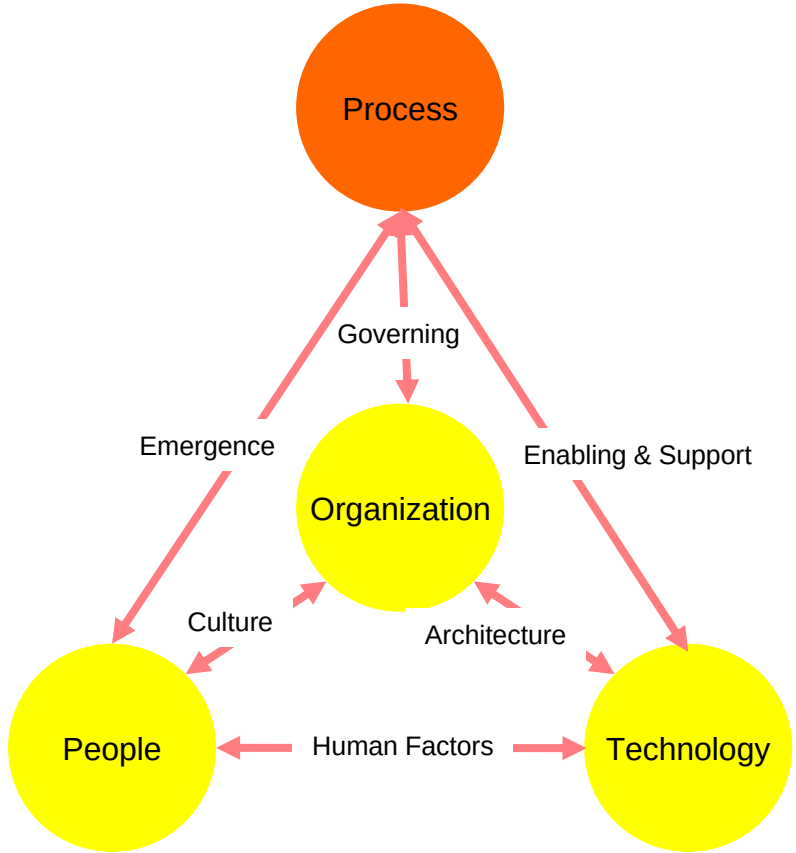
- Organization is a network of people interacting with each other. It contains interactions between people and things. It drives culture governance and architecture. Security as a component needs to map to the larger organization
- Strategy specifies the goals and objectives to be achieved as well as the values and missions to be pursued. It is the organizations formula for success and sets the basic direction.
- Design relates to the formal organization structure and reporting relationships



© 2009, ISACA. All Rights Reserved.

Process Element

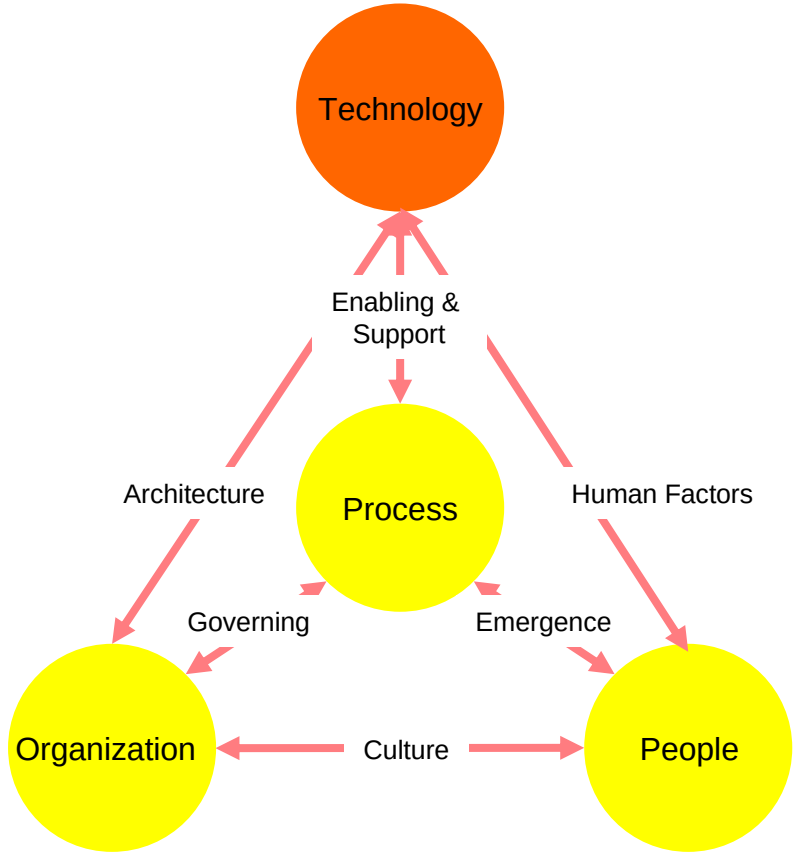
- Includes formal and informal mechanisms to get things done
- Provides vital link to all of the dynamic interconnections
- Process is designed to identify, measure, manage, and control risk, availability, integrity and confidentiality, and to ensure accountability



ISACA
Serving IT Governance Professionals
© 2009, ISACA. All Rights Reserved.

Technology Element

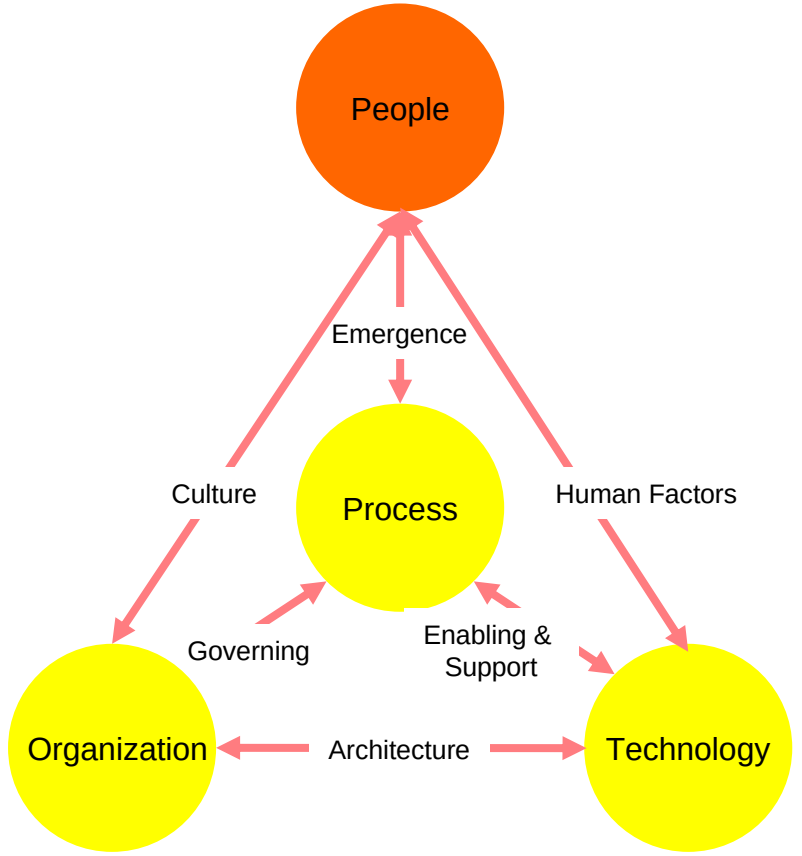
- Organization infrastructure
- Tools that make processes more efficient.
- Used to accomplish an organization's mission
- Part of an organization's infrastructure
- Can be considered a band-aid for security issues



© 2009, ISACA. All Rights Reserved.

People Element

- Represents the human resources and the security issues that surround them
- Collective of human actors including values and behaviors
- All whose efforts must be coordinated to accomplish the goals of the organization
- Not just units of “one” since each individual comes with all their experiences, values

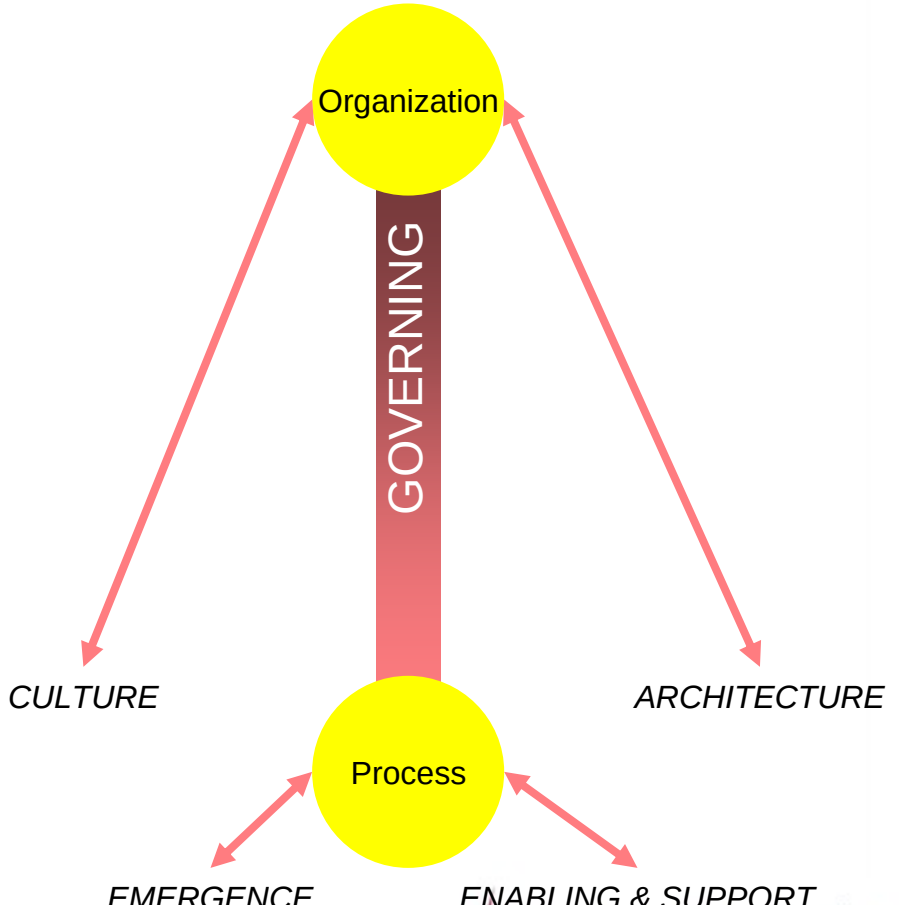


Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

Governing Dynamic Interconnection

- Steering the organization
- Responsibility of Board and C-Suite
- Demands strategic leadership, responsibility and accountability
- Sets limits within which an organization operates and is implemented within processes to monitor performance and achieve compliance while also providing adaptability to emergent conditions

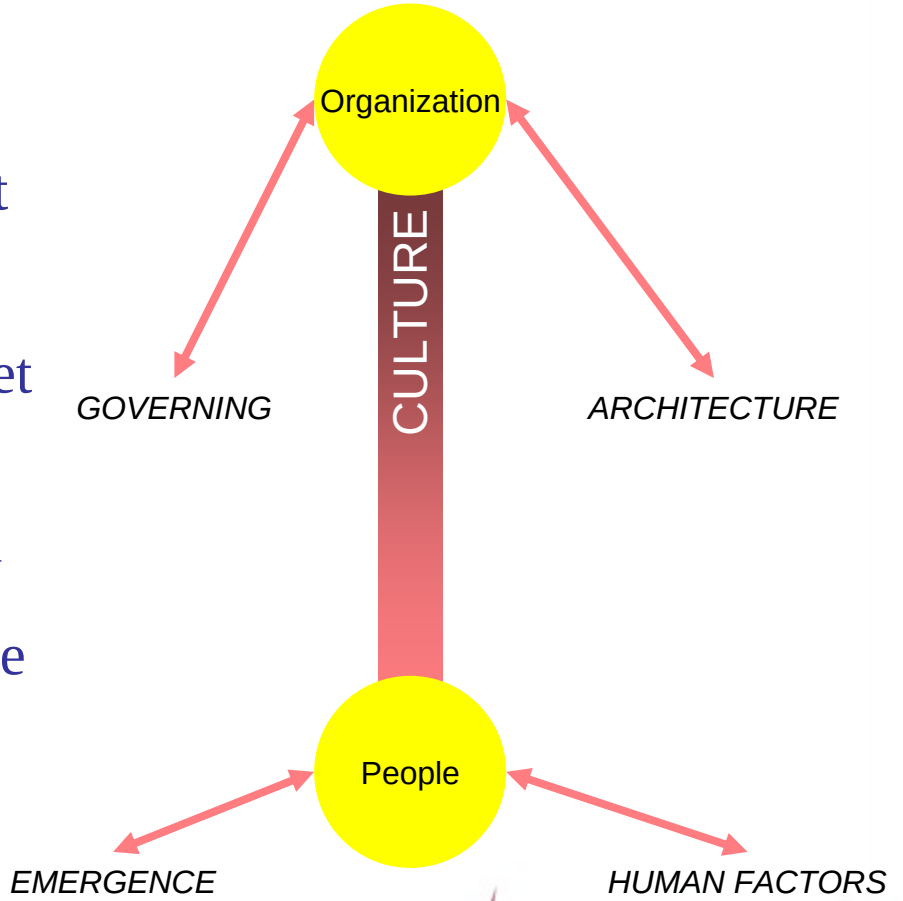


ISACA
Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

Culture Dynamic Interconnection

- Culture is a pattern of behavior, beliefs, assumptions, attitudes, and ways of doing things.
- Culture is emergent. It is learned. It creates a sense of comfort
- Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses. The responses become a set of expected and shared behaviors. These behaviors become unwritten rules which become the norms that are shared by all people who have that common history.



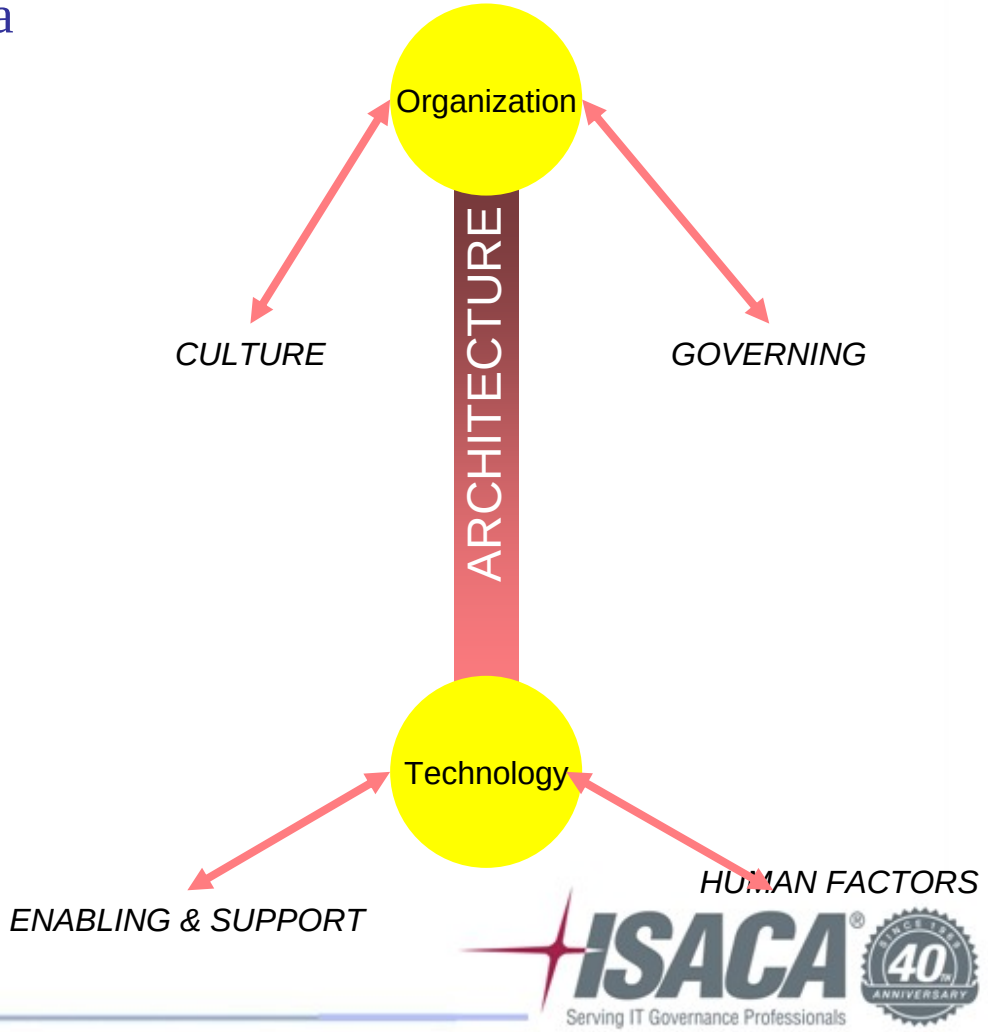
ISACA
Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

Architecture Dynamic Interconnection



- The overall design or structure of a system typically described as the interconnection of hardware, software, and components that make up the organizations infrastructure.
- **Complement to processes, policies and procedures that govern the practices**
- A security architecture is a representation of all the people, process, policies and technology that comprises an organizations security practices.



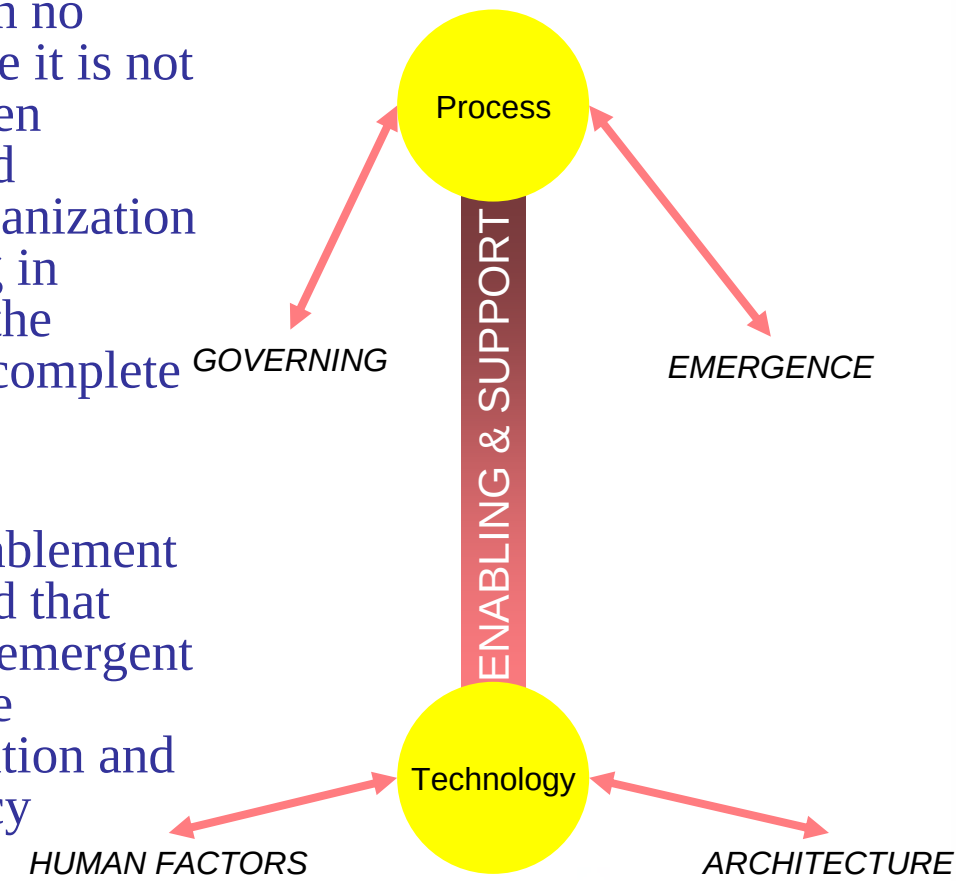
ISACA Serving IT Governance Professionals 40 ANNIVERSARY

© 2009, ISACA. All Rights Reserved.

Enabling and Support Dynamic Interconnection

A technology heavy organization with no supporting processes is at risk because it is not sustainable or extensible, and it is often disconnected from people, culture and processes. By the same token, an organization dominated by process may be lacking in supporting technology to implement the process and procedures necessary to complete an effective security system

To fully realize systemic security Enablement and Support approaches must be used that provide sufficient flexibility, even in emergent environments, that the tensions can be resolved at the point of process execution and without a need to resort to rigid policy statements or hierarchical review

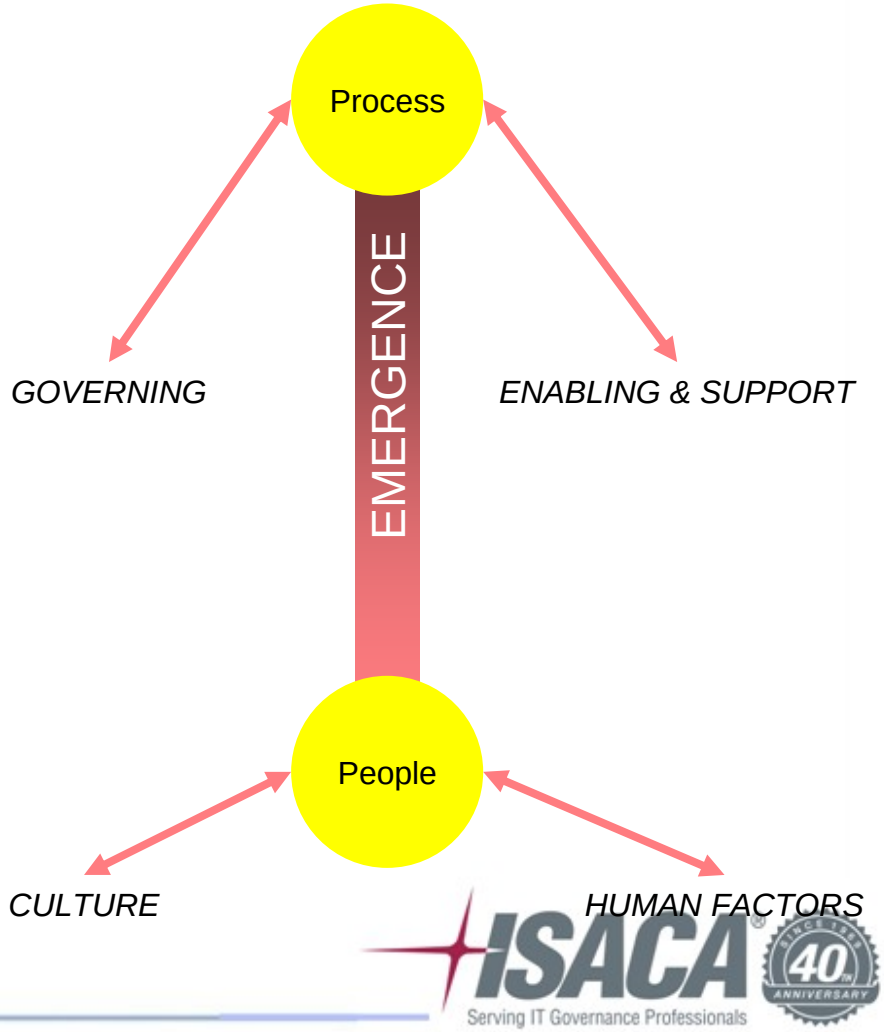


ISACA
Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

Emergence Dynamic Interconnection

- Developments and patterns that arise in the course of our enterprise which appear to have no obvious cause, and whose outcomes seem impossible to predict and control
- Dynamic process of patterns occurring over time that seem not to be created by a single entity, person, event, or rule but rather from the activity itself.
- There is nothing that commands a system to form a pattern, but instead the interactions of each part to its immediate surroundings causes a complexity which leads to order
- Emergence means surfacing, developing, growing, or evolving.

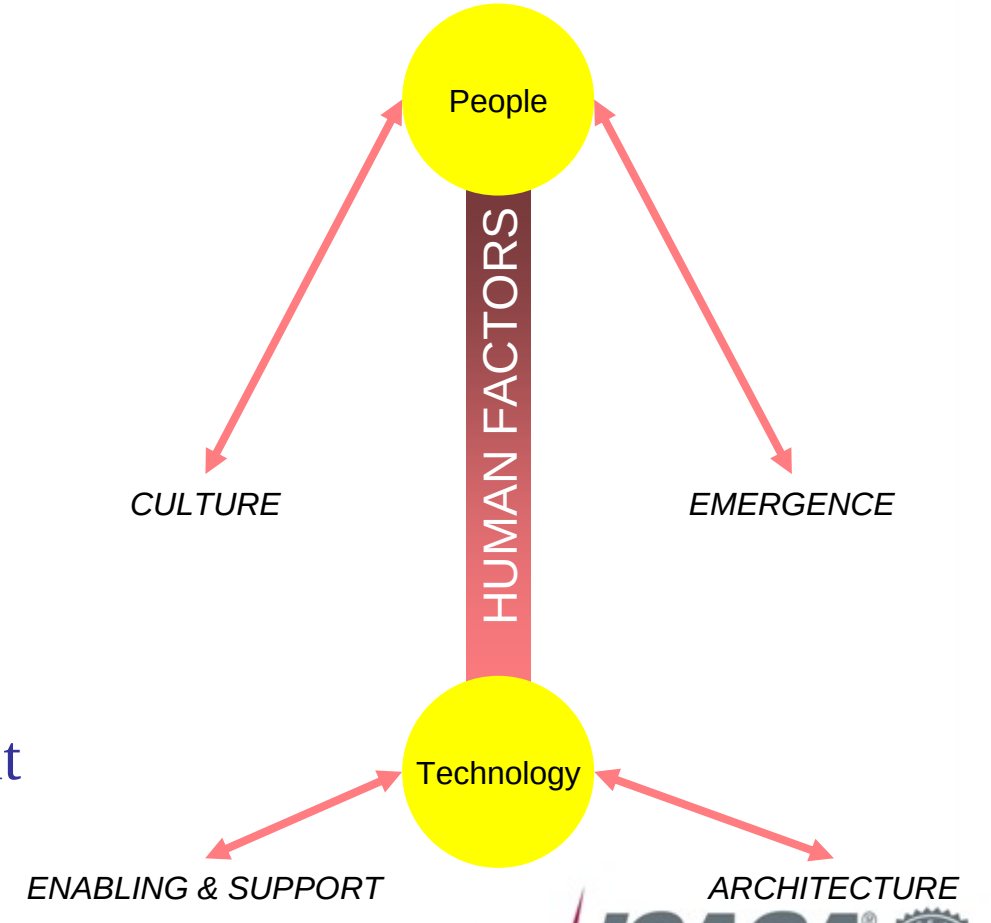


ISACA
Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

Human Factor Dynamic Interconnection

- Social properties unique to or characteristic of humans
- The way humans relate to the world around them
- Important for improving operational performance, safety and protection
- Does technology facilitate better security practices or does it make it more difficult for the people?



Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

How the Business Model for Information Security Works

© 2009, ISACA. All Rights Reserved.

Is a Systemic Approach Required?



- Are there too many variables to consider?
- Are collaboration efforts working?
- Is the strategic direction unclear?
- Can emergent opportunities be identified and captured?
- Are existing ways of dealing with issues working for all parties?
- Are relationships and process between different areas of the organization efficient and effective?
- Do external influences cause operational processes to change creating a sense of uncertainty?

ISACA Serving IT Governance Professionals 40th Anniversary

© 2009, ISACA. All Rights Reserved.

Systems Thinking Is



- A conceptual framework, a body of knowledge, and tools that are used to make full patterns clearer and help us see how to effectively manage change
- A discipline for seeing wholes and inter-relationships rather than static snapshots
- A discipline for seeing the structures that underlie complex situations and for discerning high from low leverage change

Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.

The Systemic Approach



- The systemic approach is relational. Relationships between actors are crucial
- View towards the interaction among components of systems rather than individuals
- Organization resources combine and interact in an order intrinsic to the purpose and objectives to be delivered and must be managed as such
- The systemic view is orientated towards the long term
- Systems tend to preserve themselves so actors tend to become accustomed to habits

ISACA Serving IT Governance Professionals 40 ANNIVERSARY

© 2009, ISACA. All Rights Reserved.

Problem Analysis



- Traditional approach to break down complex tasks into manageable subjects takes away our intrinsic connection to the larger whole
- Problem resolution can become an attempt to address obvious symptoms without identifying the underlying cause. This results in short term benefit and long term malaise.
- There is a need to find someone or something outside of ourselves to blame.
- We do not see how our actions extend beyond the boundary of our position. Our actions have consequences that appear to come from the outside when they return to hurt us.
- If we focus on events the best we can do is predict an event before it happens. We cannot create an environment where the event will not happen
- Either - Or thinking is a point in time correction and does not provide lasting improvement.

ISACA Serving IT Governance Professionals 40 ANNIVERSARY

© 2009, ISACA. All Rights Reserved.

Thinking About Problems



- Systems thinking is a discipline for seeing the structures that underlie complex situations
- The essence of systems thinking lies in seeing inter-relationships rather than linear cause-effect chains
- Reality is made up of circles but we see straight lines
- This thinking helps teams and individuals see beyond events and into the forces that shape change

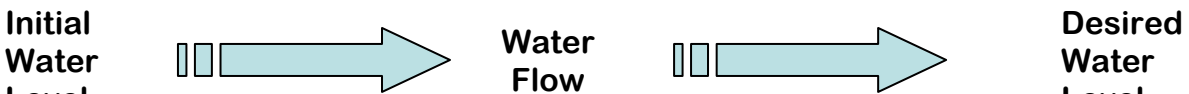
ISACA Serving IT Governance Professionals 40 ANNIVERSARY

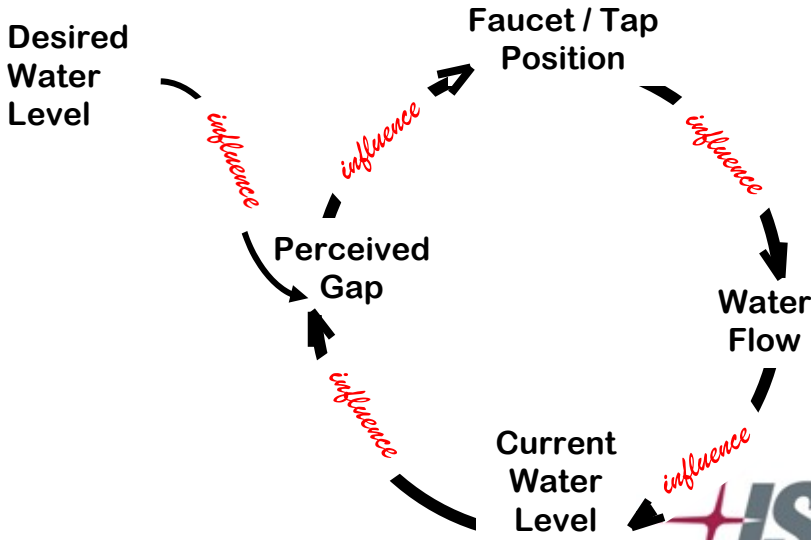
© 2009, ISACA. All Rights Reserved.

Linear vs. Circular Thinking









© 2009, ISACA. All Rights Reserved.

Understand the Whole Problem



- We push harder and harder on familiar solutions while the fundamental problem persists.
- The easy or familiar solution may be addictive and dangerous.
- Short term improvements can lead to long term dependency.
- There is an optimal rate of growth which is not ***Fast, Fast, Fast***. When growth becomes excessive the system will respond by slowing down.
- Seeing interrelationships underlying a problem leads to new insight.

© 2009, ISACA. All Rights Reserved.

Benefits of Systemic Thinking



- Create a better understanding of the big picture
- Obtain the greatest benefit from innovation efforts
- Make innovation more strategically useful and beneficial
- See the element (security) as part of the big picture
- Understand the feedback relationship between what is studied and other parts of the system
- Envision different environments so that change becomes indispensable. Creative Vision Statements essential to creating change.

ISACA Serving IT Governance Professionals 40 ANNIVERSARY

© 2009, ISACA. All Rights Reserved.

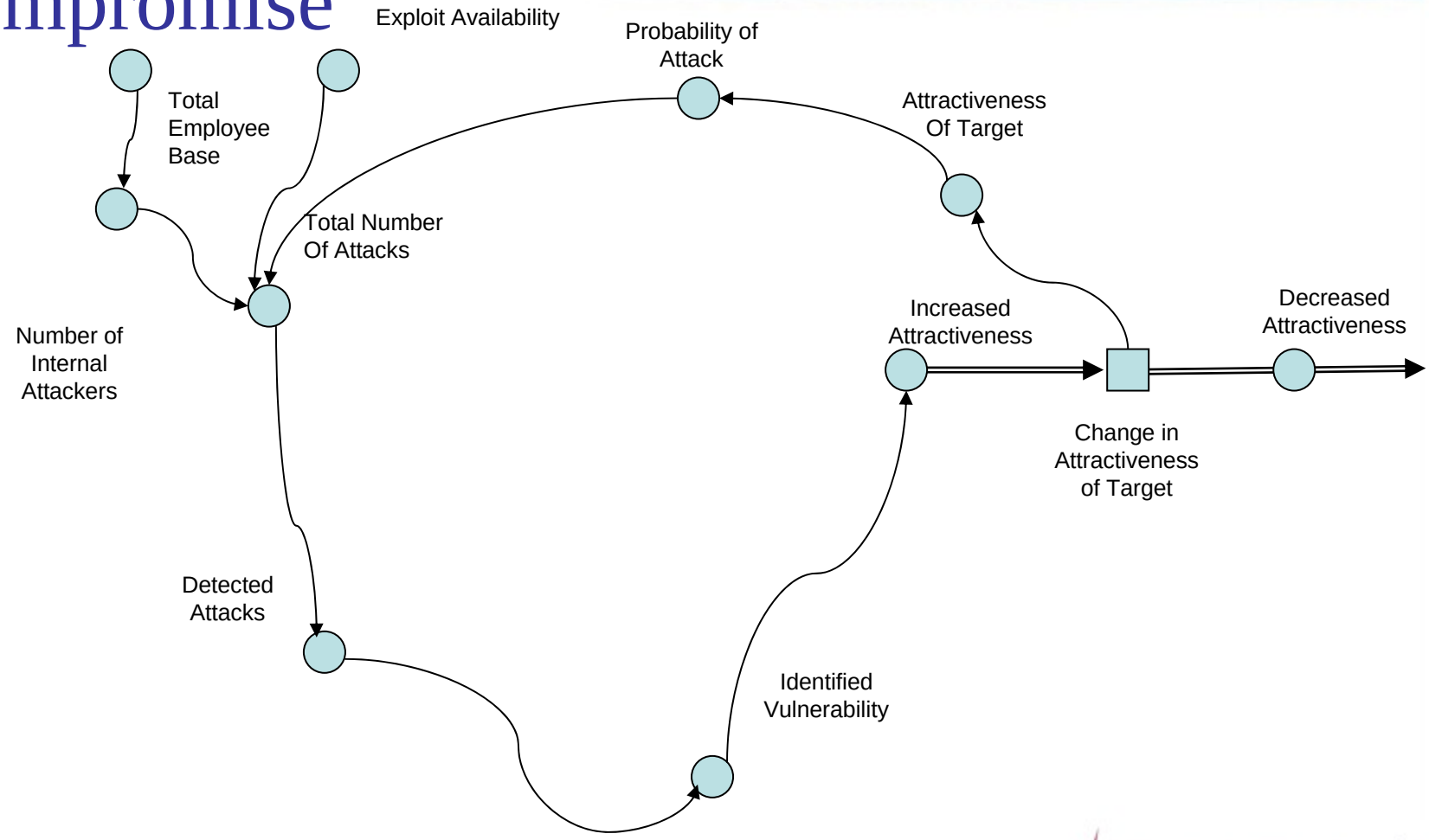
Systemic Models and Information Security

The Risk of Internal Compromise Example

© 2009, ISACA. All Rights Reserved.

System Dynamics Model – Internal Compromise

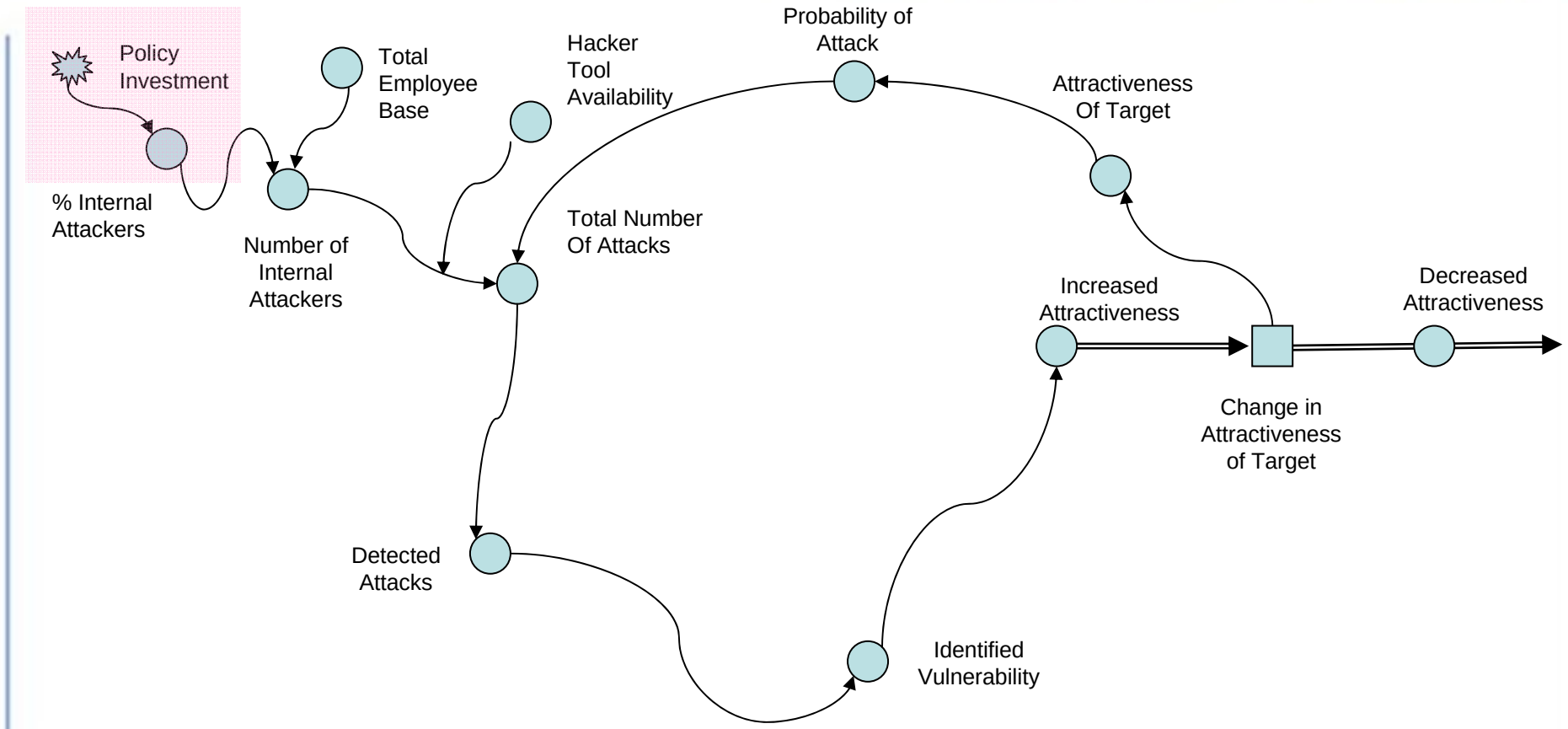




© 2009, ISACA. All Rights Reserved.

Internal Compromise - Add Security Policy



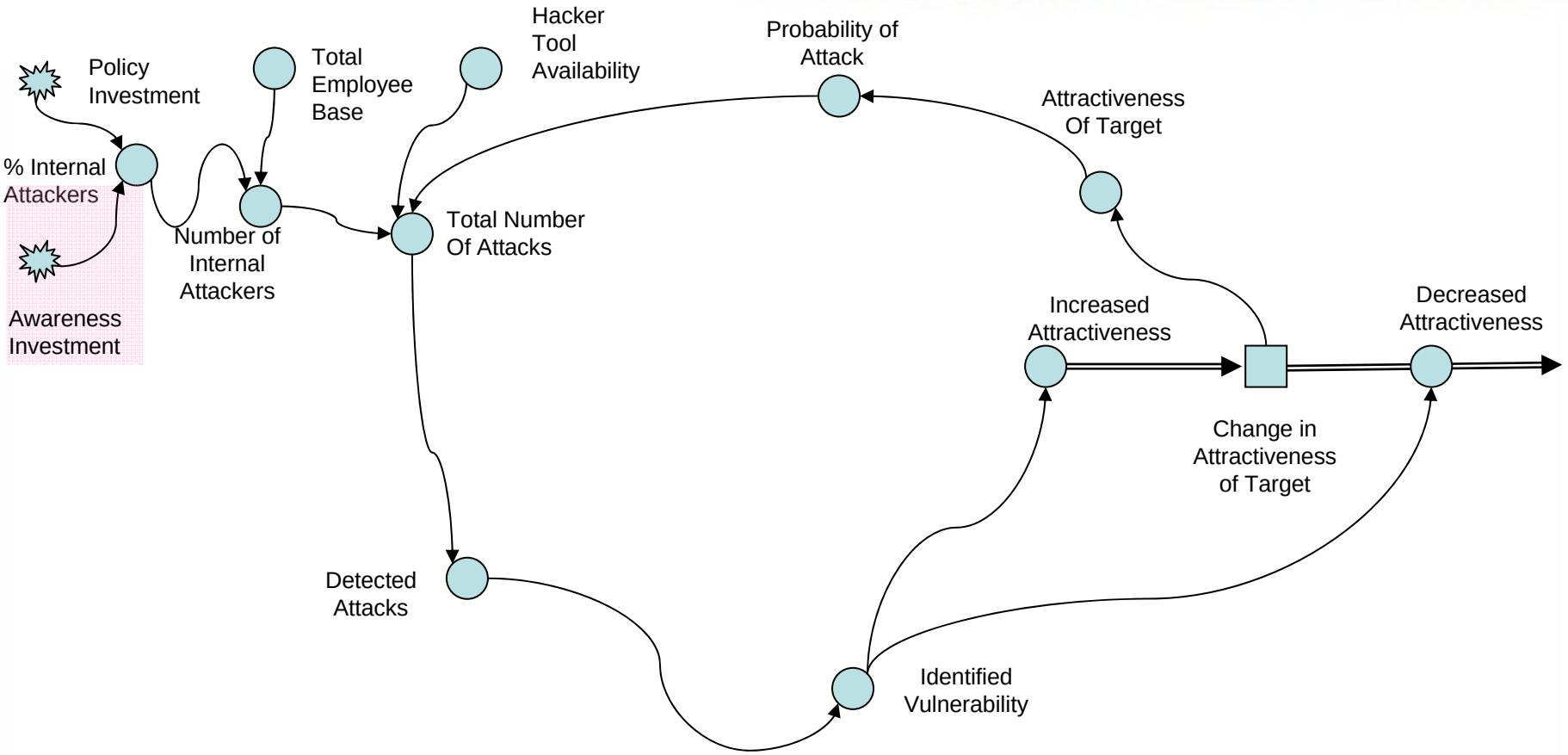




© 2009, ISACA. All Rights Reserved.

Internal Compromise – Add Awareness



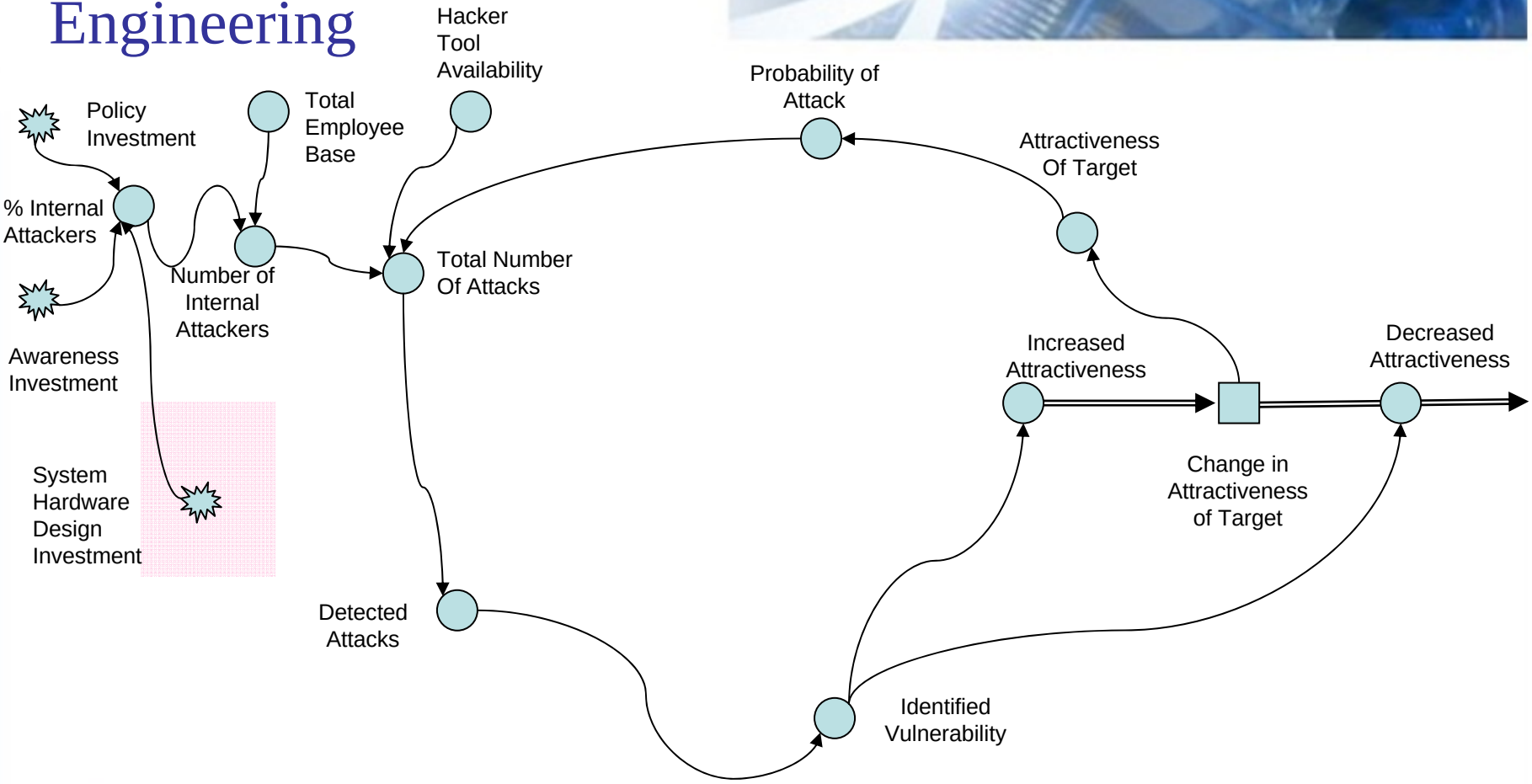


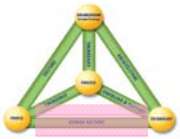


© 2009, ISACA. All Rights Reserved.

Internal Compromise – Add Human Factors Engineering



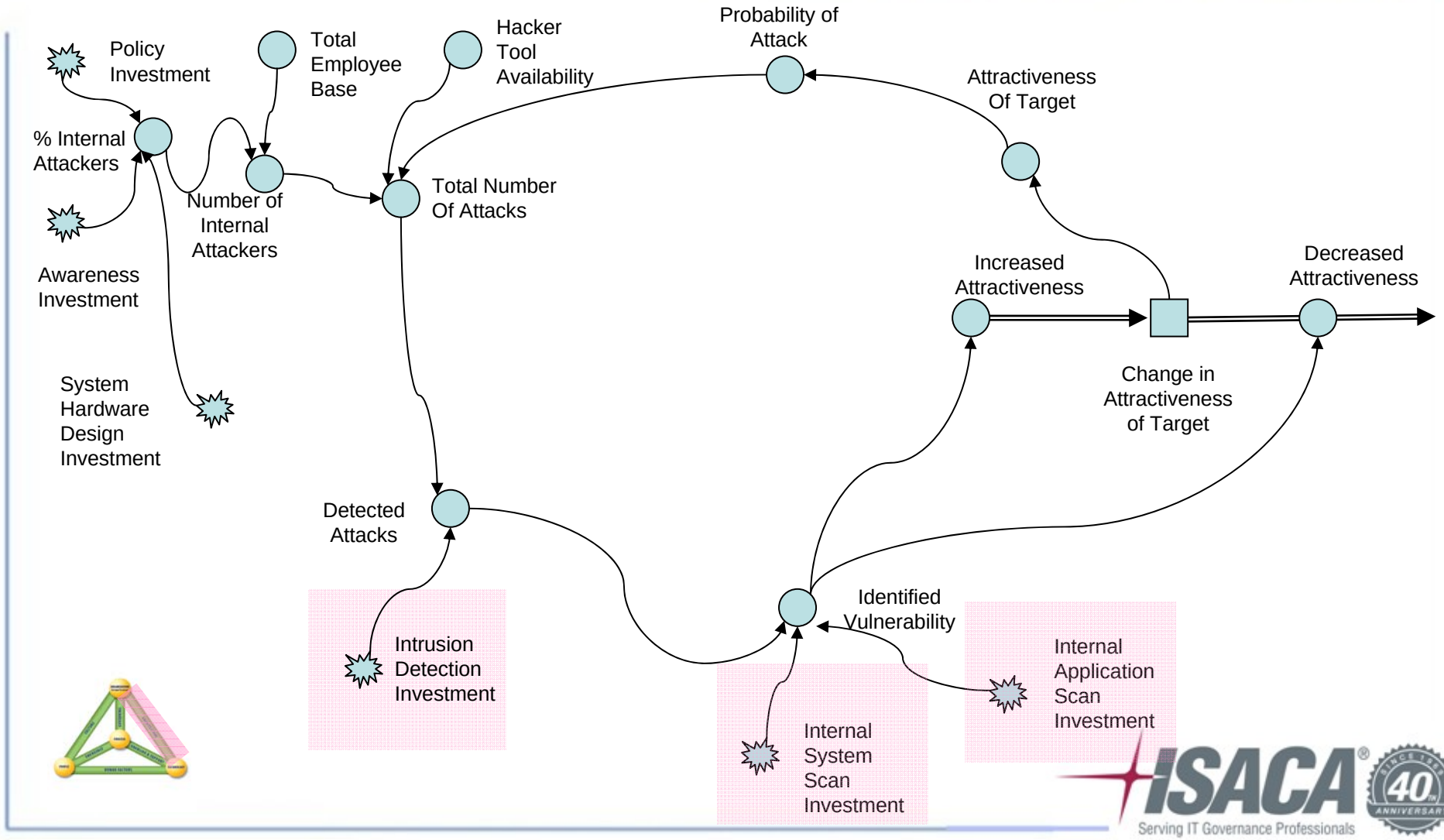




© 2009, ISACA. All Rights Reserved.

Internal Compromise – Add Internal System and Application Testing

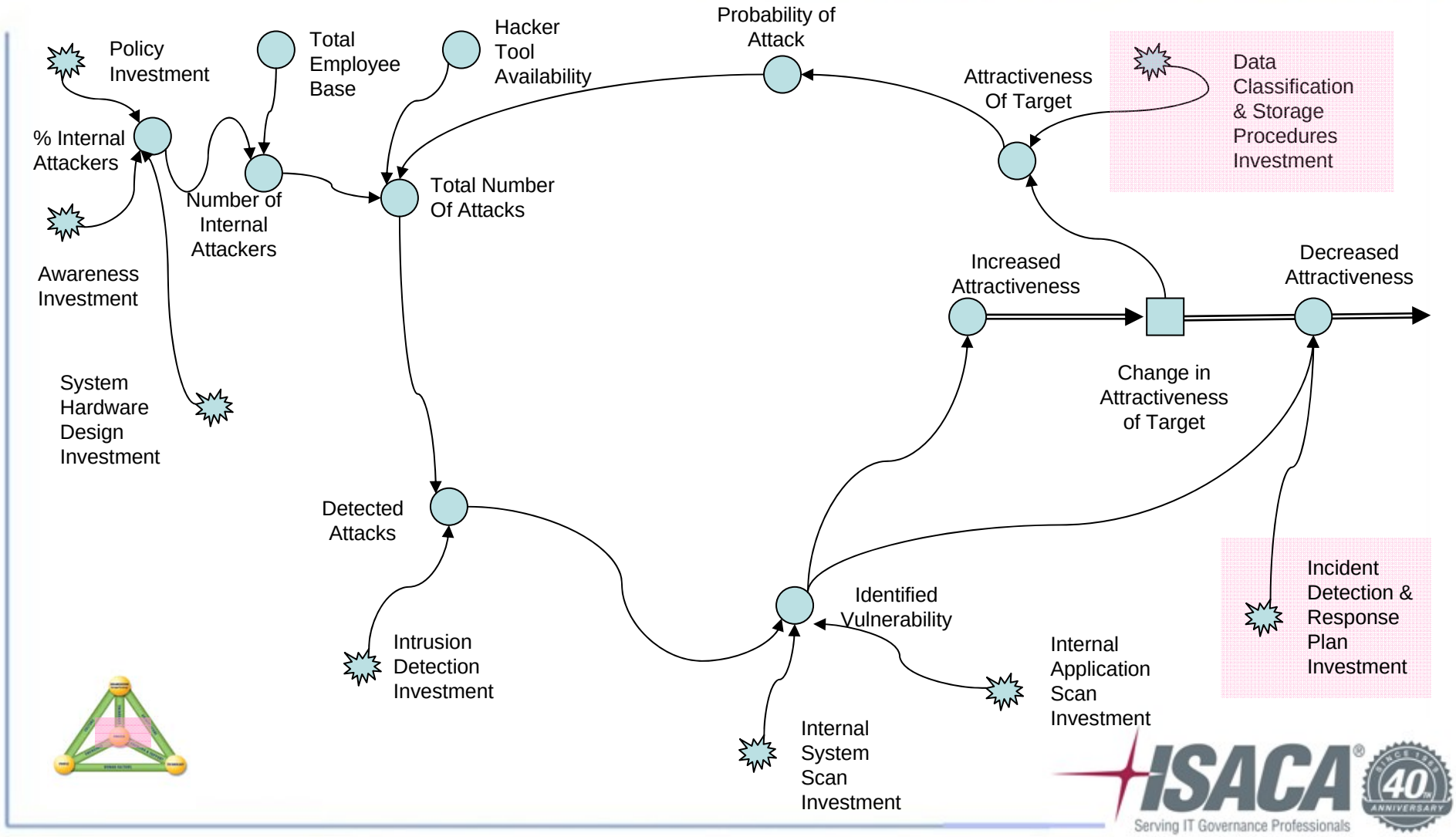




© 2009, ISACA. All Rights Reserved.

Internal Compromise – Add Procedure Changes

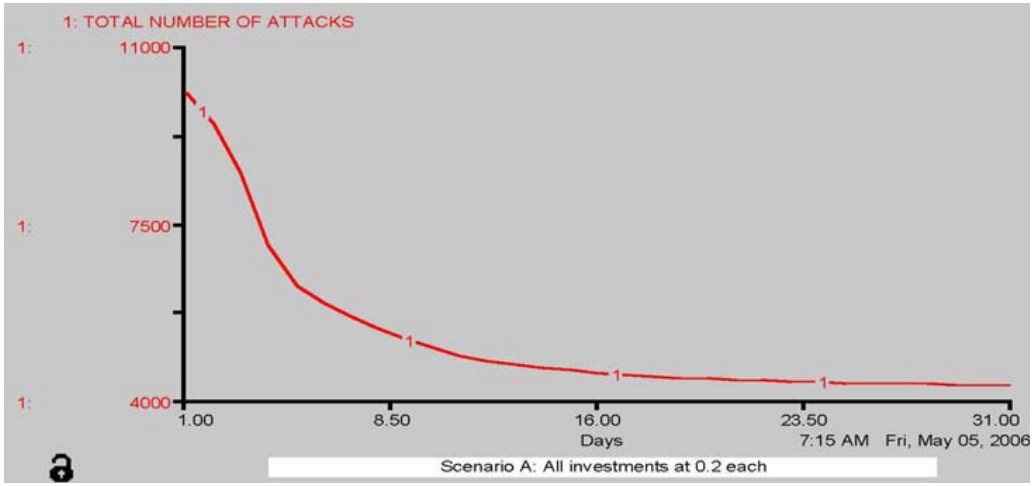




© 2009, ISACA. All Rights Reserved.

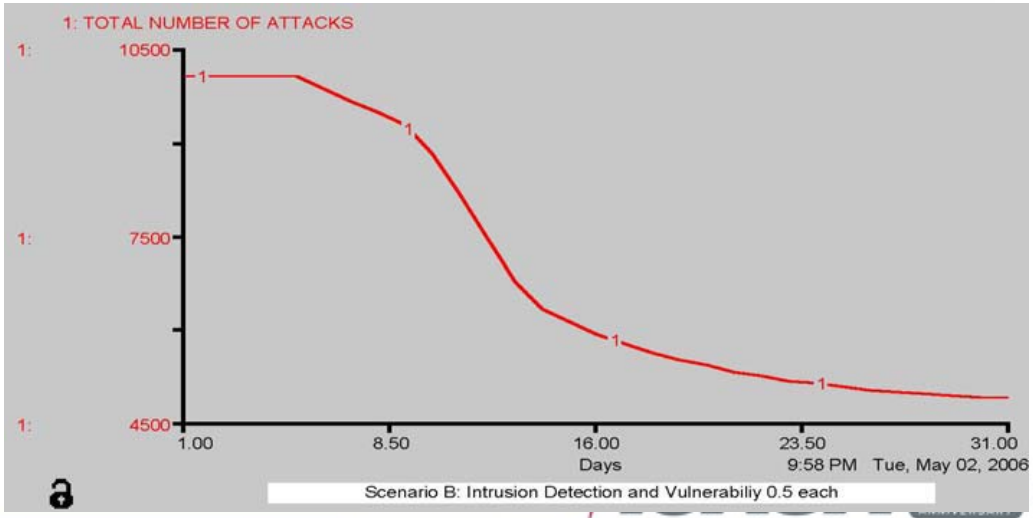
Internal Compromise – Strategy Comparison





Equally Weighted Investment Strategy

Detection and Vulnerability Reduction Strategy



© 2009, ISACA. All Rights Reserved.

Laws of the Fifth Discipline
Peter Senge

© 2009, ISACA. All Rights Reserved.

Laws of the Fifth Discipline



- Solutions that shift problems from one part of the system to another often go undetected
- The harder you push, the harder the system pushes back
- Behavior grows better before it grows worse
- The easy way out usually leads back in
- The cure can be worse than the disease

ISACA® 40 ANNIVERSARY
Serving IT Governance Professionals
© 2009, ISACA. All Rights Reserved.

Laws of the 5th Discipline



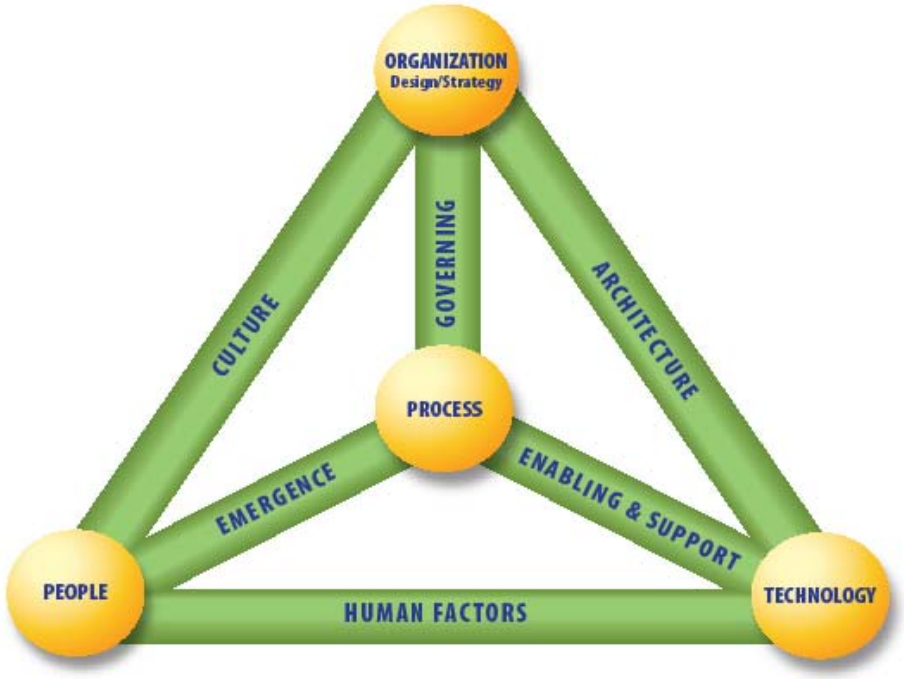
- Faster is slower
- Cause and effect are not closely related in time and space
- Small changes can produce big results – but the areas of highest leverage are often the least obvious
- You can have your cake and eat it too – but not at the same time
- Dividing the elephant in half does not produce two small elephants
- There is NO blame

ISACA Serving IT Governance Professionals 40th ANNIVERSARY

© 2009, ISACA. All Rights Reserved.

Questions?





ISACA® 40th ANNIVERSARY
Serving IT Governance Professionals

© 2009, ISACA. All Rights Reserved.