

Best Practices for Creating a Unified Risk Management Approach

Michael Croy

Director, Business Continuity Solutions

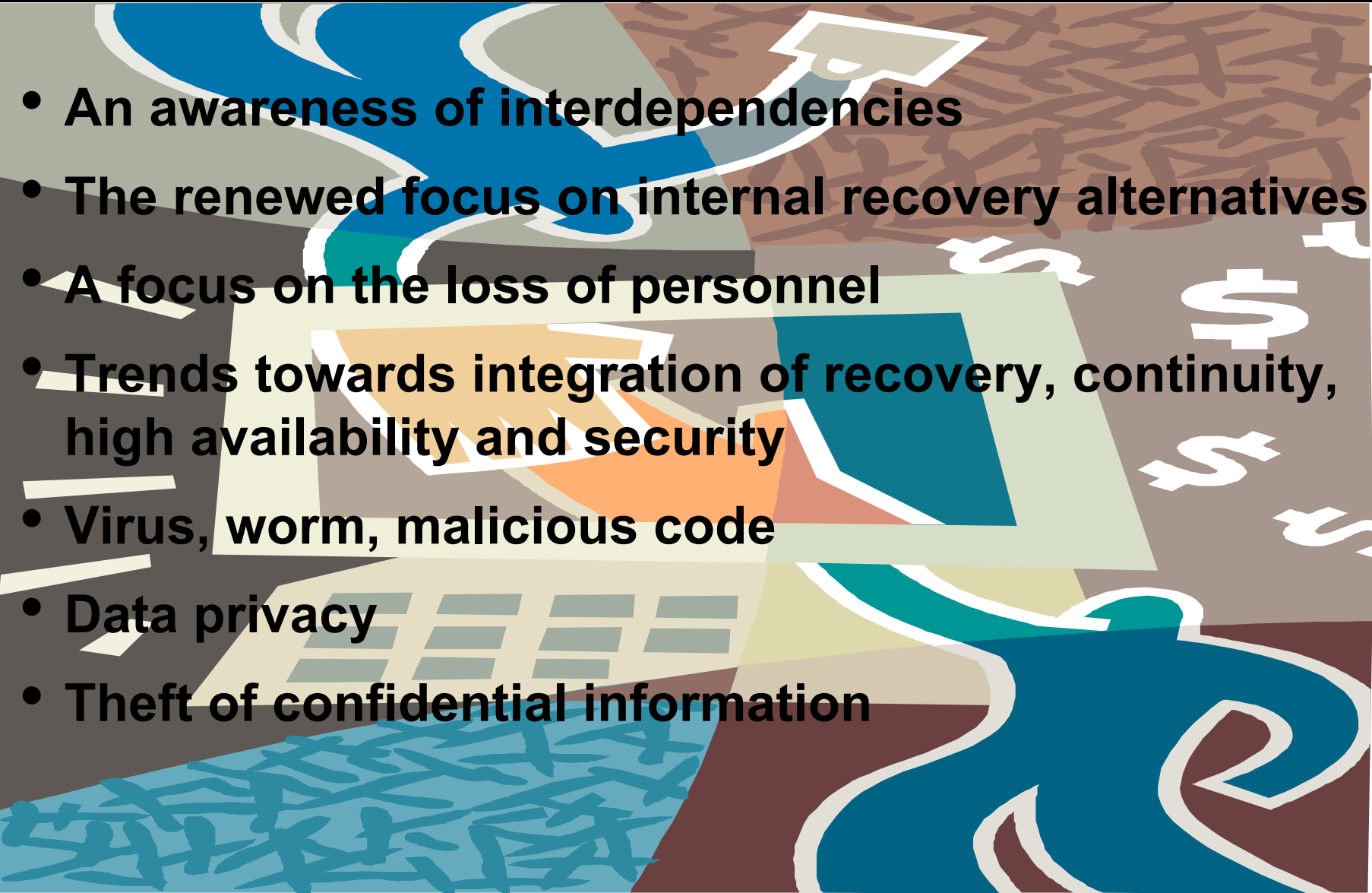
Edward Smith

Director, Security Solutions

F  **R S Y T H E**

Delivering the business value of IT.SM

Risk Management Today

- 
- An awareness of interdependencies
 - The renewed focus on internal recovery alternatives
 - A focus on the loss of personnel
 - Trends towards integration of recovery, continuity, high availability and security
 - Virus, worm, malicious code
 - Data privacy
 - Theft of confidential information

- 
- **Strategies for dealing with the data explosion, both electronic and paper based records**
 - **Planning for loss of strategic facilities**
 - **The impact of the Internet & e-mail outages**
 - **Awareness of communications issues & transportation limitations**

- Requirements of Corporate Data
 - Available (BCP)
 - Recoverable (DR)
 - Confidential (security privacy)
 - Data Integrity (security controls)
 - Accountability (audit & monitoring controls)



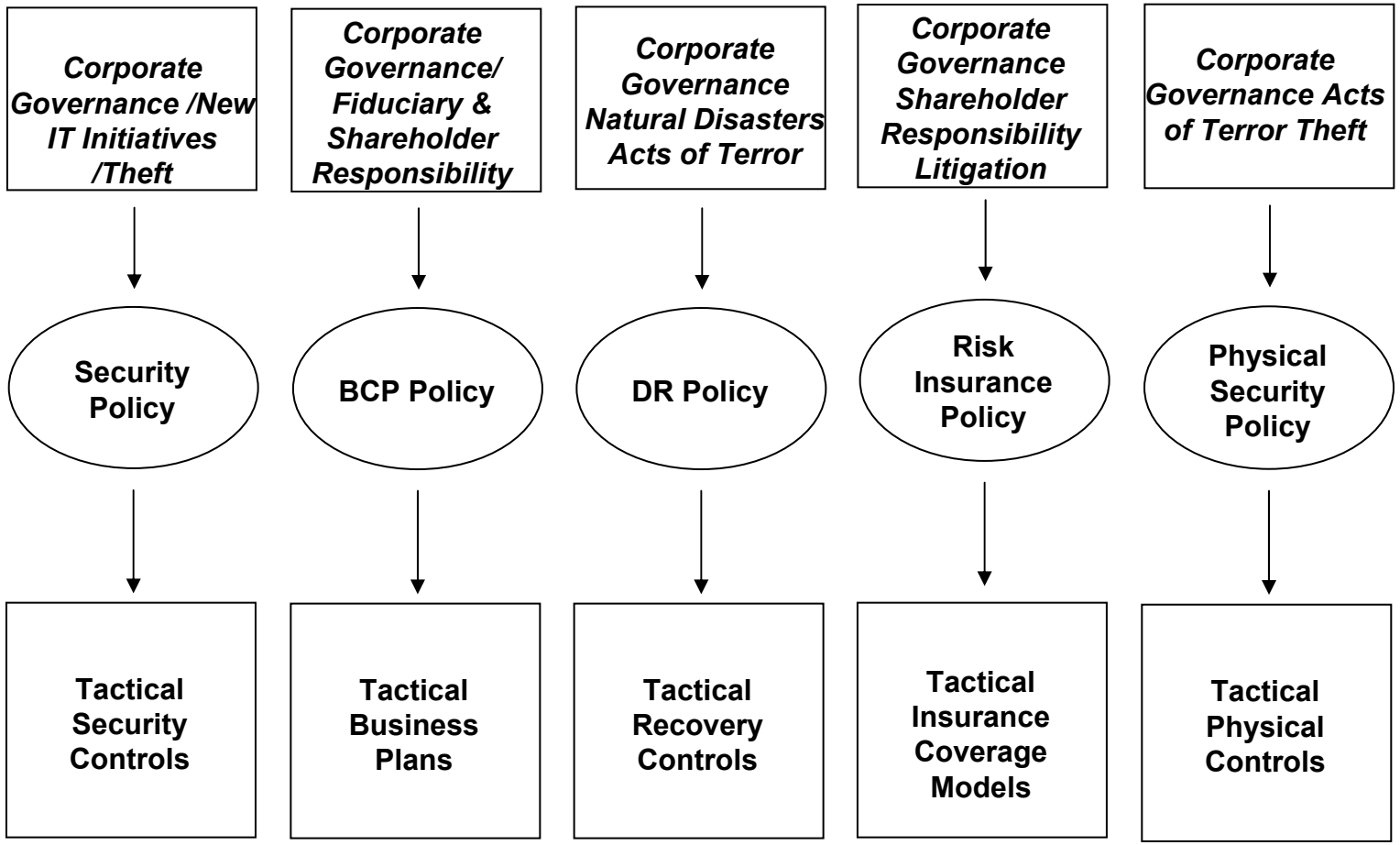
The “Silo” Approach

- Traditional risk management has been reactive, physically-oriented, with a focus on insurance
- Doesn't examine the business impacts that a physical or logical crisis would bring
- Does not tie together common compliance themes
- Does not allow for economies of scale in tying together common strategies to risk mitigation
- Difficult to accomplish corporate goals with so many disparate approaches to mitigate risk

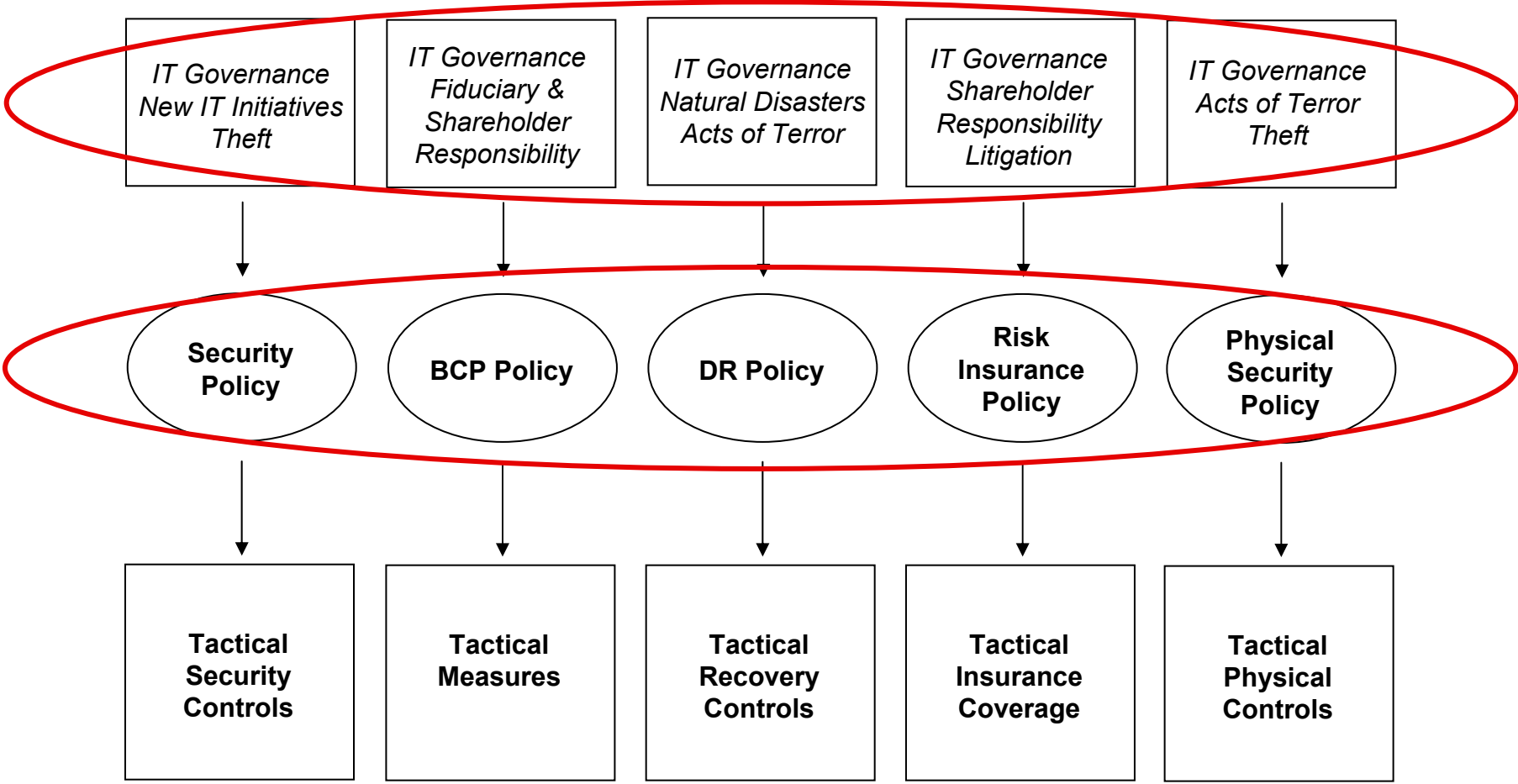


(Not that kind)

The "Silo" Approach



Fiscal and fiduciary responsibility of the business



Today's Convergence of Risk Strategies

Executive level responsibility

Governance / Fiduciary & Shareholder Responsibility / New IT Initiatives / Business Response / Natural Disasters / Acts of Terror / Theft / Litigation

Common Policies That Drive:

Information Security

Business Continuity

Disaster Recovery

Risk Management

Physical Security

Tactical Security Controls

Tactical Measures

Tactical Recovery Controls

Tactical Insurance Coverage

Tactical Physical Controls

- Realize the relationship between the silos and business units
- Map the risk management plan to the needs of all business segments
- Compliance: SOX, HIPAA, GLBA, Basel II, EU Data Standards, SB1386, Patriot Act, SEC 38A.1, and many more
- Maximum relationship benefit is achieved through silo inter-dependencies
- Formalized security programs
- BC planning that protects the business first (RTO/RPO)

Company Profile

- Small, private start-up in 1949
- Publicly-traded since 1969
- For past decade, revenue increased 10X YTY
- Risk management initiatives are tactical... they are reactively “siloed,” i.e. stuck in 1969



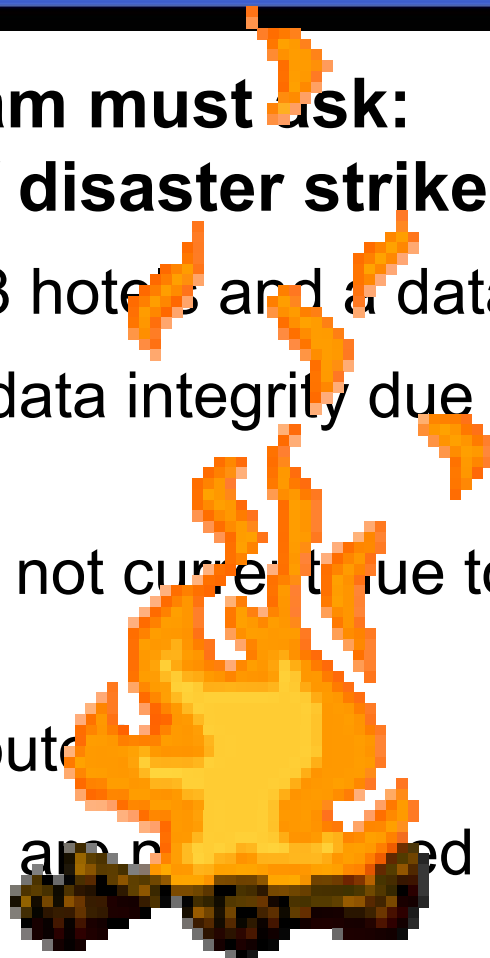
Hotel California Today

- Awareness level is rising rapidly with the executive team
- Obvious drivers understood
 - Customer credit card data (VISA CISP)
 - Regulatory impacts, i.e. SOX, SB1386
 - No formal security policy
 - Information security controls may not be adequate
 - No real physical security controls in place
- Assess
 - Q: Is this a proactive risk management plan?
 - A: No. It needs to change.
 - Q: Will this plan enable me to protect the business adequately?
 - A: No.

The executive team must ask:

“What happens if disaster strikes?”

- Fire destroys 3 hotels and a data center in San Diego
- Questionable data integrity due to lack of security controls
- Recovery plan not current due to lack of change management
- Open to distributed denial of service attacks
- Business units are not involved in DR planning



**Without collaboration between all business units,
the disaster recovery plan will fail.**

So, what's needed?

- New and improved risk management strategy
- Strategic planning in a collaborative environment
- Processes that are teamed with and support the business as well as IT
- Cross-organizational teams w/executive ownership, i.e. CEO or Chief Risk Officer
- A realistic look at threats and vulnerabilities – both physical and logical

Today's Convergence of Risk Strategies

Executive level responsibility

Corporate Governance / Fiduciary & Shareholder Responsibility / New IT Initiatives / Business Response / Natural Disasters / Acts of Terror / Theft / Litigation

Common Policies That Drive:

Information Security

Business Continuity

Disaster Recovery

Risk Management

Physical Security

Tactical Security Controls

Tactical Measures

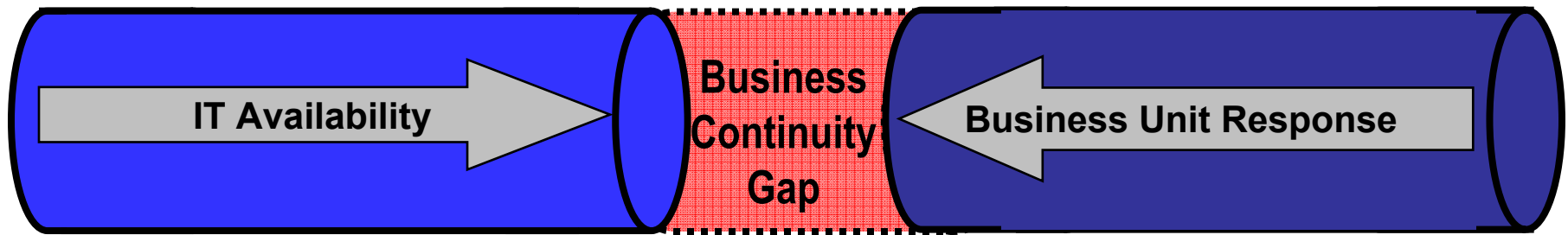
Tactical Recovery Controls

Tactical Insurance Coverage

Tactical Physical Controls

Remember the Business Continuity Gap?

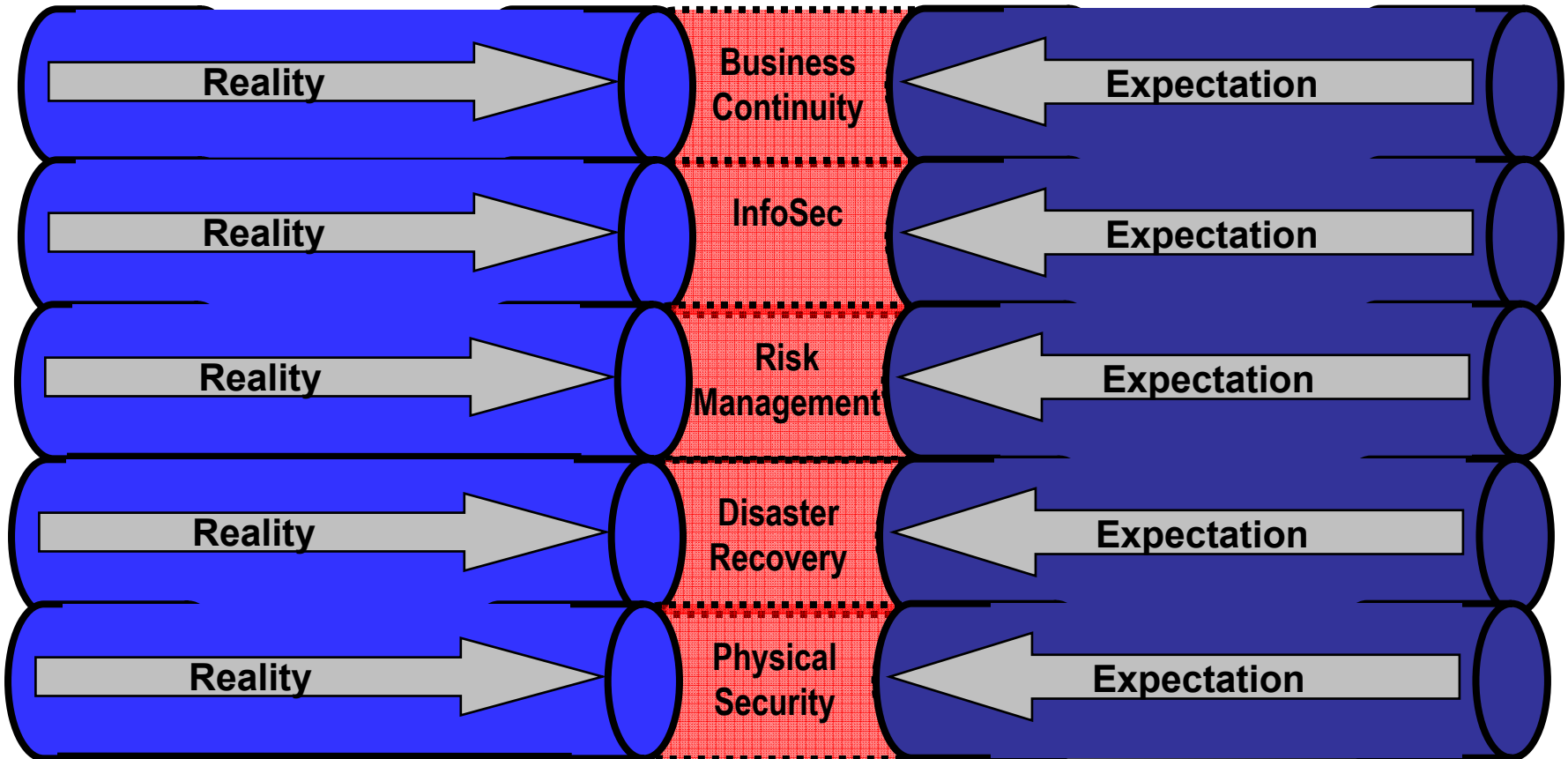
It's Reality vs. Expectation



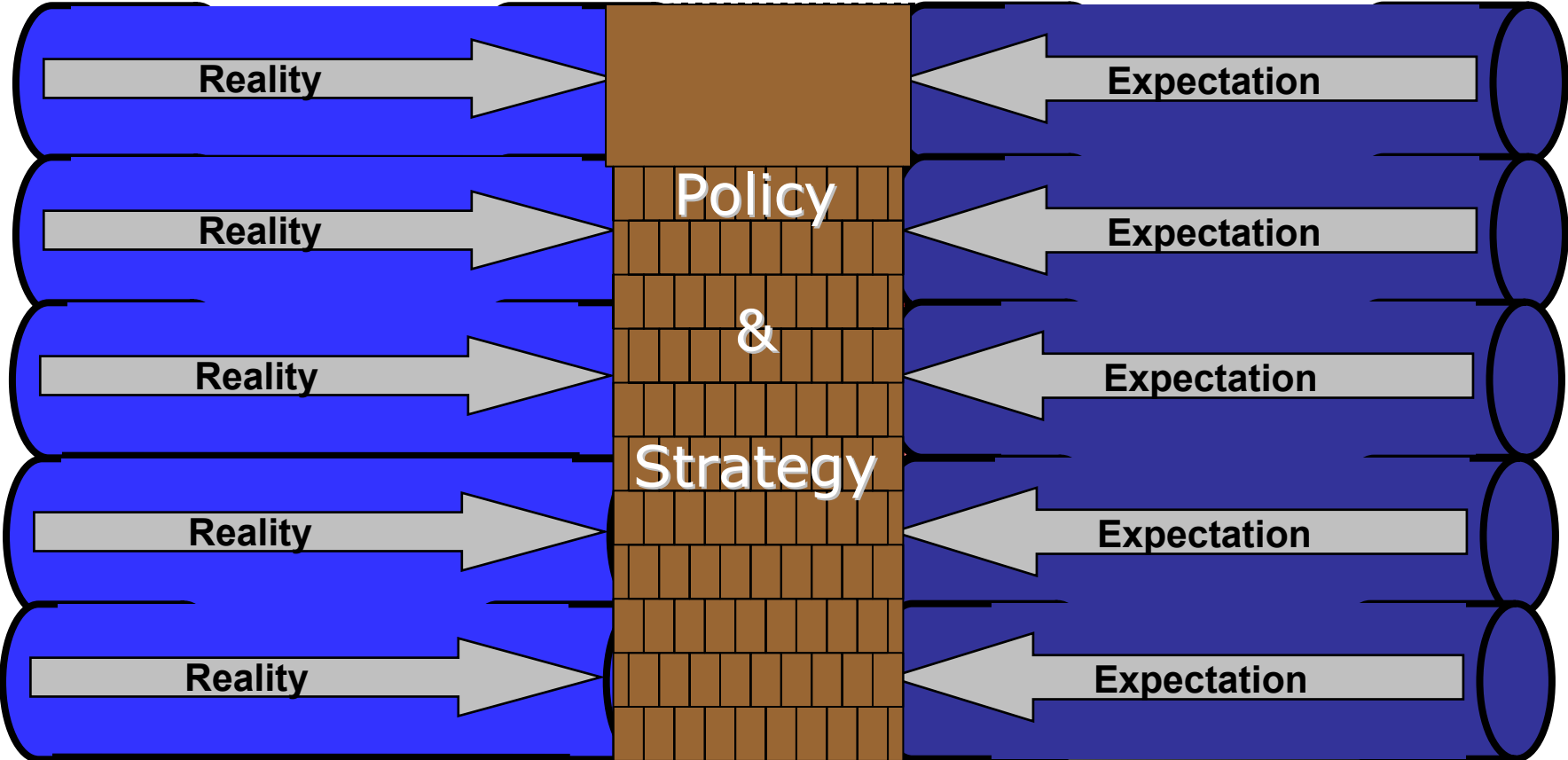
BUT.....

It's not just Business Continuity

A policy of non-collaboration



Common goals across the organization will remove the silos and close the gaps



- Realize economies of scale – maximum ROI
- Foster environment of sharing information between business units and IT
- Increased technology efficiencies drive business improvement
- Understanding the business context of IT
- Ability to effectively leverage IT infrastructure to support business goals
- Enhanced ability to meet compliance goals

- Reassess your approach to recovery, continuity, availability and security
- Get business owners involved in the process
- The new way of thinking: GET ON WITH IT
- Adjust the mindset
 - The business is open but the effectiveness is minimized
 - The business feels little to no effect



Michael Croy

Director, Business Continuity Solutions
mcroy@forsythe.com

Edward Smith

Director, Security Solutions
esmith@forsythe.com



Delivering the business value of IT.SM