

# **Business Continuity and Audit Controls**

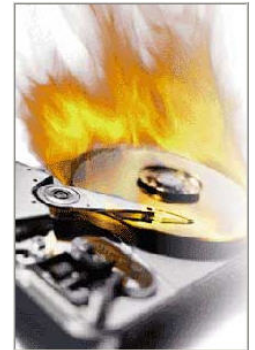
**Chris Ardagh**

**March 18, 2008**





# Disasters Waiting to Happen...



## ❑ United States

- ↳ 46% of Executives said their ability to deliver continuous service during a disaster is improving
- ↳ 39% graded their firms' capacities at a 'C Level' or lower (in 2005 it was only 24%)
- ↳ Only 26% of companies have Pandemic Plans

## ❑ Canada

- ↳ 72% of Executives admit to having no disaster recovery or business continuity plans
- ↳ 44% impacted by disasters in last 24 months



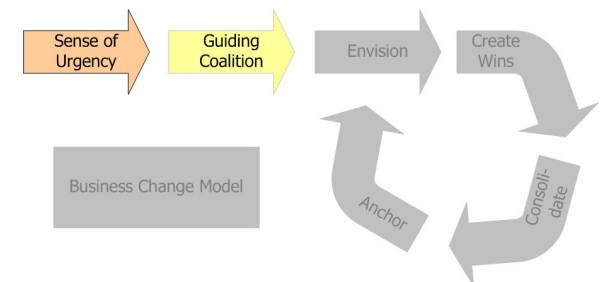
## Today's Objectives is to Understand:

- ❑ Adopting a business continuity strategy
- ❑ Keeping the momentum during audits
- ❑ Importance of auditing in business continuity
- ❑ Link between business continuity and audit
- ❑ Understanding and overcoming challenges
- ❑ Regulatory requirements and functions
- ❑ Identified gaps between BCP and controls



## Why Conduct BCP Audits?

- ❑ Provide Management Assurance
- ❑ Identify Control Gaps
- ❑ Regulatory Compliance
- ❑ Identify Actions to Enhance Maturity
- ❑ Ensure Business Process Owners are Accountable to their Plans and Testing





# What is Business Continuity Management?

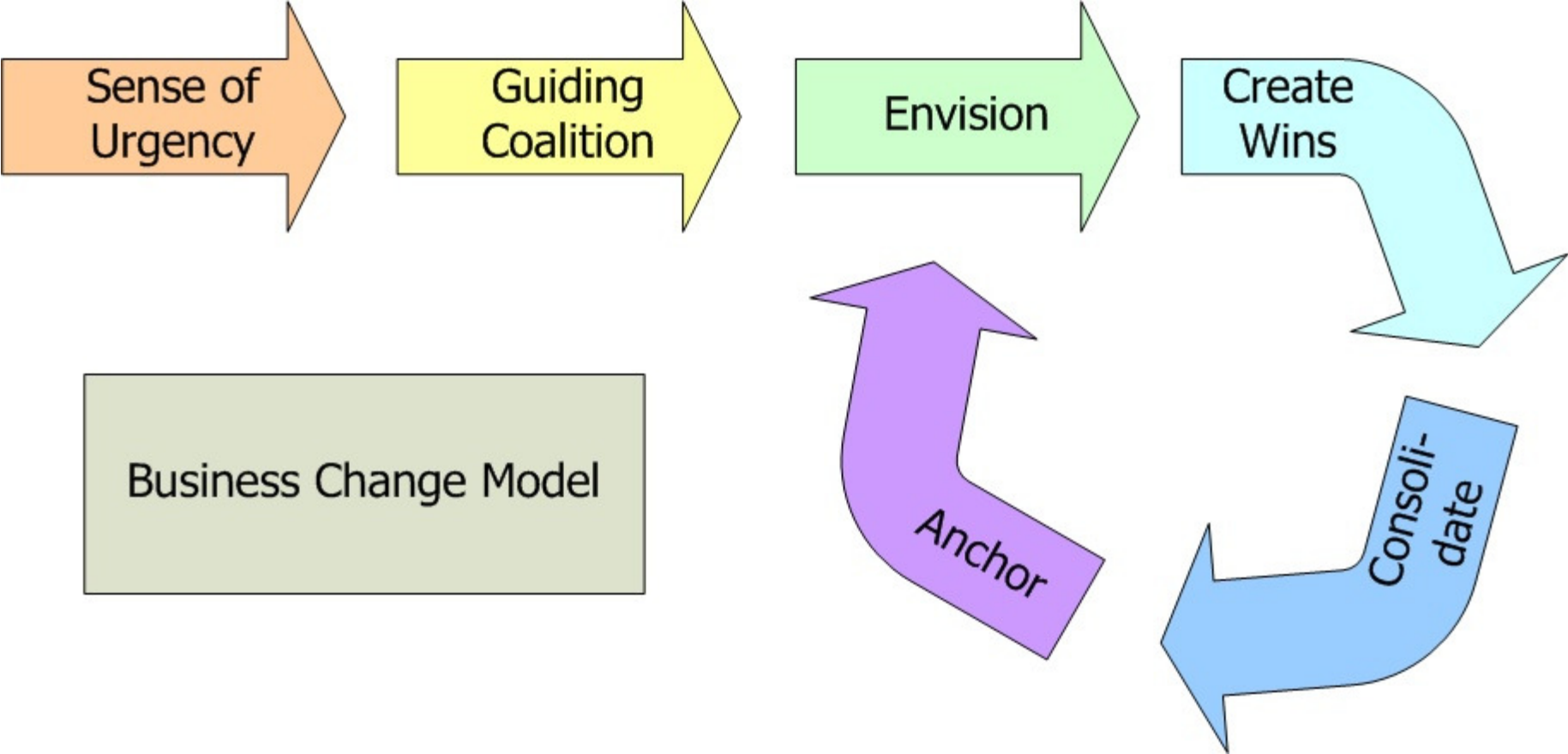


**...the development of strategies, plans, and actions which focus on assuring continuous business processes.**

**It is the major factor that determines and organization's survival during and after a significant business disruption.**

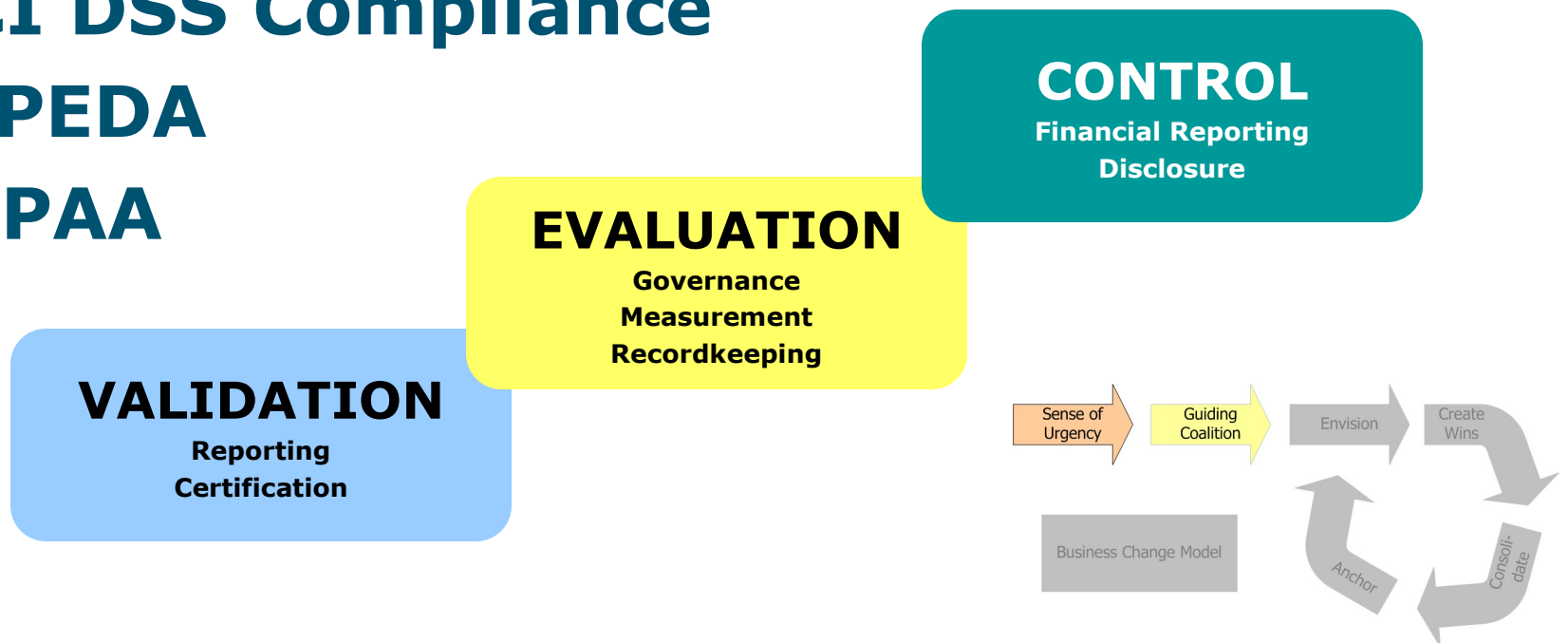


# Business Continuity...simply a Business Change



# Challenge #1: Regulatory Requirements

- ❑ **Sarbanes-Oxley Act**
- ❑ **Bill 198** (often referred to as C-SOX)
- ❑ **Security and Exchange Commissions**
- ❑ **PCI DSS Compliance**
- ❑ **PIPEDA**
- ❑ **HIPAA**



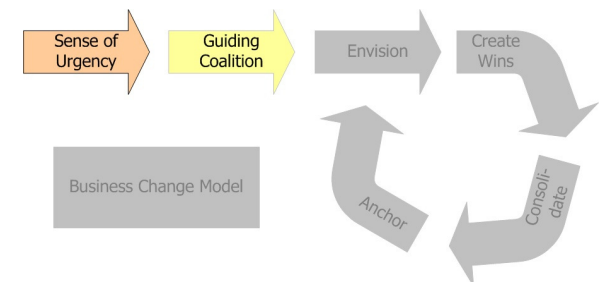


## Challenge #2: Effective IT Controls

- ❑ Most IT organizations have no way to detect changes made outside their sanctioned change-approval process
- ❑ Remember...

**Trust is  
not a  
control**

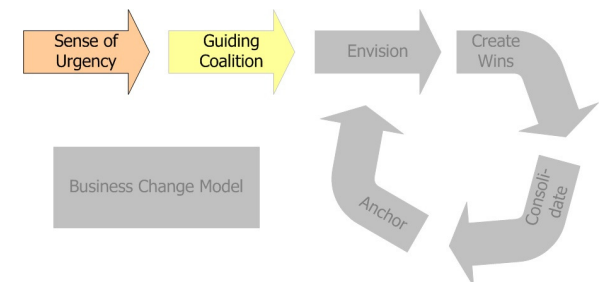
**Hope is  
not a  
strategy**





## Challenge #2: Effective IT Controls

- ❑ Establish, document, and communicate
- ❑ Enforce separation of duties
- ❑ Implement process to guide workflow
  - ↳ **change management**
  - ↳ **event monitoring and correlation**
- ❑ Implement controls to detect inappropriate activities
  - ↳ **events occurring outside the process**

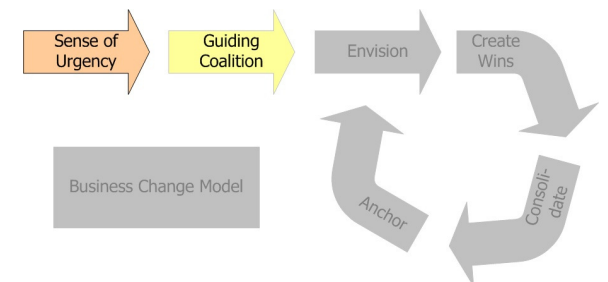




## Challenge #3: It's All in 'Interpretation'

### □ Recommendations, not standards

- ↳ Most legislation does not define specific actions for 'internal controls'
- ↳ Many companies have utilized existing standards:
  - COBIT
  - ISO 17779:2005
  - BS-15000

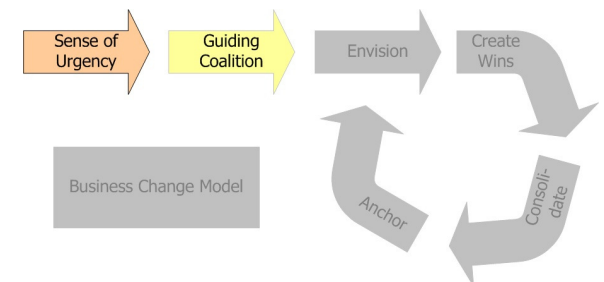




## Challenge #4: Don't Be Surprised

### □ Prepared Organization

- ↳ Periodic document review;
- ↳ Change log;
- ↳ Authorization processes;
- ↳ “Three ring binder” of
  - authorized work orders;
  - State of the infrastructure;
  - Sign off.





## Challenge #5: Establish Sense of Urgency

### ❑ **Cost – When an outage occurs**

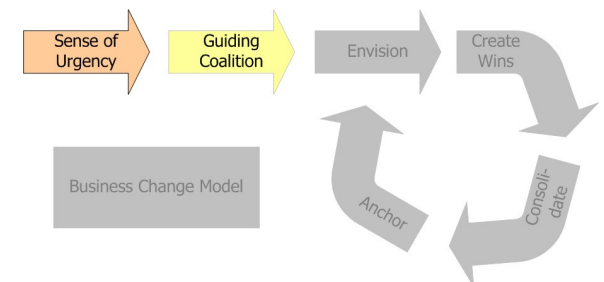
- ↳ Loss of revenue and/or market share
- ↳ Penalties for missed SLA's and obligations
- ↳ Enormous recovery costs

### ❑ **Risk – Lack of continuity plans**

- ↳ Loss of image and reputation
- ↳ Loss of operational capabilities

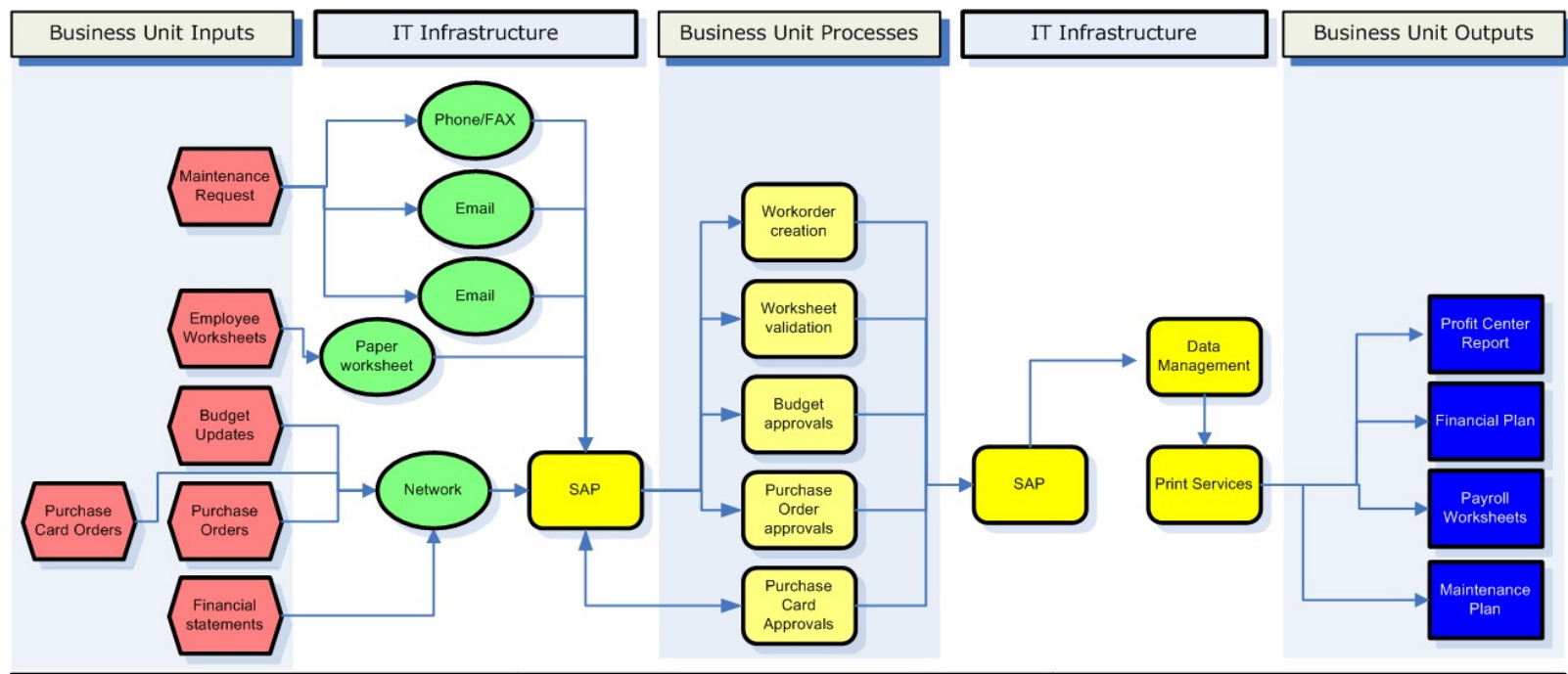
### ❑ **Revenue – Opportunity**

- ↳ Continuity as a differentiator
- ↳ Capability and Maturity

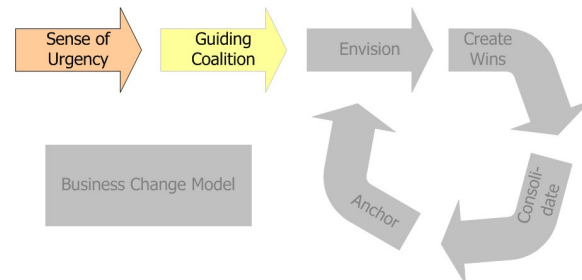




# Challenge #6: Monetizing Cost of Downtime



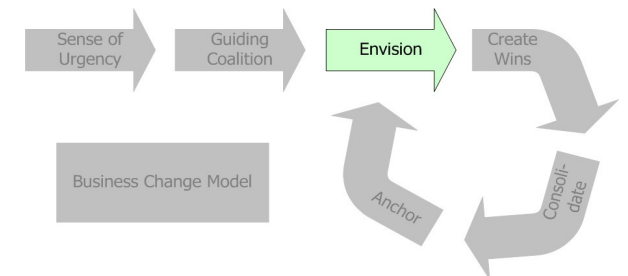
- ❑ Historical data
- ❑ Revenue loss
- ❑ Productivity loss



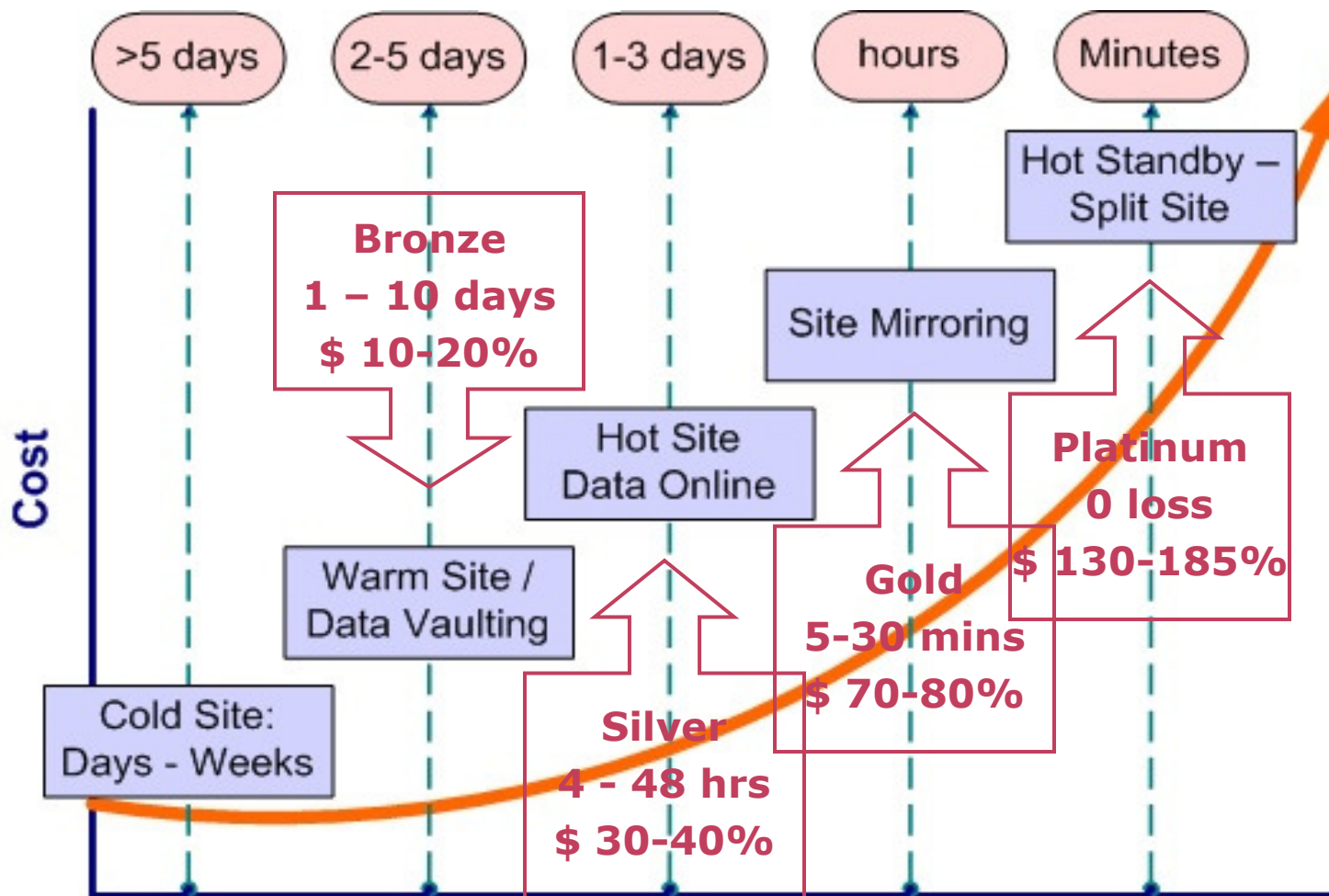
# Envision - Why Are You Planning?



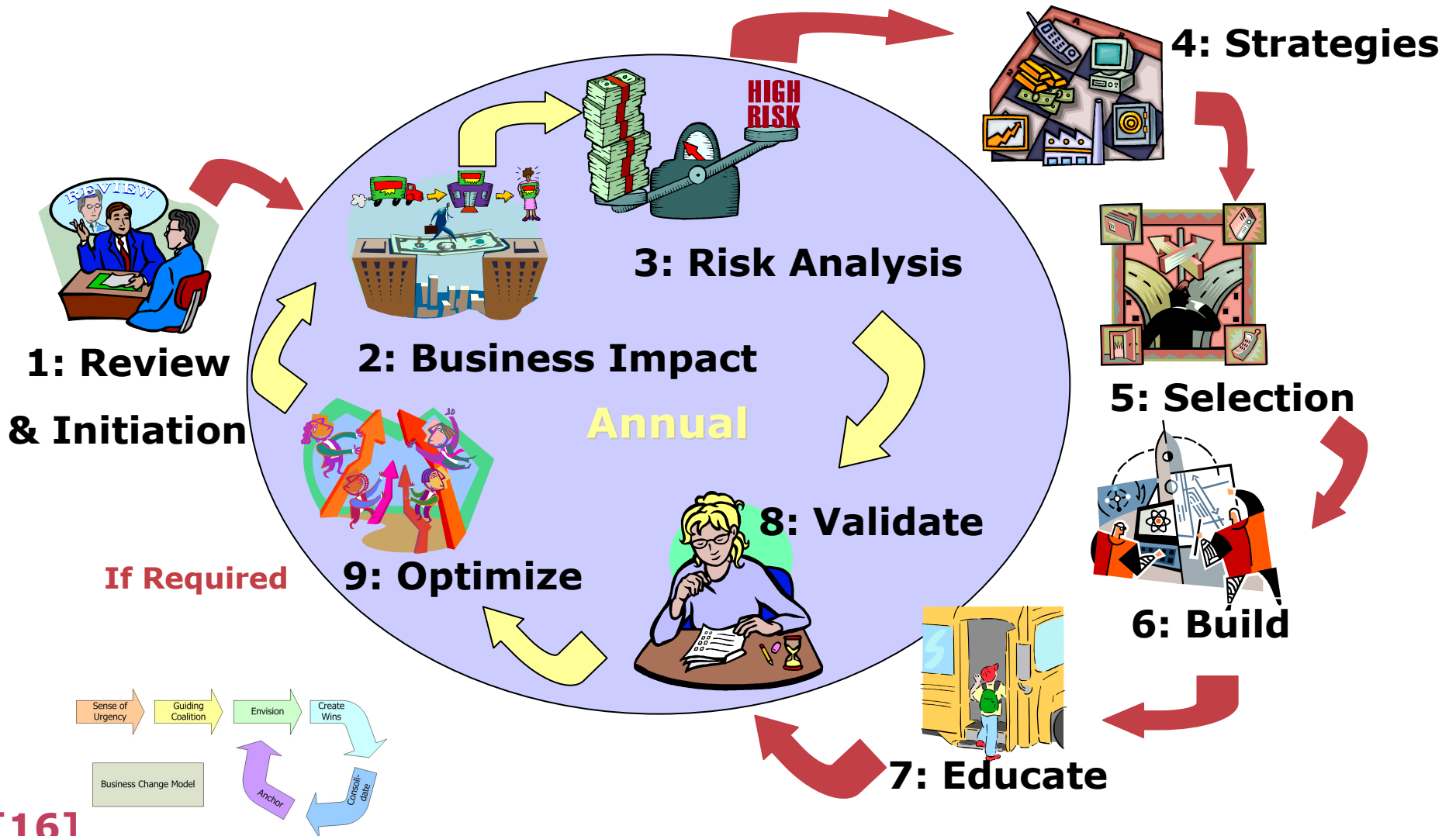
- ❑ Regulatory Requirements
- ❑ Manage Business Disruption
- ❑ Organization Reputation
- ❑ Revenue Retention
- ❑ Minimize Outage Visibility
- ❑ Unplanned Events



# Challenge #7: Do Costs Outweigh Benefits?



# Developing Business Continuity Service in Nine Steps





## Summary

- Understand your business objectives
- Define your business approach
- Overcome your challenges
- Ensure validation for success



**Questions?  
Thank-you**

**Chris Ardagh**  
[chrisa@carefactor.com](mailto:chrisa@carefactor.com)