

# Making the Jump to Risk Management

Jeff Blackmon, FBCI, CISSP, CBCP, ITIL  
*Strategic Continuity Solutions, LLC.*



## Jeff Blackmon, FBCI, CISSP, CBCP, ITIL

- Started BC/DR planning work in the mid 1980's
  - Financial
  - Petroleum
  - Foreign Military
  - Pharmaceutical
  - Healthcare
  - U.S. Government
- Contract Consultant based in Kansas City area, but have been working remote for almost all projects.

## Topics:

- Risk Categories
- Definitions
- Inside Risk Management (new parts and pieces)
- Qualitative and Quantitative Exposure
- BC, Security and Compliance in Risk Management
- Discussion?

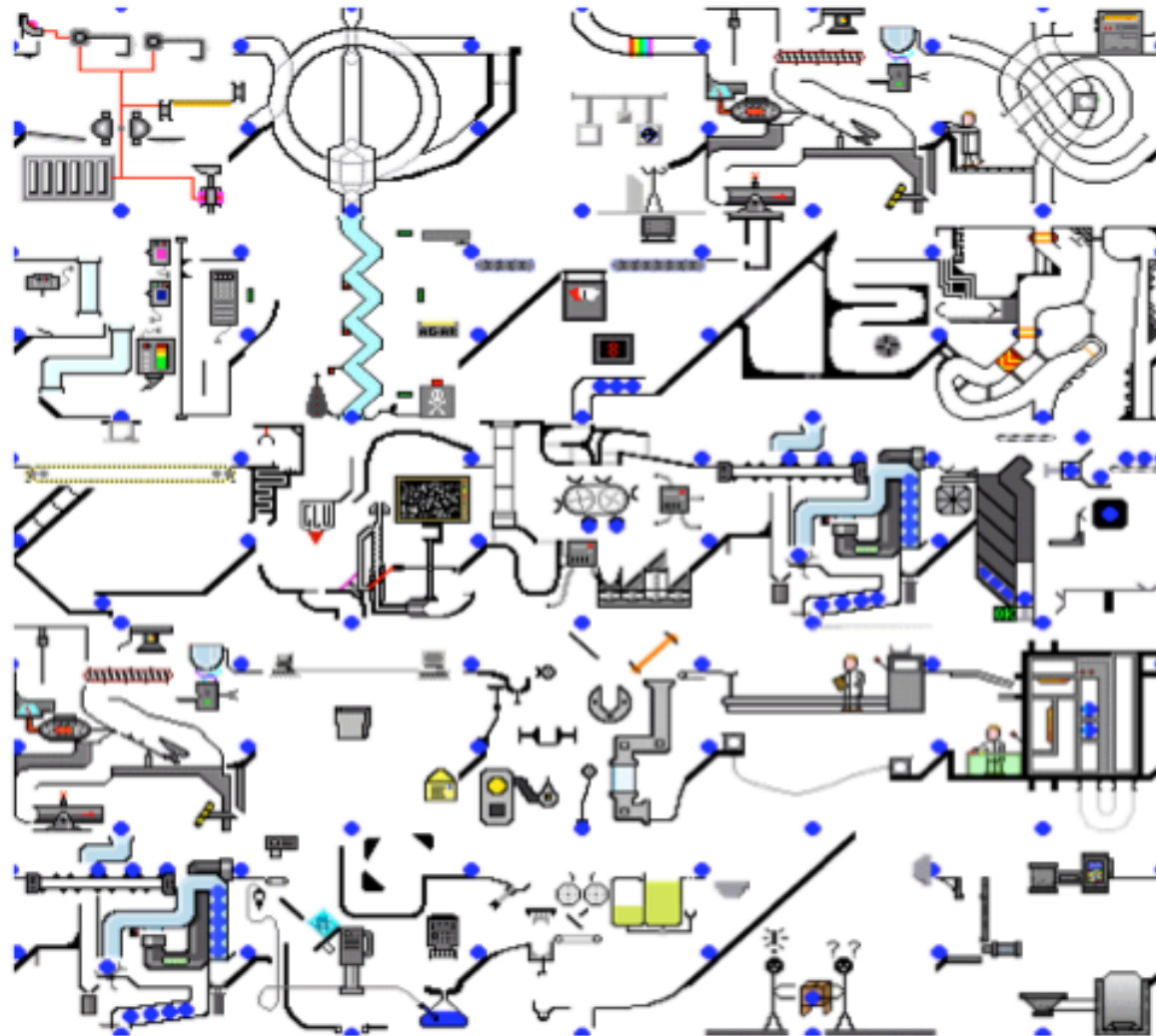
## What Risk Management is NOT:

- NOT the consolidation of Compliance, Security and BC into a single function
- NOT changing any of the functions of Compliance, Security or BC

## Risk Management IS:

- More Collaboration between Compliance, Security and BC
- More Communication between Compliance, Security and BC

## Some times Risk Management appears to be very convoluted



## Risk Categories:

- Compliance
- Credit
- Liquidity
- Market
- Operational
- Strategic
- Other

## Risk Categories:

- **Compliance**
- Credit
- Liquidity
- Market
- **Operational (Business Continuity and Security)**
- Strategic
- Other

## Risk

- A measure of the potential for loss in terms of both the likelihood of the incident and the consequences of the incident (Probability and Impact)

## Risk Analysis

- The development of a quantitative or qualitative estimate of risk for combining estimates of incident likelihood and consequences



## Risk Assessment

- The process by which the results of a risk analysis are used to make decisions through relative ranking of risk reduction strategies

## Risk Management

- The planning, organizing, leading and controlling of an organization's assets and activities in ways, which minimize the adverse operational and financial effects of accidental losses upon the organization (Mitigation and Contingency)

## Risk Resolution:

- Take no action and accept the risk
- Defer action for short term
- Develop action plan
  - Avoid the risk
  - Transfer risk to third party (such as insurance)
  - Mitigate the risk
    - Prevent risk event
  - Contingency if risk event occurs
    - Lessen the Impact

**Threats and Vulnerabilities are unlimited. The funds to mitigate them are not.**

Overall Goals:

- Manage exposure to Risk
- Improve resilience
- Control costs

ROI from Risk programs is derived more from keeping and attracting clients than it is from loss avoidance.

## Key element, Know your loss potentials:

- Natural, man-made, technological or politically related
- Accidental versus intentional
- Internal versus external
- Manageable risks versus those beyond the company's control

## Single Loss Expectancy (SLE)

- $SLE = \text{Asset Value (\$\$)} \times \text{Impact}$

## Annual Lose Expectancy (ALE)

- $ALE = SLE \text{ (from above)} \times \text{yearly estimates}$

- $\$ \text{ Risk Exposure} = \text{Asset Value (\$\$)} \times \text{Impact} \times \text{yearly estimates}$

## \*NEW\* Emerging Risk Register

- Event: What could happen? (Threat)
- Probability: How likely is it to happen?
- Impact: How bad will it be if it happens?
- Mitigation: How can we reduce the probability?
- Contingency: How can we reduce the impact?
- Reduction = Mitigation x Contingency
- Exposure = Risk – Reduction

## \*NEW\* Emerging Risk Register, also to include

- Risk record owner
- Mitigation strategy
  - Mitigation cost
  - Mitigation expected loss return
- Contingency strategy
  - Contingency cost
  - Contingency expected loss return
- Status/dates of actions
- New adjusted Risk Exposure rating

Risk Impact				
Rating Assessment	Low (<20%)	Mod (21%-50%)	High (51%-80%)	Extreme(81%+)
Quality	Minor degradation	Obvious degradation	Major degradation	Effectively Useless
Time	<5% time increase	5%-10% time increase	10%-20% time increase	>20% time increase
Cost	Insignificant cost increase	<10% cost increase	10%-25% cost increase	>25% cost increase

**Find best assessment based on Quality, Time and Cost Impact**



## Risk Exposure Results (Qualitative Example)

Impact	Low (<20%)	Mod (21%-50%)	High (51%-80%)	Very High(81%+)
Probability/year				
>91% (Very High)	Moderate	High	Very High	Very High
61%-90% (High)	Moderate	High	High	Very High
21%-60% (Mod)	Low	Moderate	High	High
<20% (Low)	Low	Low	Moderate	High

**Impact x Probability = Risk Exposure**

**Classifications above based upon company Risk Acceptance profile**

## Risk Exposure Results (Partial Quantitative)

Impact	Low (<20%)	Mod (21%-50%)	High (51%-80%)	Very High(81%+)
Probability/ year				
>81%	Moderate	High	Very High	Very High
61%-80%	Moderate	High	High	Very High
41%-60%	Low	Moderate	High	Very High
21%-40%	Low	Moderate	High	High
5%-20%	Low	Low	Moderate	High
<5%	Very Low	Low	Moderate	Moderate

**Impact x Probability = Risk Exposure**

**Classifications above based upon company Risk Acceptance profile**

## Risk Exposure Results (Quantitative)

ALE	Low	Moderate	High	Very High
Total Risk Costs	< \$10,000	\$10,000 - \$100,000	\$100,000 - \$500,000	>\$500,000

**Impact x Probability = Risk Exposure in \$\$**

**Classifications above based upon company Risk Acceptance profile**

Event: Communications Loss

If 1 of our 2 fiber cables are cut. Note major construction taking place on property.

Effect: Lose 50% of communication bandwidth

Expected Loss: \$250,000

Risk Impact: **High** Probability: 10%

Risk Exposure: **Moderate**

Record Owner: Bob Smith, Network Comms

## \$ Risk = Asset Value (\$\$) x Impact x yearly estimates

$$250,000 \times .50 \times .10 = \$12,500.00 = \text{ALE}$$

Mitigation: Do physical trace of fiber cables, mark routes and document. Cost = \$2,000

New Probability = 5%

Updated Risk Exposure:  $250,000 \times .50 \times .05 =$   
\$6,250.00

New Risk Exposure category = **Low**

Event: Encryption Failure

If Stand Alone banking Encryption Key server were to do a hard crash.

Effect: Lose 100% of ACH cash transfer

Expected Loss: \$1,250,000

Risk Impact: **Very High** Probability: 20%

Risk Exposure: **High**

Record Owner: Sam Smith, CFO

**\$ Risk = Asset Value (\$\$) x Impact x yearly estimates**

$1,250,000 \times 1.00 \times .20 = \$250,000.00$  or ALE

Mitigation: Provide remotely located failover server for Encryption. Cost = \$12,000

New Probability = 4%

Updated Risk Exposure:  $1,250,000 \times 1.00 \times .04 = \$50,000$

New Risk Exposure category = **Moderate**

Quantitative processes give much more accurate Annual Loss Expectancy (ALE), but remember, the numbers determined for loss and expectancy must be accurate. Otherwise a company's Risk Exposure calculations can vary widely.

More common for a company to start with Qualitative, and move to Quantitatively.



## So how does Risk Management **CHANGE** Business Continuity, Security and Compliance?

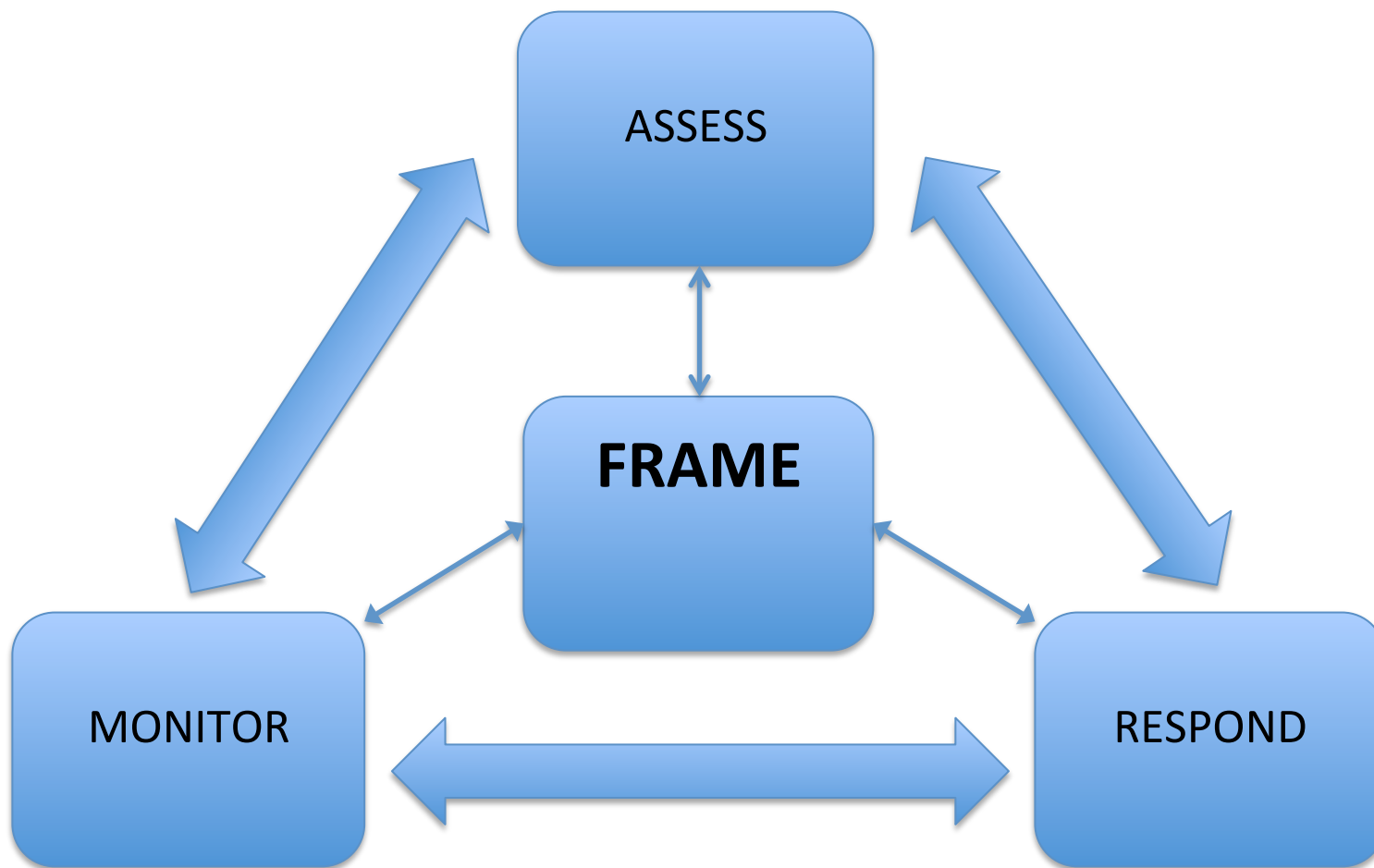
Actually, little if any. BC still does BC work and is not going away. This is the same for Security and Compliance.

Risk Management is about **collaboration and communication** between the departments for better integration.

### Overall Goals:

- Manage exposure to Risk
- Improve resilience
- Control costs





# Why is Business Continuity Important to the Risk Management process?

Much of the information used in Risk Management comes directly from the Business Continuity process.

Unaltered and unchanged. Just copied over.

## Emerging Risk Register

- **Event**: What could happen? (Threat)
- **Probability**: How likely is it to happen?
- **Impact**: How bad will it be if it happens?

Much of this information should come from the BC Risk Assessment

## Emerging Risk Register

- **Mitigation**: How can we reduce the probability?
- **Contingency**: How can we reduce the impact?

Both of the above should be part of the Business Continuity plans. Now just carried into Risk Management.

$\$ \text{ Risk} = \text{Asset Value } (\$ \$) \times \text{Impact} \times \text{yearly estimates}$

Asset Value should come from the Business Impact Analysis (BIA)



## Importance of Compliance in Risk Management

- Much has changed in dealing with compliance and audit groups over the last 20 years
- CFOs do not speak RTOs, RPOs, Gigabit Ethernet, AIX and so on
- They are very aware of PCI, OCC, FFIEC, Sarbane-Oxley and many other compliance regulations
- Considerable amount of their work is considered direct Risk Management
- Compliance groups usually have direct access to C-Level executives and can relay concerns and issues to the people that can provide the priority to get them fixed

## Importance of Security in Risk Management

- Primary group within a company for risk mitigation
  - Firewalls
  - Intrusion detection
  - malware scan
  - access control
  - and many more

None of Security's functions will change

# Importance of Business Continuity in Risk Management

- Primary group within a company for Contingency
  - IT Recovery order based on BIAs and follow-up strategies
  - Manage the people aspect of an event
  - Determine and document threat
  - Determine and document vulnerabilities
  - and much more

None of Business Continuity's functions will change

Compliance

Communications to  
management

Security

Mitigation

Business Continuity

Contingency




## Risk Management Standards

- ISO 31000:2009
- NIST 800-30
- NIST 800-37

# Questions



## Jeff Blackmon, FBCI, CISSP, CBCP, ITIL

-  001-(913)-971-4081
-  Jeff@Strat-Con-Sol.com
-  <https://www.linkedin.com/in/jeffrey-d-blackmon-fbci-cissp-cbcp-til-f-876205>

