



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

April 3, 2013



ISOAG April 2013 Agenda

- | | | |
|-------------|---|---|
| I. | Welcome & Opening Remarks | Michael Watson, VITA |
| II. | Business Continuity Planning | Jean Rowe, Verisign |
| III. | Annual Report - 2012 Preview | Michael Watson, VITA |
| IV. | Upcoming Events & Other Business | Michael Watson, VITA |
| V. | Partnership Update | Bob Baskette, VITA
Michael Clark, NG |



**“I never thought
it would happen to us...”**

Business Continuity Planning
Jean Rowe

Agenda

- What is business continuity?
- Why do you care?
- What types of plans are needed?
 - Life Safety
 - Crisis Management
 - Business Process Recovery
 - IT Disaster Recovery
- What is the process for creating business process recovery plans?



What is Business Continuity?

Business Continuity Defined

The ability of an organization to ensure continuity of service, to support its customers and to maintain its viability before, during and after an event.



Purpose of Business Continuity

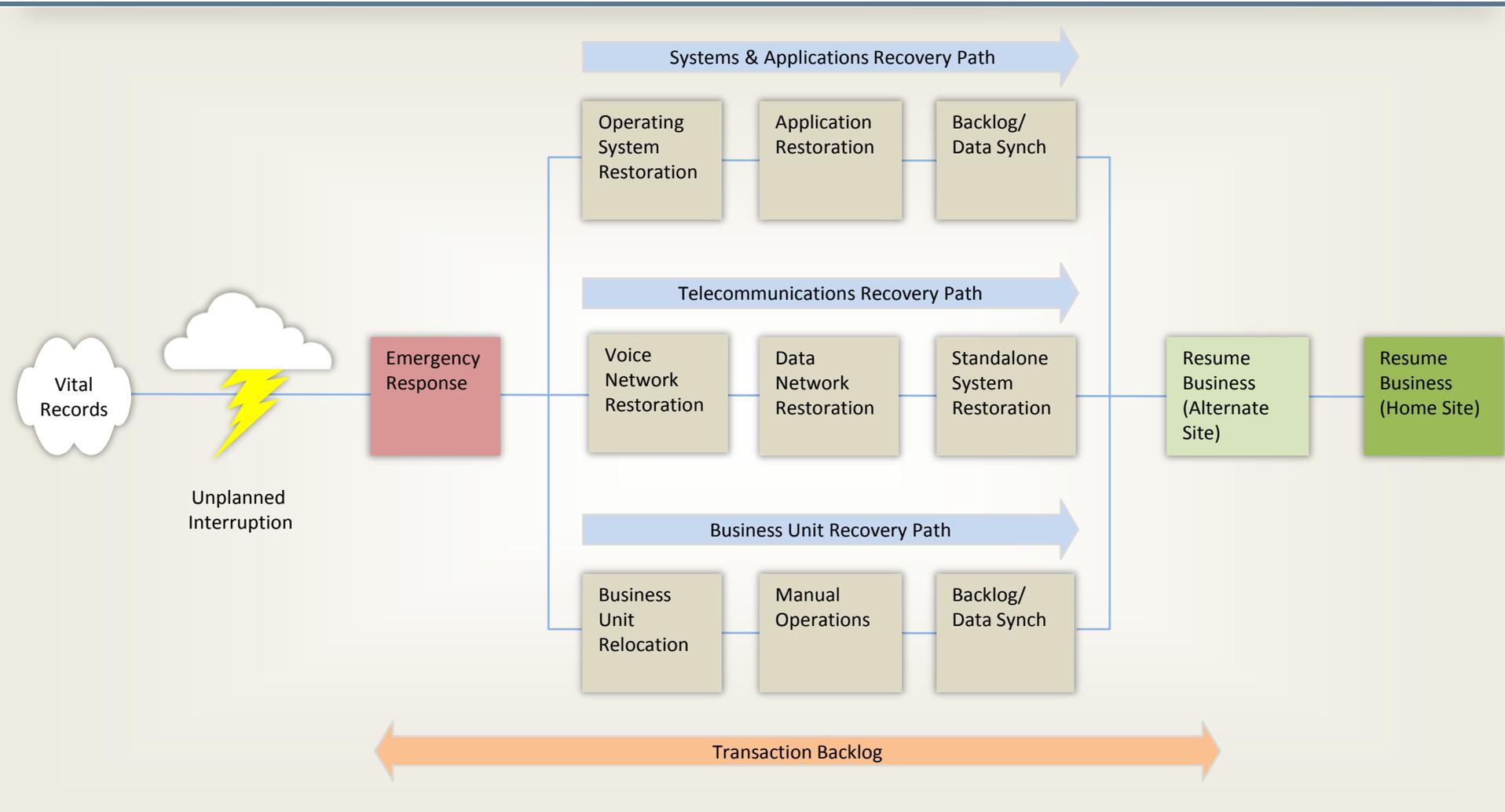


- Ensure continuity of time-critical business processes
- Safeguard corporate assets
- Minimize effects of an interruption
- Train personnel to handle emergency conditions

Respond vs. React



Business Continuity “the Timeline”





Why is Business Continuity Important?

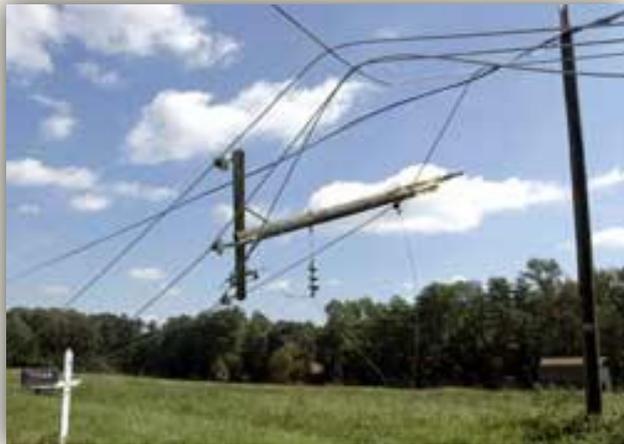
Reason #1: Disasters really do occur



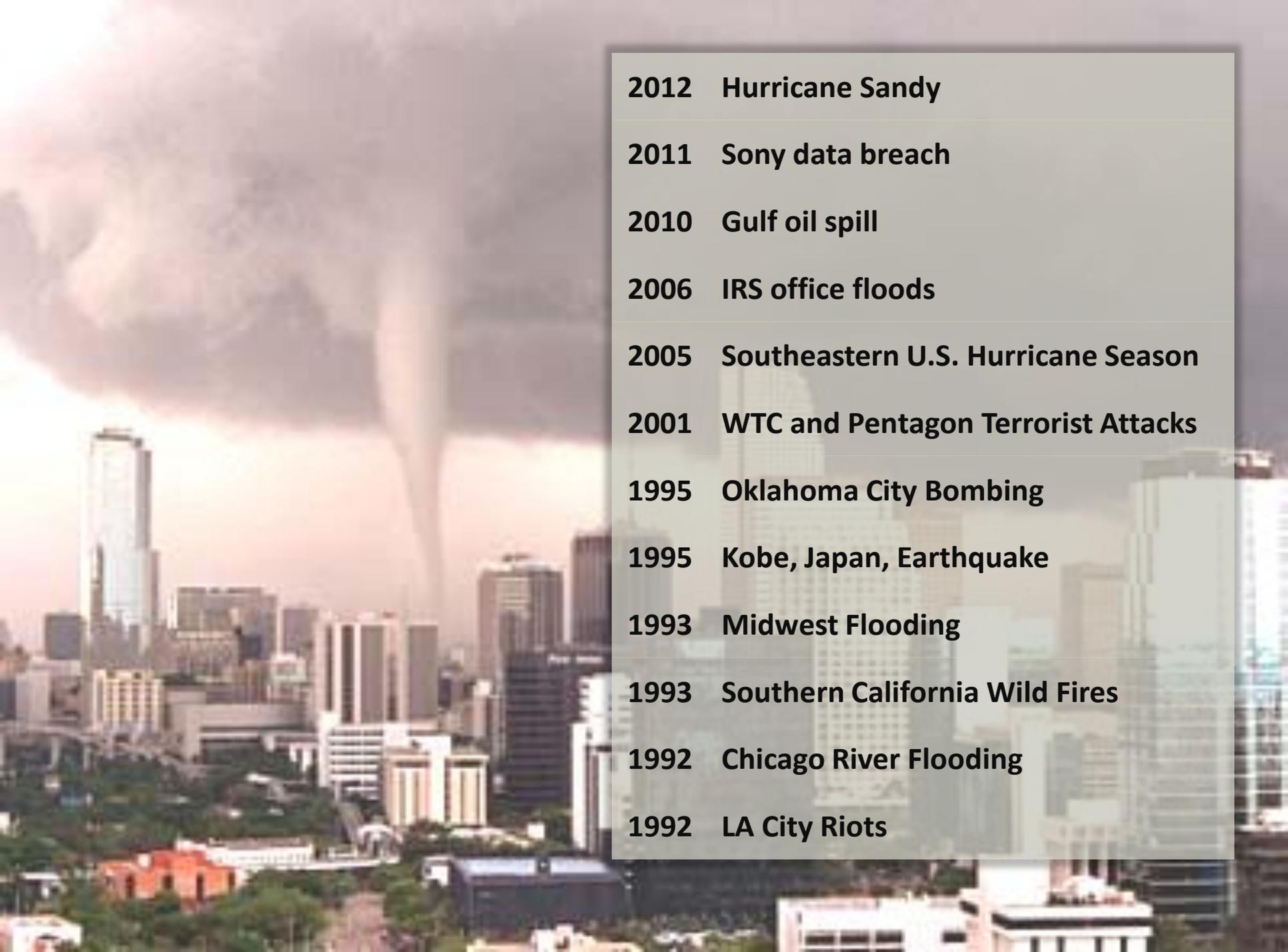
“Unparalleled destruction left an estimated 5 million to 6 million people – out of a population of 7.2 million – without electricity ”



“ Cautioned residents in mountain areas of the potential for fast-moving landslides ”



“ Loss of electricity at key treatment plants or pumping stations also could threaten the health of people who drink the water ”



- 2012** Hurricane Sandy
- 2011** Sony data breach
- 2010** Gulf oil spill
- 2006** IRS office floods
- 2005** Southeastern U.S. Hurricane Season
- 2001** WTC and Pentagon Terrorist Attacks
- 1995** Oklahoma City Bombing
- 1995** Kobe, Japan, Earthquake
- 1993** Midwest Flooding
- 1993** Southern California Wild Fires
- 1992** Chicago River Flooding
- 1992** LA City Riots

Reason #2 It's good business

- 43% of businesses that experience a disaster never reopen. 29% of such businesses close within two years, and businesses whose information systems fail due to a disaster lose, on average, 40% of daily revenues. (Contingency Planning & Management)
- Of those businesses that lost their records in a fire, 44% NEVER reopened their doors again, and 30% of those that DID reopen failed to survive beyond three years after the fire. (ARMA)



Costs of Downtime

Revenue

- Direct Loss
- Compensatory payments
- Lost future revenue
- Billing losses
- Investment losses

Financial Performance

- Revenue recognition
- Cash flow
- Lost discounts (A/P)
- Payment guarantees
- Credit rating
- Stock price

Productivity

Number of employees affected x hours out x burdened hourly rate

Damaged Reputation

- Customers
- Suppliers
- Financial markets
- Business Partners

Other Expenses

- Temporary employees
- Equip rentals
- Overtime
- Shipping
- Travel
- Legal obligations

Reason #3: It's the law

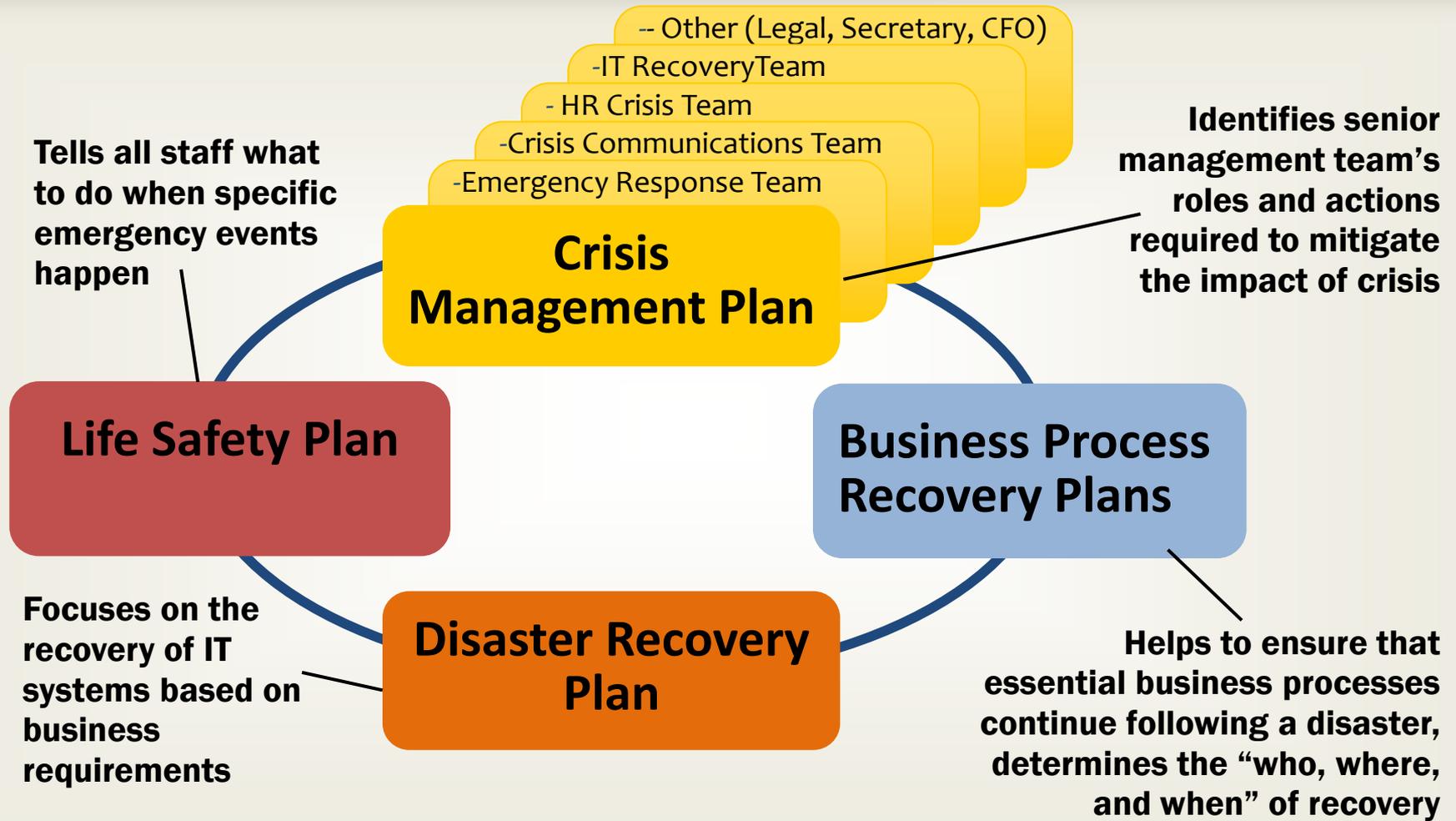
- Banking Circulars
- Banking Bulletins
- HIPAA Regulations
- FFIEC Regulations
- Amendment to Securities and Exchange Act 1934
- Executive Orders
- Sarbanes-Oxley Regulations



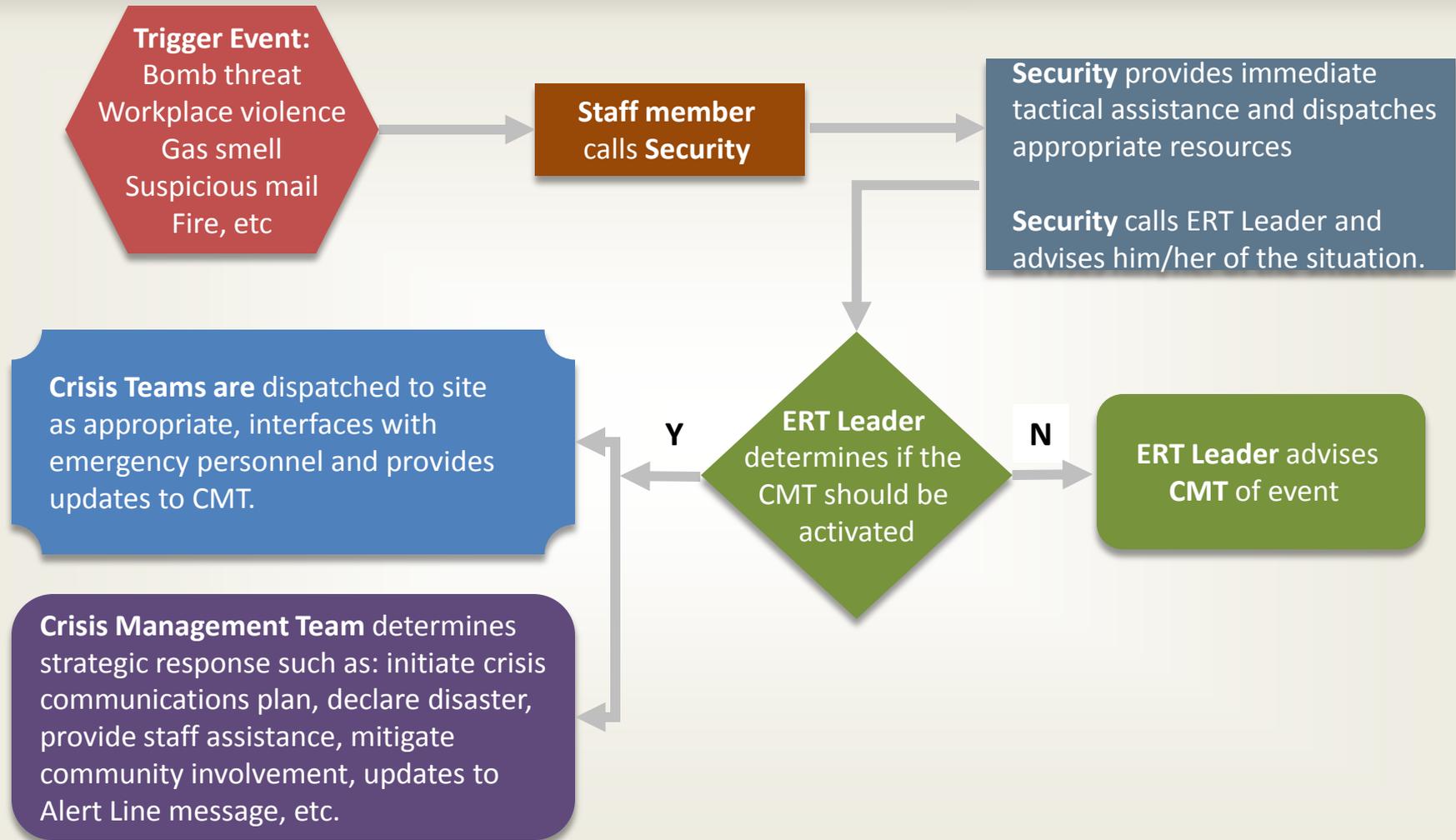


What Types of Plans are Needed?

Four Types of Plans Used at Time of Disaster



Initial Emergency Response





Crisis Management and Life Safety must integrate with Business Recovery and Disaster Recovery Plans

“Well, thank God we all made it out in time. ...
'Course, now we're equally screwed.”



What is the Process for Creating Business Recovery Plans?

Business Recovery Planning Overview



Business Recovery Planning Overview

– Framework and Governance



Create BCM
Framework and
Governance

- Identify regulatory and competitive requirements
- Define Roles and responsibilities
- Develop policy
- Create Governance Document which provides the authority and guidance necessary for effective planning

Business Recovery Planning Overview

- Understanding the Organization



Understanding the organization

- Perform Business Impact Analysis (BIA) - Analyze all processes and the impact a disaster will have on them
- Gather recovery requirements
- Identify and measure known risks to recovery

BIA:

The Business Impact Assessment Process

Purpose of BIA

- Prioritize the Recovery of Business Processes and Applications over time by:
 - Assessing Operational Impacts
 - Unfulfilled Customer Requirements
 - Legal and Regulatory
 - Corporate Image
 - Assessing Financial Impacts
 - Money Management
 - Income/Revenue
 - Delayed or Duplicate Processing
 - Regulatory / Contractual
 - Mapping Business Dependencies
- Identify Business Process Peak Periods

BIA Process

- Customized questionnaires
- Interview sessions (Group or Individual)
- Data analyzed and processes prioritized



Identifying Recovery Requirements

Business Process

Security

Transportation

Vital Records

Other Services

Facility

Equipment

Travel / Lodging

People

Applications

Risk Assessment

Types of Risk Identified by Business Continuity Planning Process

- Physical Site Risk
- Operational / Process Risk
- Vendor Risk
- Risks to Recovery

Risk Management

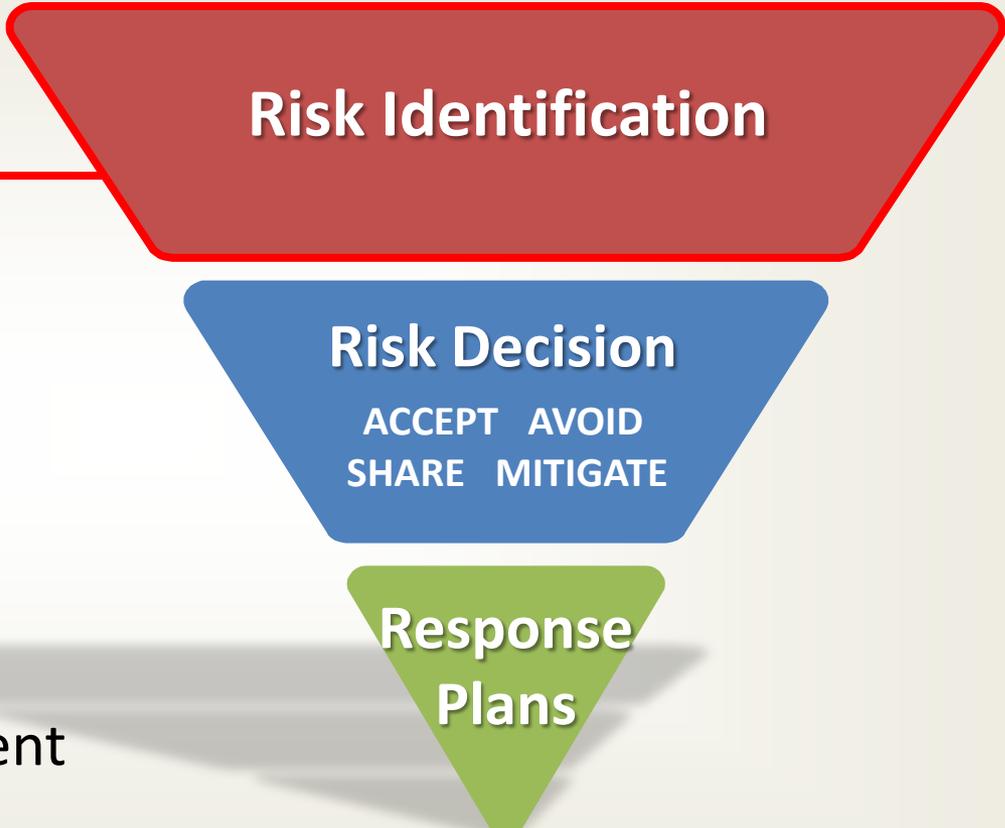
How do I know
which risks to focus on?

Use **LIP** method:

Likelihood or probability
of a specific event

Impact that event will
have, direct and indirect

Preparedness for that event



Risk Identification

Risk Decision
ACCEPT AVOID
SHARE MITIGATE

**Response
Plans**

What do I do about Risk?

- Accept the Risk or
- Eliminate the risk
- Transfer the risk or
- Mitigate the risk



How Do I Mitigate Risk?

- Vital Records Management
 - Electronic backups
 - Paper backups
- Secure Physical Site
- Vendor Management
- Eliminate Single Points of Failure
- Know your neighbors

Business Recovery Planning Overview

- Determining Recovery Strategies

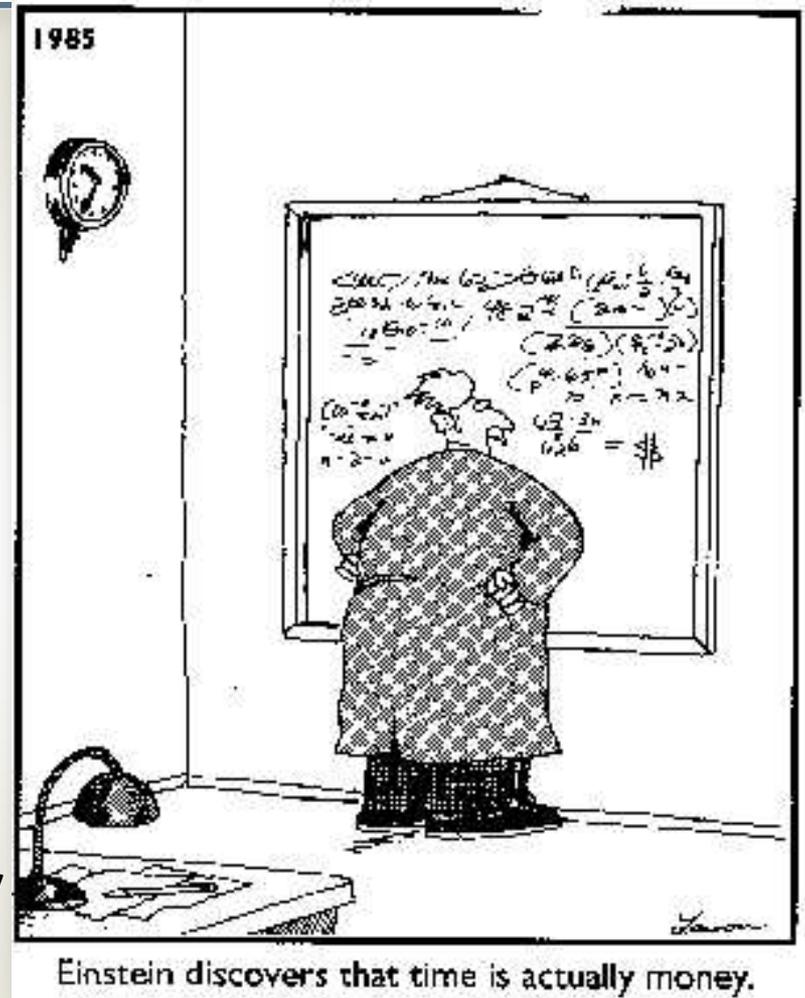
- Analyze recovery requirements
- Determine recovery alternatives and costs
- Select recovery strategies



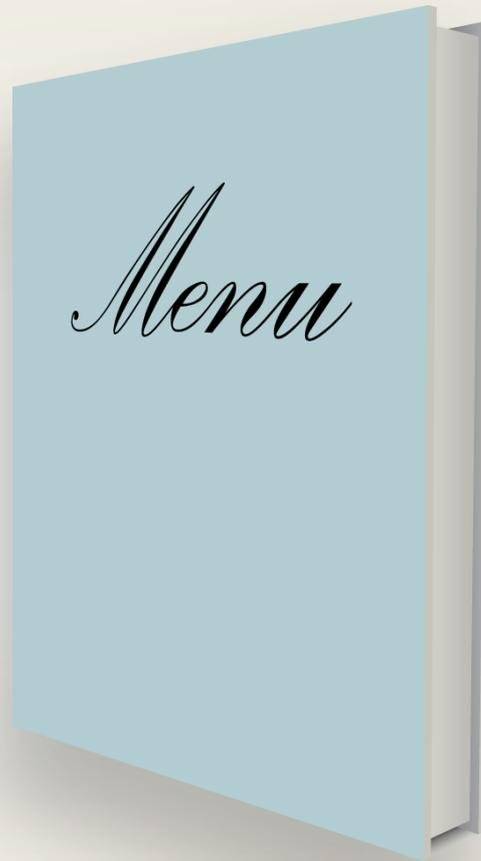
Determining
Recovery
strategies

Time is money

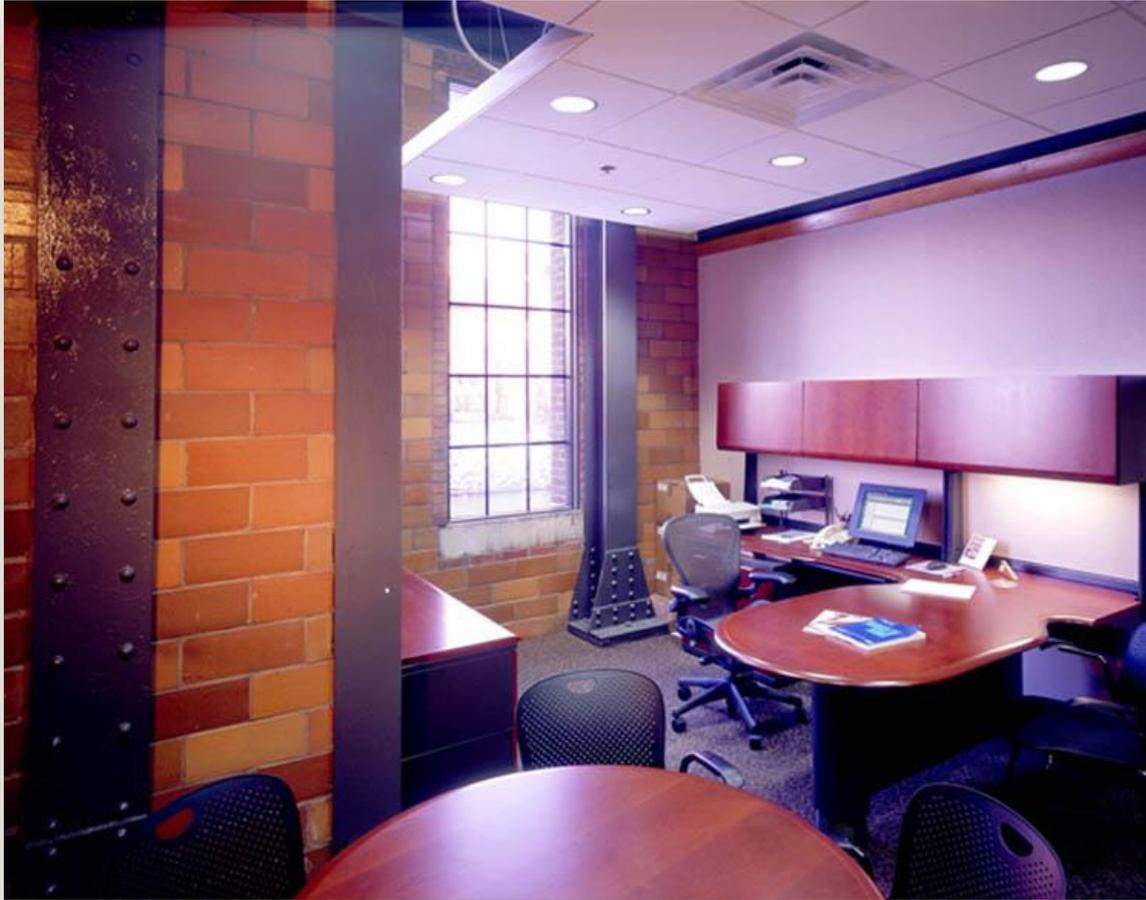
- Short recovery times cost more money
- Leisurely recovery times cost less money
- Continuous, redundant operations require changes to production environment and money



Types of Recovery Strategies



Hot Site – ready to go



- Electricity
- Security
- Network (voice/data)
- Furniture
- PC
- Phone
- Data
- Hardware

Warm Site – nearly ready to go



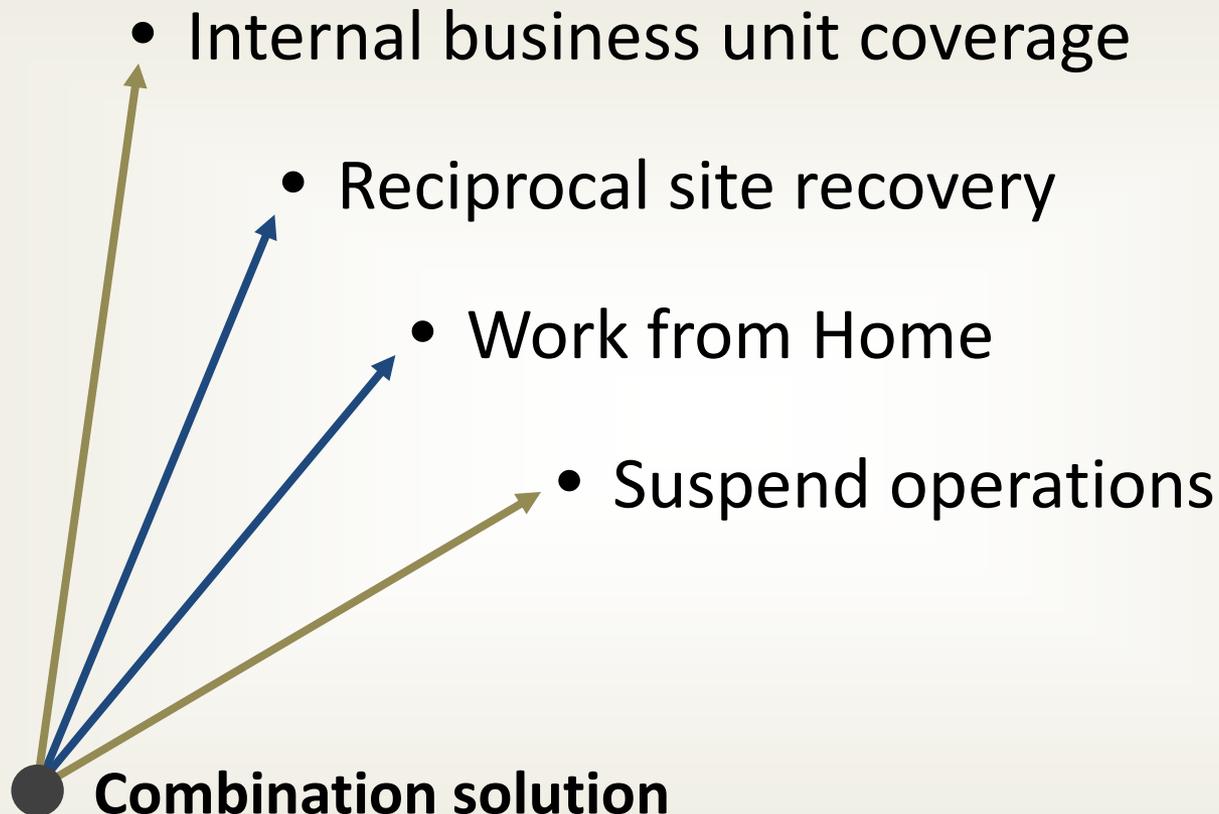
- Electricity
- Security
- Network (voice/data)
- Furniture
- PC
- Phone
- Data
- Hardware

Cold Site – blank slate



- Electricity
- Security
- Network (voice/data)
- Furniture
- PC
- Phone
- Data
- Hardware

Other Recovery Solutions



Your recovery strategy should not be a secret....



Business Recovery Planning Overview

- Developing and Implementing a Response Plan

- Detailed recovery plans are documented
- Recovery strategy is implemented / prestaged

Developing and
implementing
a response
plan

Why we have a written plan

- Safeguard human life
- Minimize critical decisions in a time of crisis
- Reduce dependency on specific personnel
- Minimize loss of data
- Facilitate timely recovery of business processes
- Minimize loss of revenue/customers
- Maintain shareholder value
- Maintain public image and reputation

Answers are in your plan

How do I contact my staff ?

**How do I get supplies
and a PC to start
working again?**

**How do I
contact my
customers?**

**The Press keeps
asking me so
many questions...
What do I tell them?**

**All my files
were destroyed...
what do I do now?**

Elements of a BRP

- Where do I go? What do I do today? What do I do in 3 days? What do tell my employees? Who is in charge?
 - Disaster Declaration Procedures
 - Emergency Evacuation Procedures
 - Detailed Task Lists over time (what to do on day 1, day 2, day 3 etc)
 - Notification Procedures
 - Contact information for all internal and external dependencies
 - Recovery locations (primary and secondary)
 - Team leaders and alternates
 - Manual workarounds and work procedures
- This may be the only document the Business Process Manager has at time of disaster

**The Plan must be
easy to understand**



Business Recovery Planning Overview

- Exercising, maintenance and review

An orange graphic element consisting of a quarter-circle shape on the left side, transitioning into a rectangular shape on the right. The text is centered within this shape.

Exercising,
maintenance
and review

- Provide recovery teams with the opportunity to rehearse their role
- Answers the question: Will this really work?

Types of Exercises and Frequency

- Dependent upon business impact

Business Impact Ratings	Min. Acceptable Type of Exercise	Minimum Exercise Frequency
High	Simulation Exercise	Within 12 Months of last exercise
Medium	Walk Through Exercise	Within 12 Months of last exercise
Low	Talk Through Exercise	Within 12 Months of last exercise

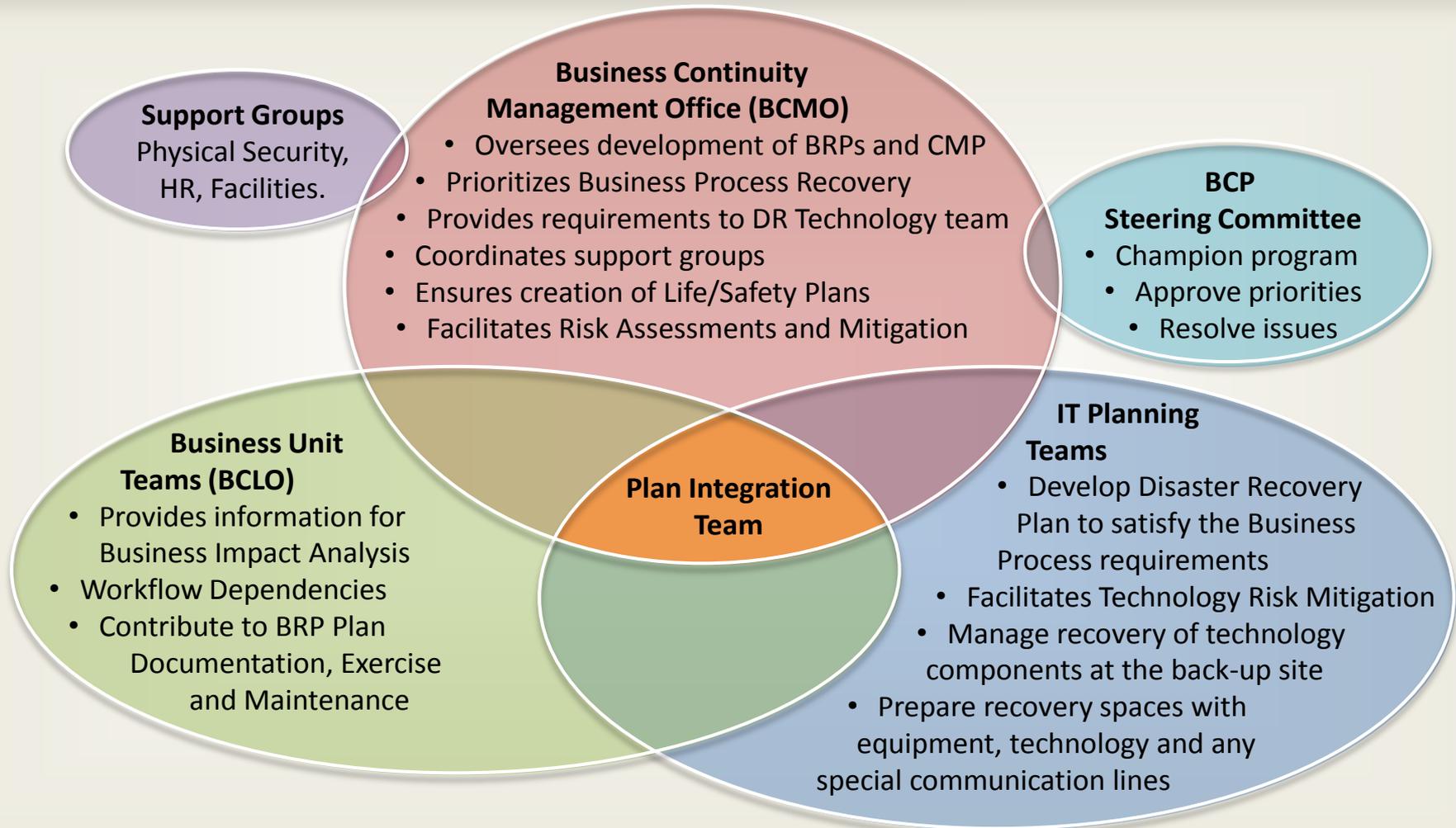
Business Recovery Planning Overview





Who Does What?

Planning roles & responsibilities



Key Messages

- This is a process that mitigates and/or reduces risks
- This is not a project, but rather an on-going process that touches every part of the organization
- BCP requires the cooperation of all the lines of business

Helpful Resources

- DRJ *Generally Accepted Practices* (GAP document) found at drj.com
- Ask the EAB found at drj.com
- ISO 22301: 2012 *Societal security – Business continuity management systems – Requirements*
- Association of Contingency Planners – Old Dominion Chapter
- jeandrowe@gmail.com

The views expressed in this presentation are my own and do not necessarily reflect the views of Verisign Inc.

***Jean D. Rowe, CBCP, MBCI, CDCP
jeandrowe8@gmail.com***



Virginia Information Technologies Agency

Preview Draft 2012 Commonwealth Of Virginia Information Security Annual Report

Michael Watson, CISO



Slides have been
intentionally omitted





Virginia Information Technologies Agency

Upcoming Events





IS Orientation

When: Thursday, June 6, 2013

Time: 1:00 pm to 3:00 pm

Where: CESC , Room 1221

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>

Next IS Orientation will be held on Sept 5, 2013



Information Security System Association

ISSA

DATE: Wednesday, April 10, 2013

LOCATION: Maggiano's Little Italy

11800 West Broad Street, #2204, Richmond, VA 23233

TIME: 11:30 - 1:00pm. Presentation starts at 11:45.

Lunch served at 12.

COST: ISSA Members: \$20 & Non-Members: \$25

SPEAKER: Mikel Draghici

TOPIC: Mobile Security

More info located here: <http://centva.issa.org/central-va-issa-feb-2013-meeting/>



DSIA Training

Network Vulnerability Assessment

Instructor: John Tannahill

Date: May 7, 2013

Time: 8:15-4:45

**Location: James Monroe Building
DOE Conf. Rm., 22nd FL**

Cost: \$ 160.00

Register: <https://hrtraining.doa.virginia.gov>



DSIA Training

Information Assurance, Application Security & Project Management Integration

Instructor: Albert Marcella, Jr.

Date: May 8, 2013

Time: 8:15-4:45

**Location: James Monroe Building
DOE Conf. Rm., 22nd FL**

Cost: \$ 160.00

Register: <https://hrtraining.doa.virginia.gov>



Future ISOAG Dates

May 1 **1:00 – 4:00 pm @ CESC**
Keynote Speaker: Todd Dergenski, ODU
on "Identity Management"

June 5 **1:00 – 4:00 pm @ CESC**
Keynote Speaker: Zac Allen and Andrea Ross, DOC
on "KANBAN Project Management"

July 10 **1:00 – 4:00 pm @ CESC**
Keynote Speaker: Rosario Igharas, Virginia529
on "Data Management"

ISOAG meets the 1st Wednesday of each month in 2013



Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

CommonwealthSecurity@VITA.Virginia.Gov



ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

Apr 3, 2013



NORTHROP GRUMMAN

Slides have been
intentionally omitted



ADJOURN

