

**MetricStream**

**MetricStream**

**GRC**

**SUMMIT 2013**

---

**MIDDLE EAST**

---

October 29 - 30, 2013 | Dubai, UAE

# Implementing Business Continuity & Disaster Recovery Management Programs

---

[www.GRC-Summit.com/MEA2013](http://www.GRC-Summit.com/MEA2013)

**MetricStream**  
**GRC**  
**SUMMIT 2013**  
**MIDDLE EAST**  
October 29 - 30, 2013 | Dubai, UAE

# The Rising World of Business 'e-continuity'...

*IT and Security  
Threats from DDOS,  
Outages*

## The Telegraph

HOME NEWS WORLD SPORT FINANCE COMMENT BLOGS CULTURE TRAVEL

Technology News | Technology Companies | Technology Reviews | Video Games

HOME » TECHNOLOGY » TECHNOLOGY NEWS

Foreign hackers 'putting UK firms out of business'

**U.S. suffered \$119 billion in disaster-related losses in 2012**

FT TRADING ROOM

US markets crippled by Nasdaq outage

GoDaddy Goes Down, Takes Half The Internet With It

*Business Risk from  
Supply Chain  
Disruption,  
Union Strikes*



*Environmental  
Threats  
Tsunami, Fires  
Storms*

MetricStream

**GRC**

SUMMIT 2013

MIDDLE EAST

October 29 - 30, 2013 | Dubai, UAE

# Latest E&Y Survey on Global State of InfoSec

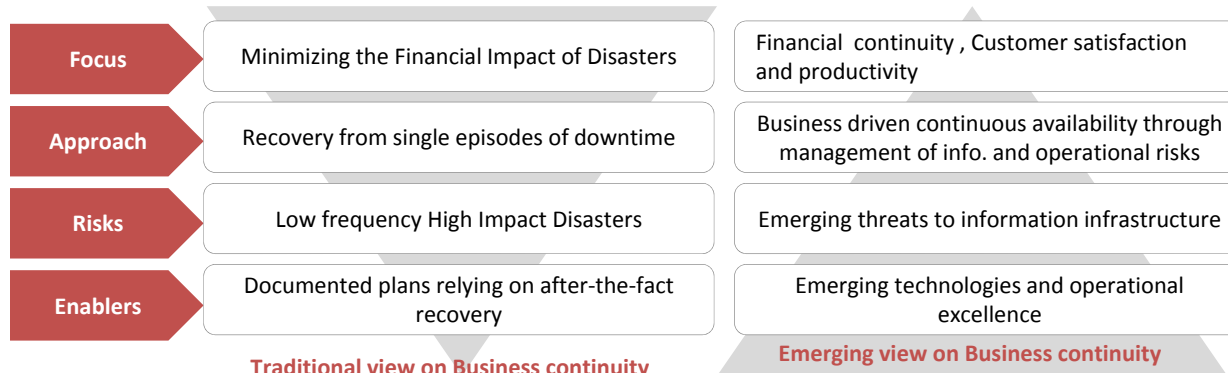
Which of the following information security areas are defined as "top priorities" over the coming 12 months?



# Emerging Business Continuity Environment



**Business requirements have evolved from "recovery" following a disruption to "providing uninterrupted operations"**



Traditional view on Business continuity

Emerging view on Business continuity

*Prerogatives during a disaster . . .*

- Ensure safety of all employees and availability of human resources at all times
- Effective management of public relations
- Ensure network uptime
- Ensure adequate logistics for continued services
- Effectively maintain critical infrastructure
- Ensure minimal downtime for critical systems

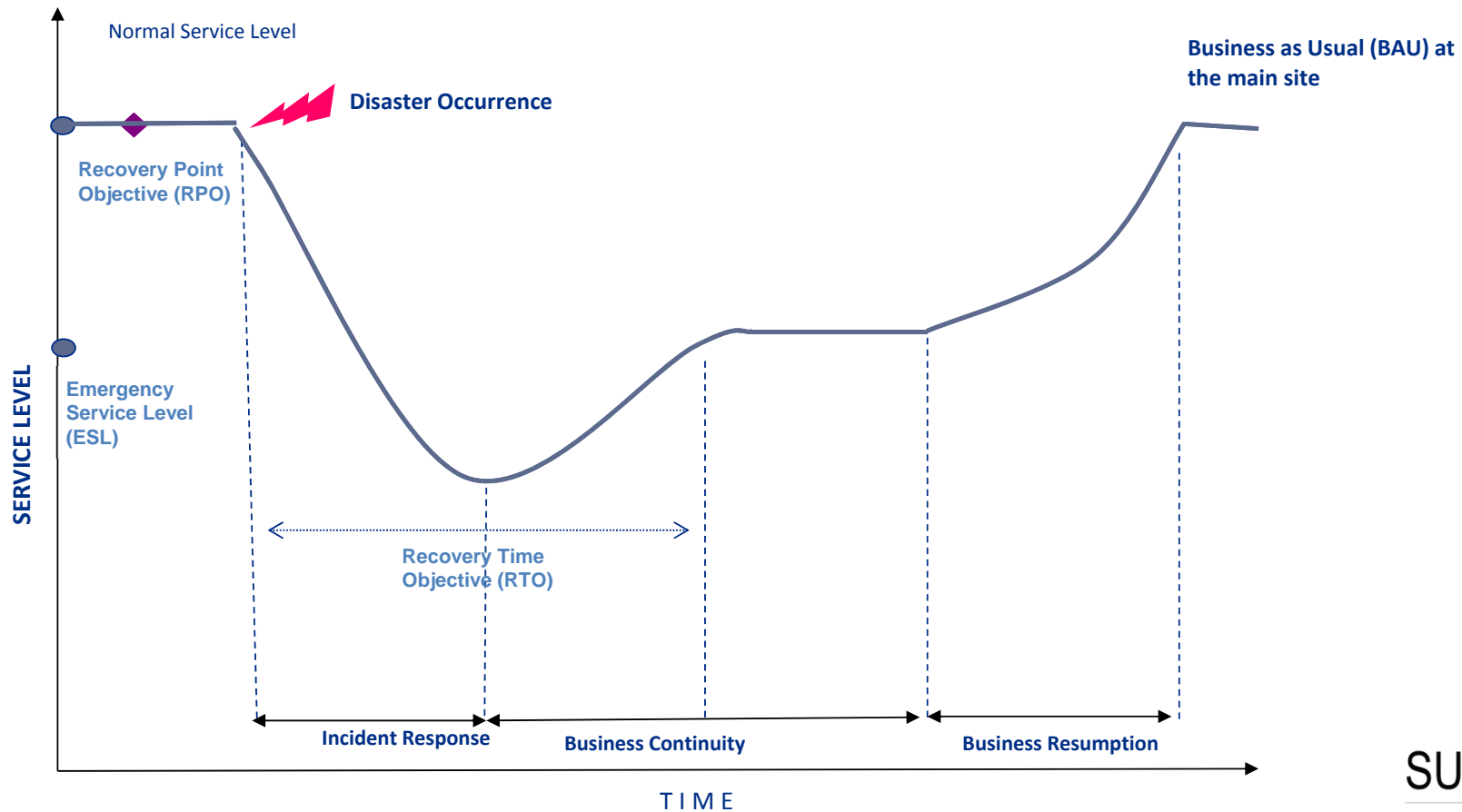
*Hence, BCM solution should cater to...*

Crisis Management plan to enable immediate response actions during disasters

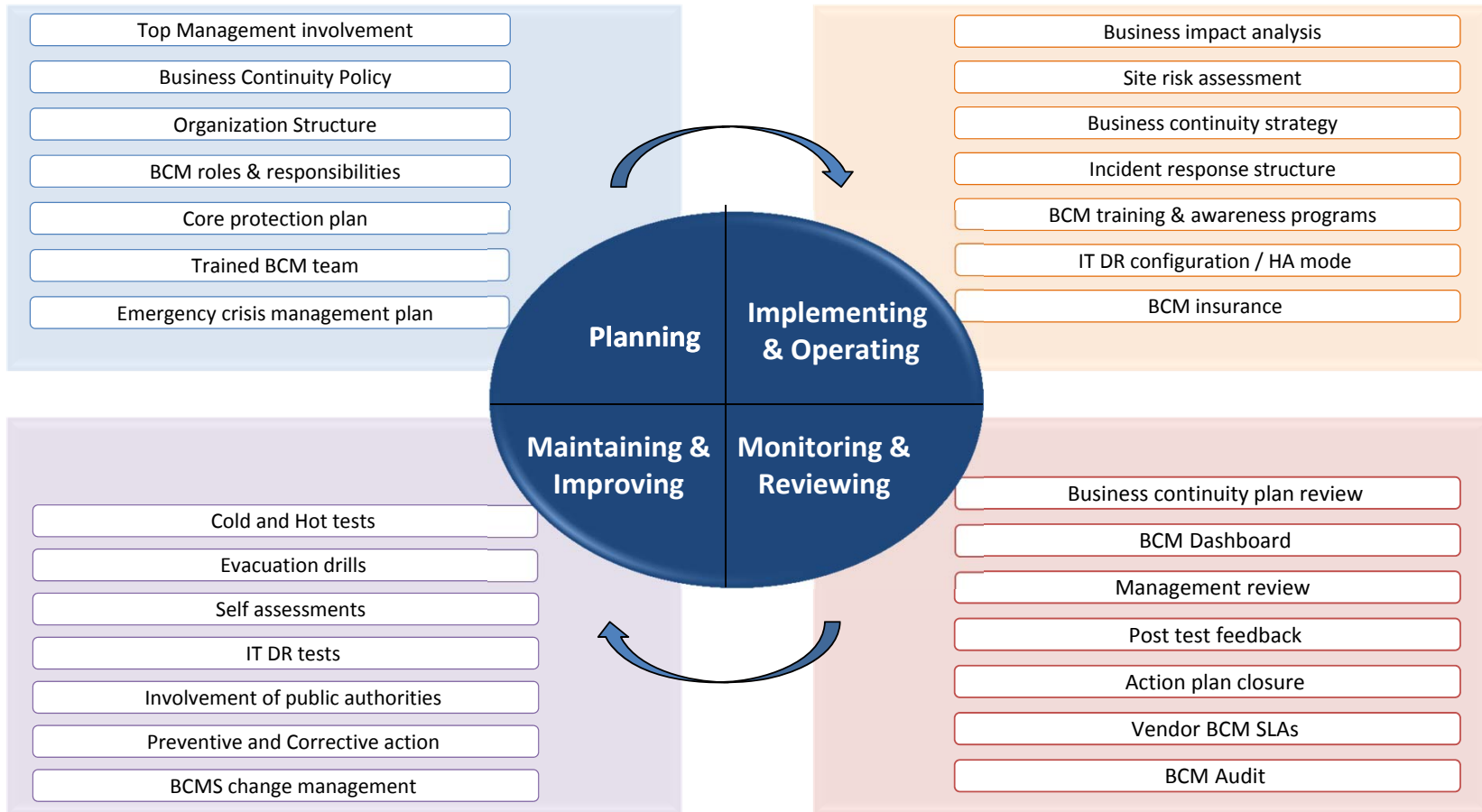
Process, people and infrastructure recovery to manage base business operations

Disaster recovery planning to enable resumption of technology dependent operations

# BCM – Concept Overview

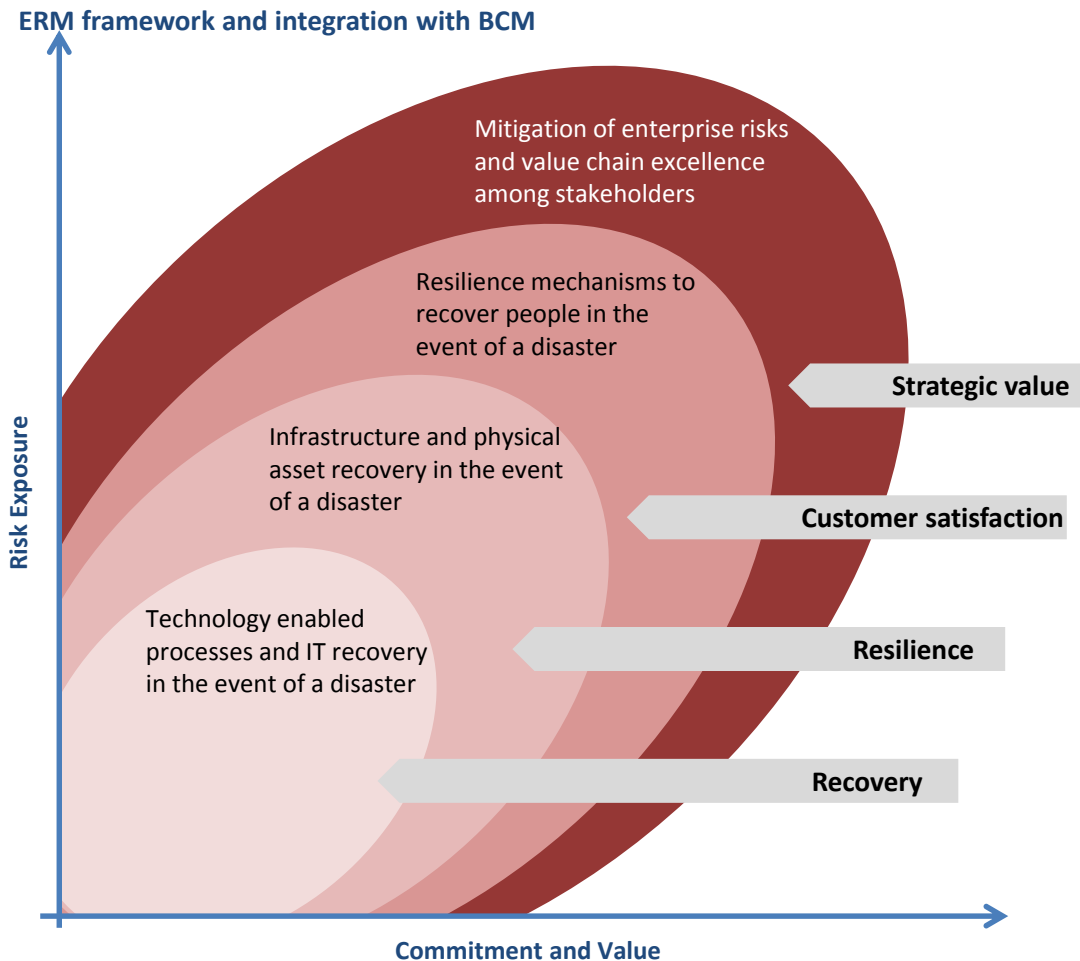


# BCMS Alignment with Standards & Best Practices





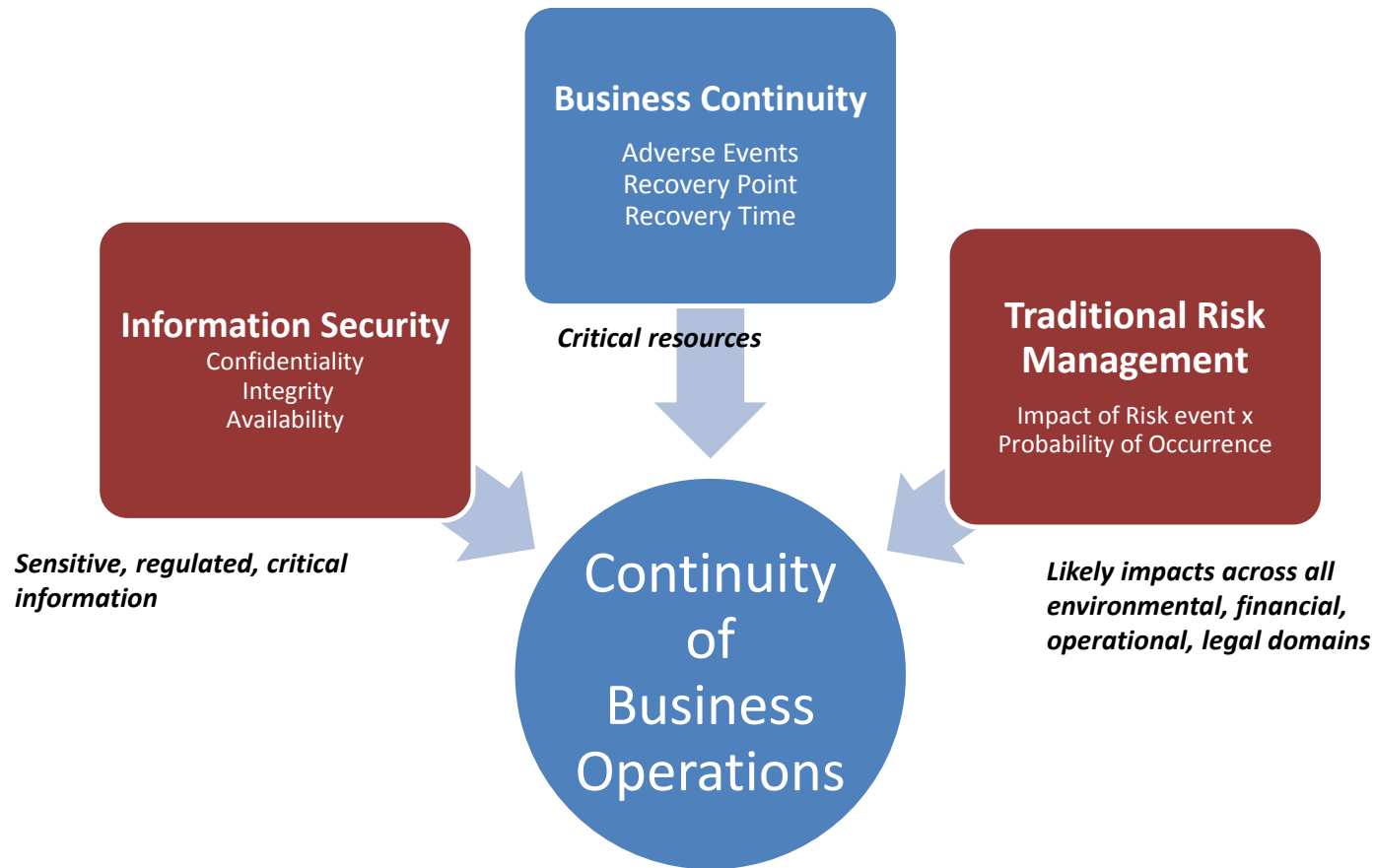
# Enterprise Risk Management – Integral part of BCM Framework



## **Business Continuity Management System integration with the Enterprise Risk Management Framework:**

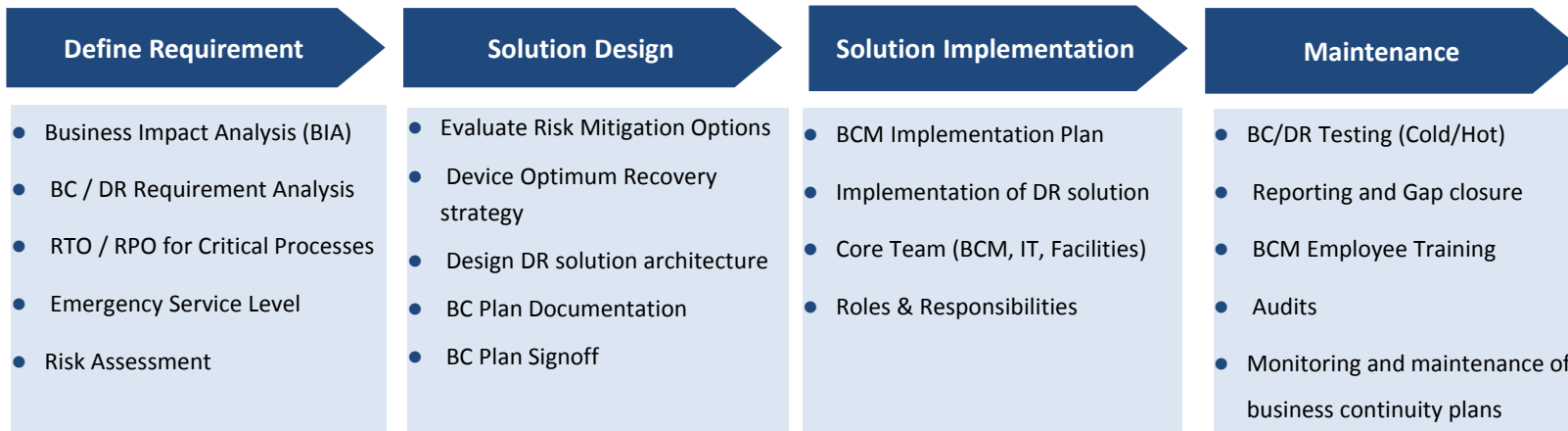
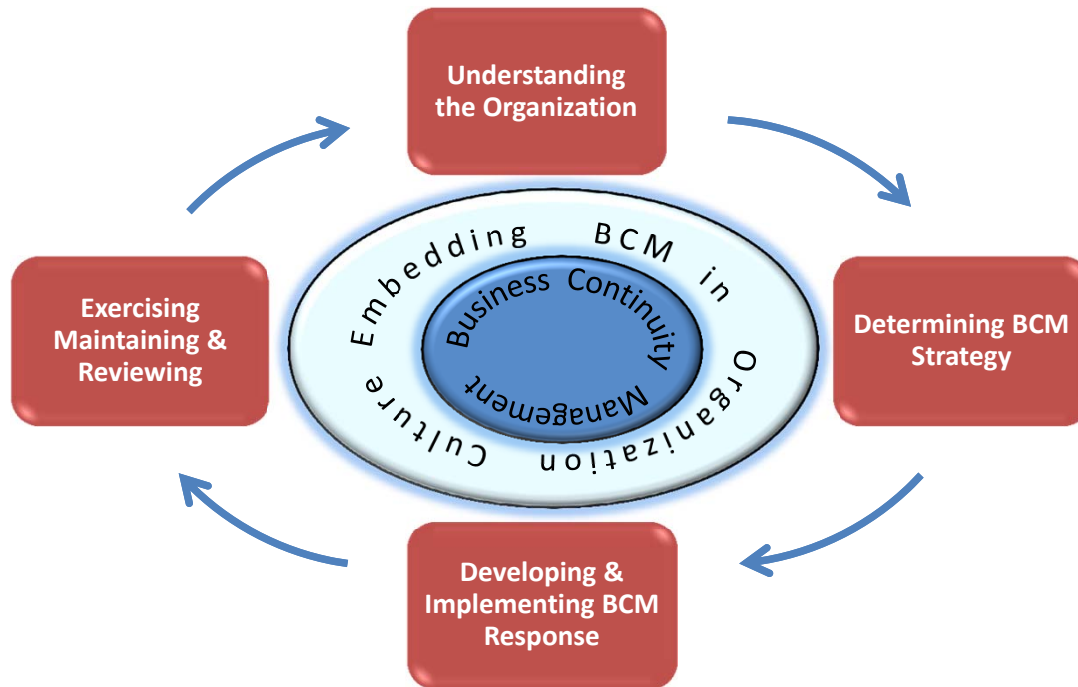
- Central Management of BCM and ERM ensure common direction and consistent understanding of organization risk
- Consistent and unified enterprise-wide risk assessment and evaluation criteria
- Alignment with the strategic imperatives and objectives of the organization

# Different Perspectives, Common Goals

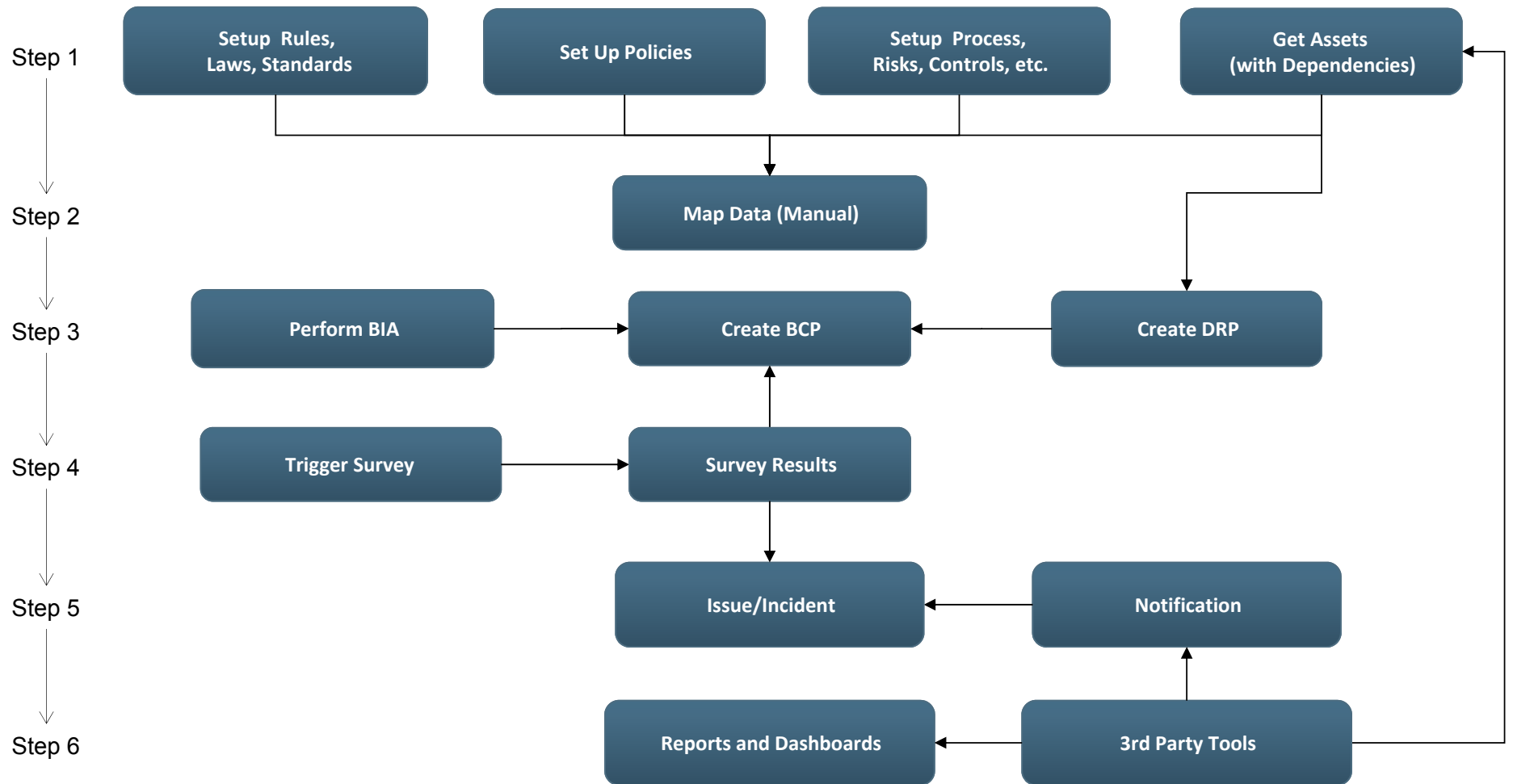


***“ensuring resources necessary to meet critical objectives are available”***

# BCM Solution Design



# MetricStream BCM Solution Flow

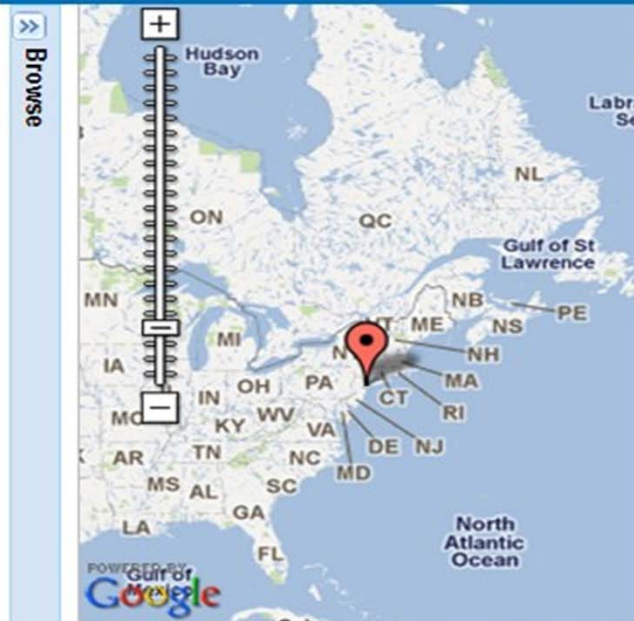




**Risk and BCP Detail By Location**

Report Data as of: 09/28/2011 10:53 AM

Location	No. of Disaster Recovery Plan	No. Of Risks	No. Of BC Plans	No. Of BIA
New York		6	2	1



## Risk Detail Report

Report Data as of: 09/28/2011 10:54 AM

Risk Name	Description	Risk L...	Risk Category	Risk Type
Dam/Levee Fai...	Contingency Plan provides guidance and documen...	Level 1	Technological o...	THREAT
Power/Utility Fa...	In terms of personnel and financial resources, the i...	Level 1	Technological o...	THREAT
Avalanche	In terms of personnel and financial resources, the i...	Level 1	Natural Events	THREAT
Biological	The management has recognized the potential fina...	Level 1	Natural Events	
Hurricane	In terms of personnel and financial resources, the i...	Level 1	Natural Events	THREAT
Tornado	The primary objective of this plan is to establish pol...	Level 1	Natural Events	THREAT

Location	No. of Disaster Recovery Plan	No. Of Risks	No. Of BC Plans	No. Of BIA
New York		2		1

**Disaster Recovery Risk Control Matrix**

Report Data as of: 09/25/2011 03:07 PM

Description	Likelihood	Impact	Action 1	Action 2	Control
Single Disk Failure	Medium	No effect	Replace failed disk in...	Order new disks. Hav...	Monitoring of RAID volumes. Keep replacemen...
Capacity overload	Medium/High	Performance degrad...	Bring on additional s...	Check power load of ...	Monitor capacity
Multiple Disk Failure	Low	No effect (failover)	Replace failed disks i...	Order new disks. Hav...	Monitoring of RAID volumes. Keep replacemen...
Multiple machine fa...	Low	Low effect (failover). ...	Repair machine, repl...	Repair machine, repl...	Monitor machine health
Software failure for ...	Medium	Users will not have a...	Update/repair softwar...	Update/repair softwar...	Update software to latest stable version.
Loss of Internet Co...	Medium	No access to software.	Switch to (hot) backu...	Switch back to primar...	Hot backup T1 connection in place.
Loss of building thr...	Low	No access to software.	Move application to b...	Move back to primary ...	n/a
Data loss	Low	Users will not have a...	Restore data from ho...	No later action neces...	Hot and offsite backups in place.
Power failure (gen...	Low	No access to software.	Move application to b...	Move back to primary ...	Hot backup data center in place.
Local network failure	Low	No access to software.	Repair network / repl...	Replace failed hardw...	Hot backup data center in place as well as hot ...
Software failure	Medium	Low effect or no acce...	Update/repair softwar...	Update/repair softwar...	Update software to latest stable version.
Unauthorised modi...	Low	Low effect on users.	Restore modified con...	Repair security breac...	Determine root vulnerability. Repair vulnerability.

Action Details Report

Filters Done

Report Data as of: 09/25/2011 03:07 PM

Critical Business Acti...	Preventative/Recover...	Resource Requireme...	Recov...	Responsibility	Status	% Com...	Comments	Activity T...
Production Services ...	<ul style="list-style-type: none"> <li>re-assess financial... minimise overheads - ...</li> <li>negotiate with supp...</li> <li>source alternative p...</li> <li>diversify product ra...</li> </ul>	<ul style="list-style-type: none"> <li>put aside cash res...</li> <li>reduce costs where...</li> <li>research new prod...</li> <li>identify alternative p...</li> </ul>	2 weeks	Recovery Time O...	Open	60%	Overhead costs are sti...	BC
Electric Distribution ...	Reassess how we ca... This should be done w... Issue a press release ...	Identify ways we coul... Appoint a customer rel...	~ 1 week	Region M&C Dire...	Closed			BC
Power Generation E...	Assess the damage h...	Plug the oil leak ASAP....	~3-4 w...	Hydro Area Mana...	Open	50%	PR process still under...	BC
Nightly Backup Faile...	Verify MDSS prod back...	Check with Db mgrs o...	~24 hrs	SA & DBA	Closed			DR
Unauthorised modifi...	On initial analysis it wo...	Repair security breach...	~1 week	DBA	Open	30%	Unable to recover cont...	DR
Multiple Disk Failure	Initial assessment rev...	Order new disks. Have...	~24hrs	SA task	Closed			DR
Loss of building thro...	Move application to ba...	Move back to primary d...	~3-4 w...	DR Coordinator	Open	50%	All systems restored. ...	DR



**BCP Risk Register Report**

Done

Report Data as of: 09/25/2011 03:08 PM

Risk ID	Risk (description)	Current ...	Date Rai...	Inherent...	Inherent...	Proxi...	Countermeas...	Resi...	Resi...	Outline Contin...	Status	Links to...	Date ...
RI-...	Hardware Failure...	Jamie O...	09/Dec/...	High	High	Medi...	Deepak Babaria	Low	Low	Alternate Reco...	Closed	RI-3453...	16-D...
RI-...	Disruption in the ...	Helen B...	10/Sep/...	Medium	High	Immi...	Balaram Nair	Medi...	Medi...	Initiate the Pri...	Open	RI-3435...	
RI-...	Power failure (ge...	Chris M...	08/Aug/...	Low	High	Long ...	Ted Bailey	Low	Low	Move applicati...	Closed		08-M...

Browse: Processes

Related Information

# ISO 22301

MetricStream has recently added a BCM content pack built around the International Standards Organization (ISO) 22301 requirements, which can be easily tailored by the organization for their specific needs.

This includes the following based on ISO 22301 requirements:

- Policies
- Processes
- Controls
- Guidelines
- Reporting Templates & Dashboards
- Checklists
- eLearning on ISO 22301

The screenshot shows the MetricStream web application interface. At the top, it says "MetricStream" and "Welcome: MetricStream Administrator". There are navigation tabs for "Issues", "AppStudio", "Compliance", "My Tasks", "Risks", "IT GRC", "RSM TSM", "My Task", "My Issues", "MGS", "Metrics Reporting", "RCSA", "IAT", "RSM Admin", and "Adm". Below these are more tabs: "Assignments", "Activities", "Alerts", "Calendars", "Configuration Parameters", "Dashboards", "Data Tables", "Infolets", "List of Values", "Reports", "Organizations", "Roles", and "Ve". The main content area is titled "BCM Regulation or Standard Content Browser". It shows a table with columns: "Regulation", "Citation or Section", "Citation Guidance", and "Control Title". The table lists several regulations, including ISO/IEC 17799, ISO/IEC 27001, ISO/IEC 27002, ISO 15489-2, and ISO/IEC 13335-5. The "Citation Guidance" column for ISO 15489-2 is expanded, showing detailed text about the purpose of the step and requirements for records management.

Regulation	Citation or Section	Citation Guidance	Control Title
ISO/IEC 17799 Code of Practice for Infor...	§ 5.1.1	Management should commit to and demonstrate s...	Leadership and high level objectives
ISO/IEC 27001 Information Security Man...	§ 4.1, 5.1, Annex A...	An Information Security Management System shoul...	Leadership and high level objectives
ISO/IEC 27002 Code of practice for infor...	§ 5.1.1	Management should commit to and demonstrate s...	Leadership and high level objectives
ISO 15489-2: 2001, Information and Doc...	§ 3.2.3, § 3.2.4, § ...	The purpose of this step is to develop a conceptua... § 3.2.4 says that requirements for records manage...	Analyze organizational objectives, functions, and act...
ISO 15489-1:2001, Information and Doc...	§ 4.1(b)		Analyze organizational objectives, functions, and act...
ISO/IEC 13335-5 Information technology ...	¶ 7.2, ¶ 8, ¶ 9, ¶ 9.1...	¶ 7.2 Identification Process. A recommended proce... When considering network connections, all those p... • review the general security requirements for netw... • review the network architectures and applications ... • identify the type or types of network connection that... • review the characteristics of the networking propo... • determine the related types of security risk, where ... • identify the references to the potential safeguard a... • document and review security architecture options... • prepare to allocate tasks for the detailed safeguar... ¶ 8 Review Corporate IT Security Policy Requireme... For example, such a policy could state that: • availability of certain types of information or servic... • no connections via dial-up lines are permitted, • all connections to the Internet must be made throu... • a particular type of security gateway must be used, • no payment instruction is valid without a digital sig...	Analyze organizational objectives, functions, and act...

# ISO 22301 Screenshots

- ISO 22301
  - Requirements
    - Business continuity plans
    - Control of documented informat
    - Business impact analysis
    - Determination and selection
    - Recovery
    - Incident response structure
    - Evaluation of business continu
    - Scope of the BCMS
    - Creating and updating
    - Risk assessment
    - Establishing resource requirem
    - Legal and regulatory requireme
    - Leadership and commitment
    - Protection and mitigation
    - Warning and communication

**Name\***  
Scope of the BCMS

**Section No/Citation \***  
4.3.2

**Area of Compliance\***  
ISO 22301

**Details** | Related To | Additional Details

**General**

**Description**

The organization shall  
a) establish the parts of the organization to be included in the BCMS,  
b) establish BCMS requirements, considering the organization's mission,

**Classification**  
Business Practice

**Type**  
Key Requirement

**Impact and Penalties**  
Insignificant

**Penalties for Non-Compliance**

**Ownership and Security**

**Owner Organizations\***  
MetricStream, Branch Banking, Branch Sales

**Level 1 Approver**

**Restrict Access To\***  
No Restriction

**Validity (Dates)**

**Valid From** **Valid Until**

RTF Editor - MetricStream Enterprise Governance Risk Complian...

http://msi-demo1.metricstream.com/itgrc/metricstream/system/Advancedricht

The organization shall  
a) establish the parts of the organization to be included in the BCMS,  
b) establish BCMS requirements, considering the organization's mission, goals, internal and external obligations (including those related to interested parties), and legal and regulatory responsibilities,  
c) identify products and services and all related activities within the scope of the BCMS,  
d) take into account interested parties' needs and interests, such as customers, investors, shareholders, the supply chain, public and/or community input and needs, expectations and interests (as appropriate), and  
e) define the scope of the BCMS in terms of and appropriate to the size, nature and complexity of the organization.

When defining the scope, the organization shall document and explain exclusions; any such exclusions shall not affect the organization's ability and responsibility to provide continuity of business and operations that meet the BCMS requirements, as determined by business impact analysis

# ISO 22301 Screenshots

- ISO 22301
  - Requirements
    - Business continuity plans
    - Control of documented informat
    - Business impact analysis**
    - Determination and selection
    - Recovery
    - Incident response structure
    - Evaluation of business continu
    - Scope of the BCMS
    - Creating and updating
    - Risk assessment
    - Establishing resource requirem
    - Legal and regulatory requireme
    - Leadership and commitment
    - Protection and mitigation
    - Warning and communication

<b>Name*</b> Business impact analysis	<b>Area of Compliance*</b> ISO 22301
<b>Section No/Citation*</b> 8.2.2	
<b>Details</b>   Related To   Additional Details	
<b>General</b>	
<b>Description</b> The organization shall establish, implement, and maintain an evaluation process for determining continuity and recovery priorities, objectives and targets.	
<b>Classification</b>	<b>Type</b>
<b>Impact and Penalties</b>	<b>Penalties for Non-Compliance</b>
<b>Ownership and Security</b>	
<b>Owner Organizations*</b> MetricStream, Branch Banking, Branch Sales	
<b>Level 1 Approver</b>	
<b>Restrict Access To*</b> No Restriction	
<b>Validity (Dates)</b>	
<b>Valid From</b>	<b>Valid Until</b>
<b>Modify/Review/Approve</b>	
<b>Action*</b>	

RTF Editor - MetricStream Enterprise Governance Risk Compliance Platfor...

http://msi-demo1.metricstream.com/itgrc/metricstream/systemi/Advancedrichtexteditor?

The organization shall establish, implement, and maintain a formal and documented evaluation process for determining continuity and recovery priorities, objectives and targets. This process shall include assessing the impacts of disrupting activities that support the organization's products and services.

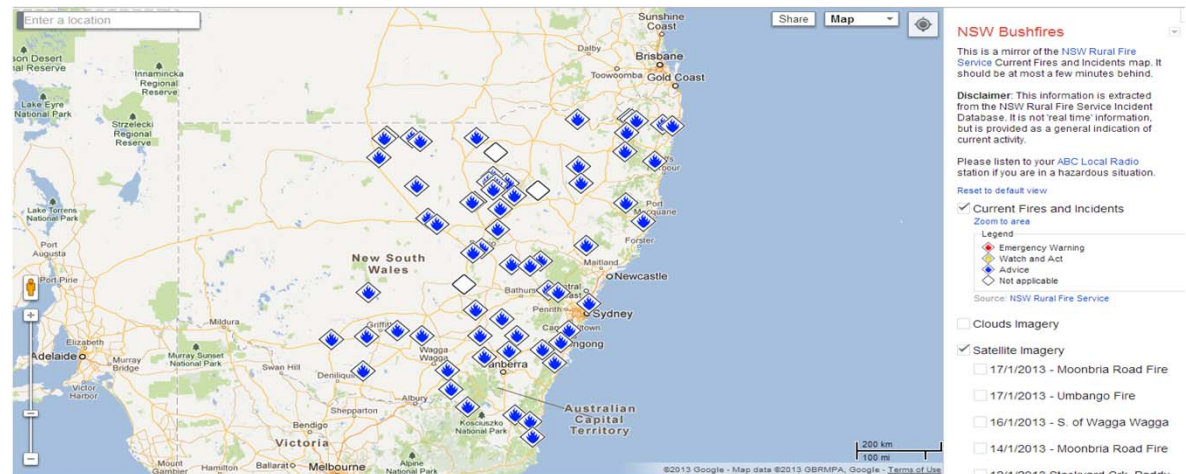
The business impact analysis shall include the following:

- a) identifying activities that support the provision of products and services;
- b) assessing the impacts over time of not performing these activities;
- c) setting prioritized timeframes for resuming these activities at a specified minimum acceptable level, taking into consideration the time within which the impacts of not resuming them would become unacceptable; and
- d) identifying dependencies and supporting resources for these activities, including suppliers, outsource partners and other relevant interested parties.

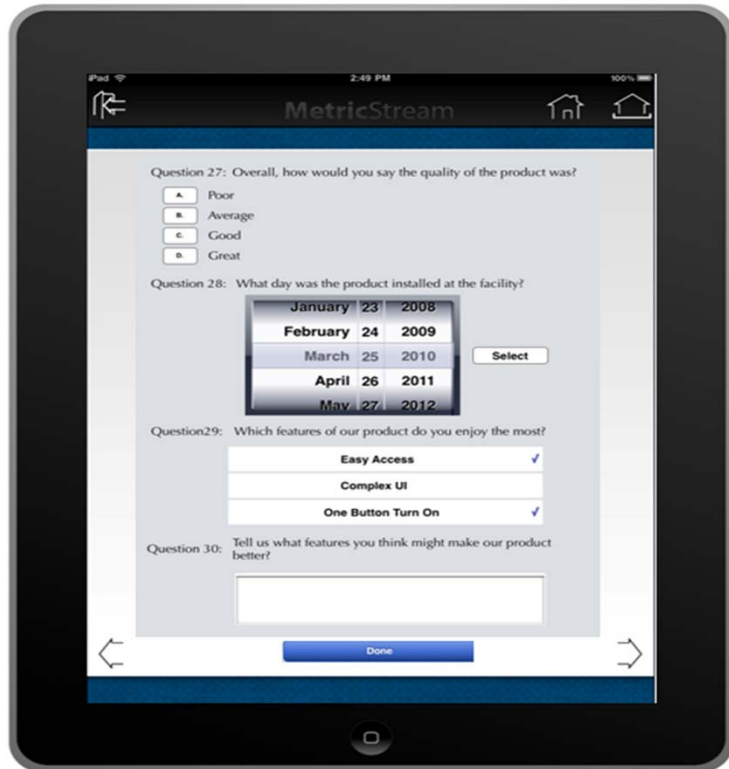
100%

# Social Media for Situational Awareness

- Track Social Media platforms like:
  - Twitter
  - Facebook
  - Pinterest
  - Google (Google +, Youtube, Crisis Map etc.)
- Correlate Information with Organizational Assets / Facilities / Risks
- Trigger / Update Incident Management Workflows & Notifications
- Real-Time Reports & Dashboards
- Leverage Social Media for Communications During Emergencies

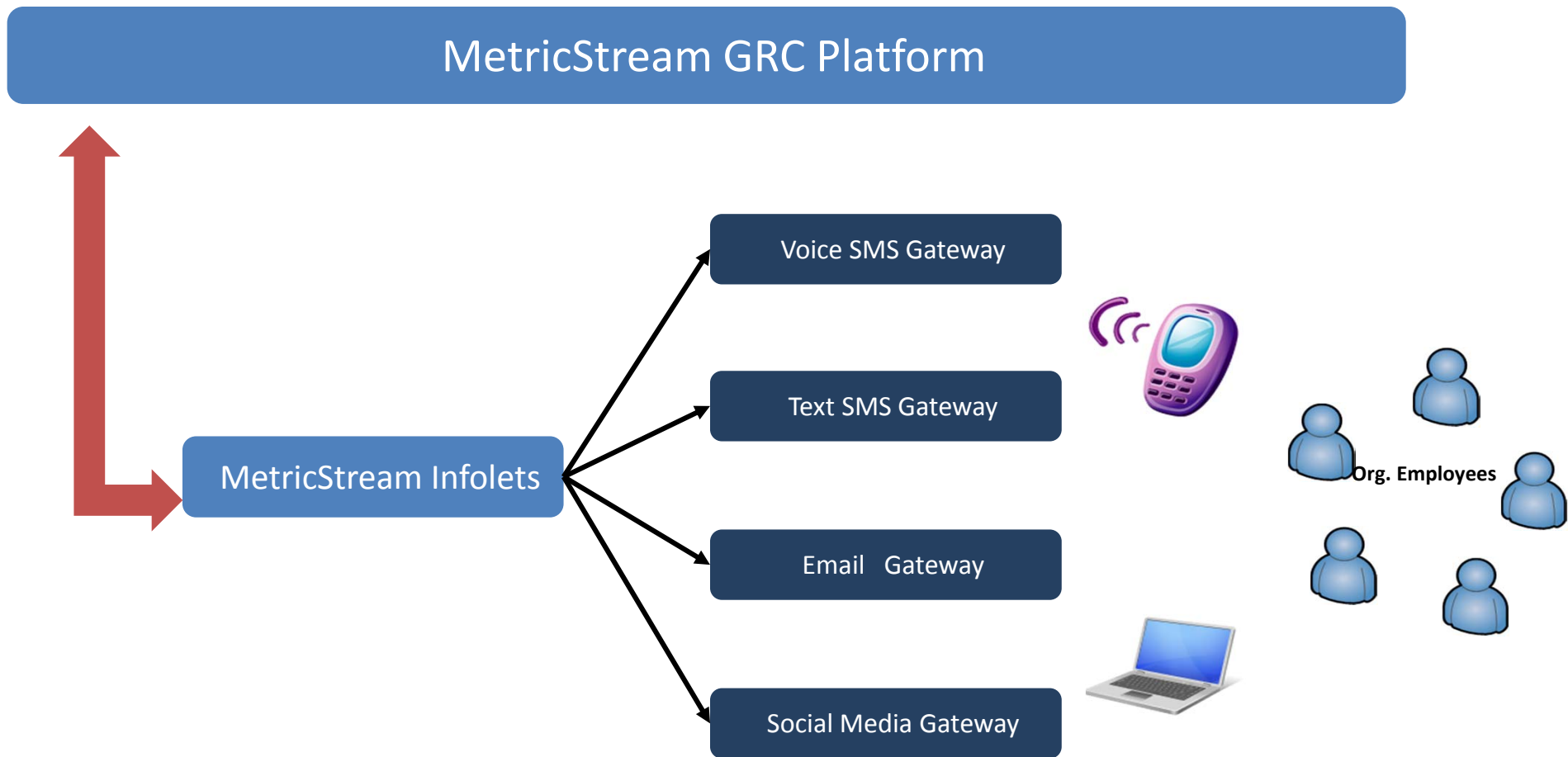


# MetricStream Mobile App for BCM



- Native Apps for Tablets
  - AppStudio support for tablet and web interface for apps
- BCM Users
  - Offline Access to BC/DR Plans : Role Specific with checklists / tasks for different scenarios
  - Sync whenever plans are updated online (Push) and update task status
  - On-site, geo-tagged information & evidence gathering capabilities – share photos & videos to command-center & stakeholders
  - Alerts / status notifications
  - Feeds from sources like FEMA
  - Ability to broadcast emergency notifications via social media

# Emergency Mass Notification



# Summary – Best Practices for BCMS

- **Common GRC Platform for a 360 degree view of risk**
  - Leverage GRC Management – ‘Single platform, version of the truth’
  - Develop common nomenclature and terminology within threat reports
  - Implement a common policy, risk, control framework and issue management
  - Implement common processes for incident response and crisis management
  - **Business Continuity**
  - Consider the end-end eco-system, including 3<sup>rd</sup> parties and suppliers
  - Understand the risks of security attacks inherited in backups
  - **Risk Management and Information Security**
  - Collect and develop better information and evidence about attack vectors, adversaries, and threat agents
  - Develop use cases for threat landscapes
  - Collect security intelligence that cover incidents in an end-to-end manner
  - Perform a shift in security controls to accommodate emerging threat trends
- impact achieved by

MetricStream

**GRC**  
SUMMIT **2013**  
MIDDLE EAST

October 29 - 30, 2013 | Dubai, UAE