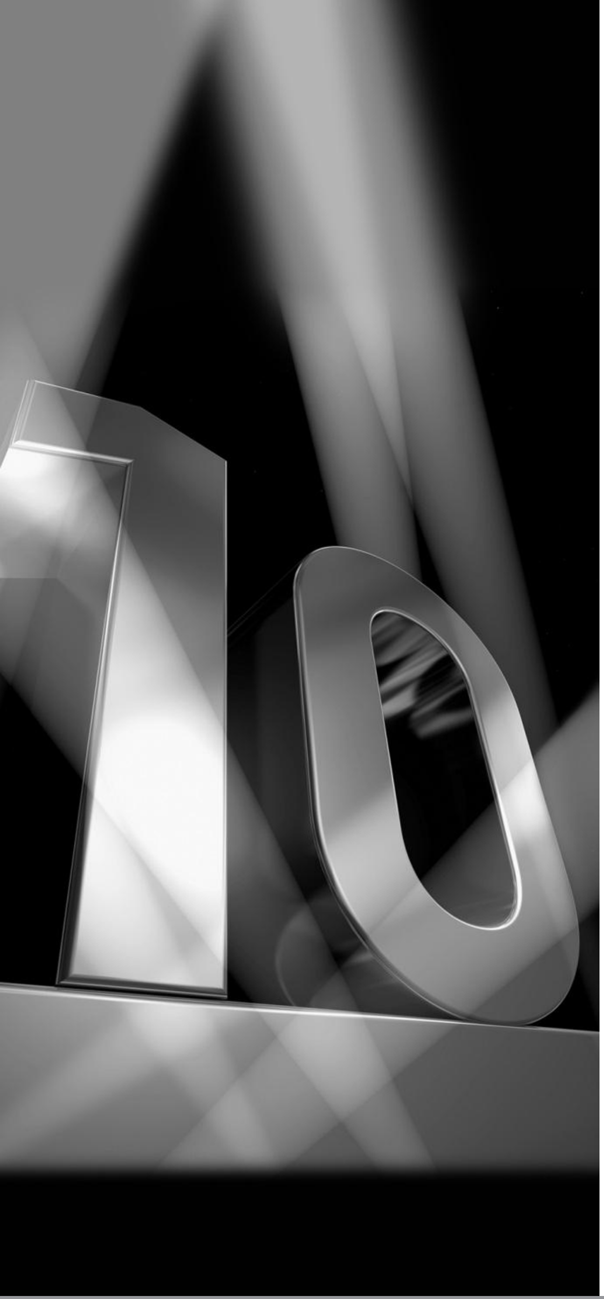


Enabling ISO 22301 Compliance with Archer Business Continuity Management & Operations

Patrick Potter
GRC Strategist, Business Continuity Management and Audit

RSA Archer grc summit 2013

A decade of sharing your success

Disclaimer-Safe Harbor Statement

This presentation is for informational purposes only. This document contains certain statements that may be deemed “forward-looking statements" within the meaning of the Private Securities Litigation Reform Act of 1995.

Forward-looking statements are based on assumptions and assessments made by us in light of our experience and perception of historical trends, current conditions and expected future developments. Actual results and timing of events may differ materially from those contemplated by the forward-looking statements due to a number of factors, including regional, national or global political, economic, business, competitive, market and regulatory conditions.

Any reproduction, retransmission, or republication of all or part of this document is expressly prohibited without the permission of RSA.

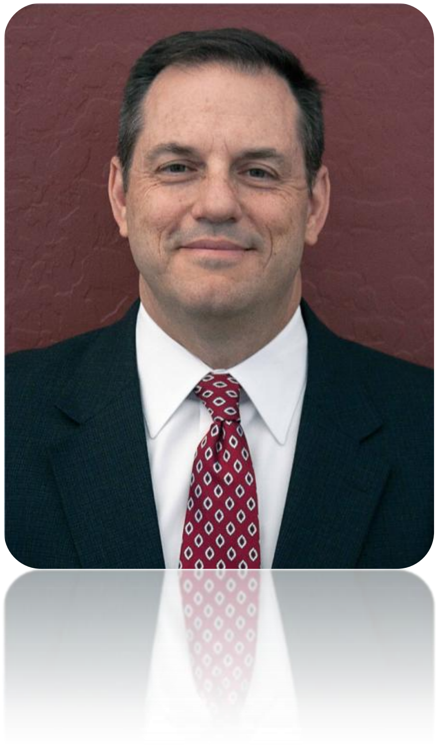
Session Abstract

As a BCM practitioner, you understand the importance of the new ISO 22301 standard, but what changes do you make to your BCM program to comply? This session will provide ways that you can use RSA Archer to implement the tenets of the standard by understanding your organization’s BCM needs, implementing measures to manage disruptive events, and monitoring your program’s effectiveness.

Today’s Speaker

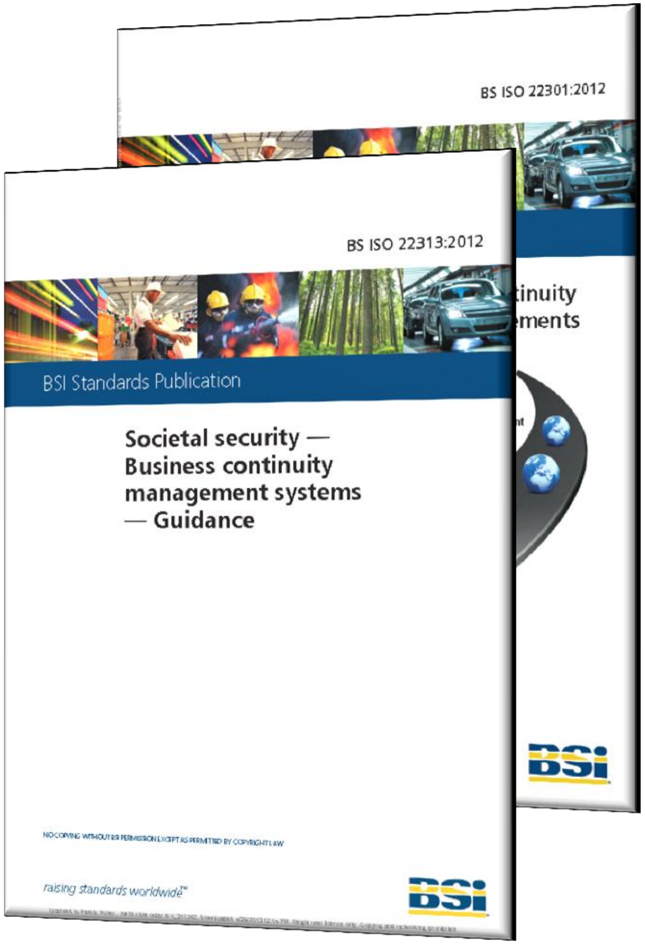
Patrick Potter, GRC Strategist – BCM and Audit

- At RSA, Patrick is responsible for applying his experience in BCM, audit and other related disciplines to the strategy of RSA Archer’s GRC solutions
- Prior to RSA, Patrick worked in financial services and high-tech manufacturing as Director of Internal Audit; Director - CISO; and Vice President of Technology Reengineering
- Patrick also held senior consulting positions where he led internal audit and business continuity management engagements for clients in airlines, energy/utilities, financial services, education, manufacturing and hospitality industries



ISO 22301/22313

- ISO 22301 specifies requirements to *plan, establish, implement, operate, monitor, review, maintain and continually improve* a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise
- ISO 22313 provides guidance, where appropriate, on the requirements specified in ISO 22301



BS ISO 22301:2012

tinuity
ments

BS ISO 22313:2012

BSI Standards Publication

Societal security —
Business continuity
management systems
— Guidance

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

raising standards worldwide™

Business Continuity Management System

A Business Continuity Management System (BCMS) Emphasizes the Importance of:

- Understanding the organization’s needs and the necessity for establishing business continuity policy and objectives
- Implementing and operating controls and measures for managing an organization’s overall capability to manage disruptive incidents
- Monitoring and reviewing the performance and effectiveness of the BCMS
- Continual improvement based on objective measurement

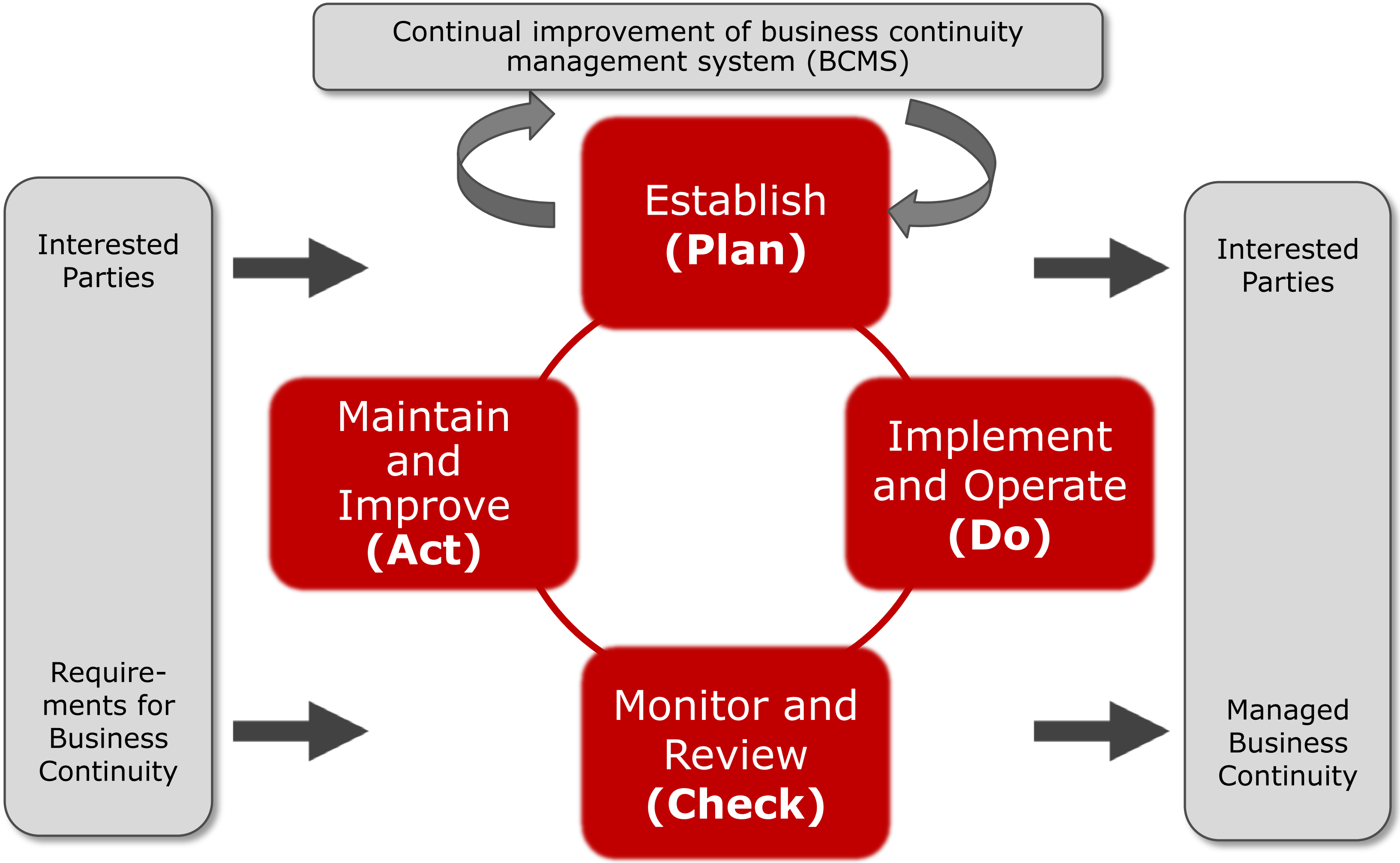
BCMS Components

A BCMS, like any other management system, includes the following key components:

- a policy
- people with defined responsibilities
- management processes relating to:
  - planning
  - implementation and operation
  - performance assessment
  - management review
  - improvement

- a set of documentation providing auditable evidence
- any BCMS processes relevant to the organization (BC, DR, CM)

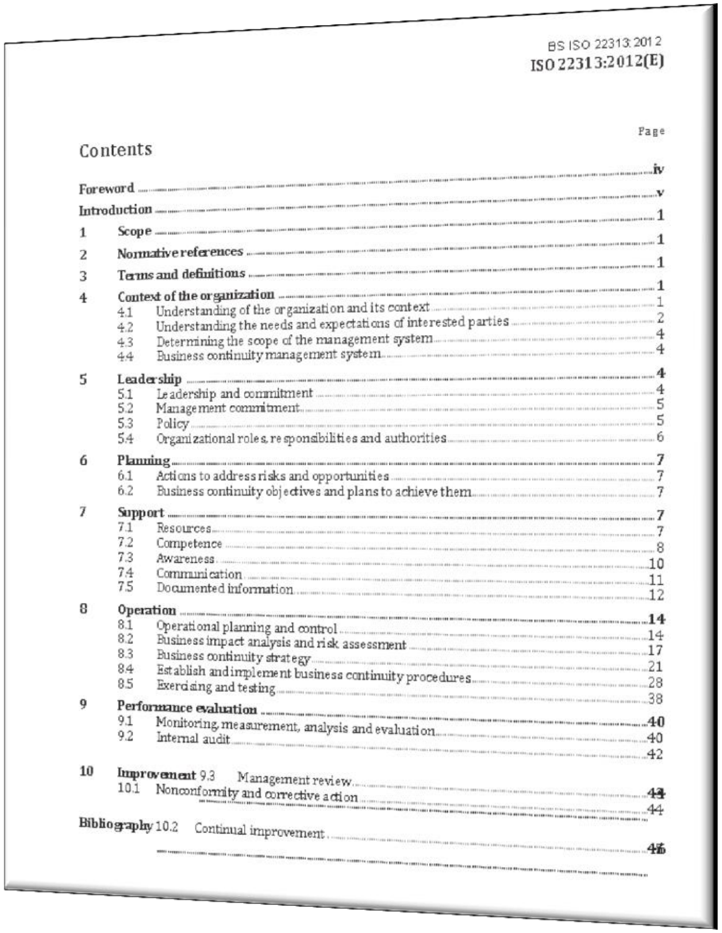
Plan-Do-Check-Act


Continual improvement of business continuity management system (BCMS)
Interested Parties
Require-ments for Business Continuity
Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check)
Maintain and Improve (Act)
Interested Parties
Managed Business Continuity

ISO 22313 Figure 1 – PDCA Model applied to BCMS processes

Review of Key Sections

- 4 Context of the organization
- 5 Leadership
- 6 Planning
- 8 Operation Planning and Control
- 9 Performance Evaluation

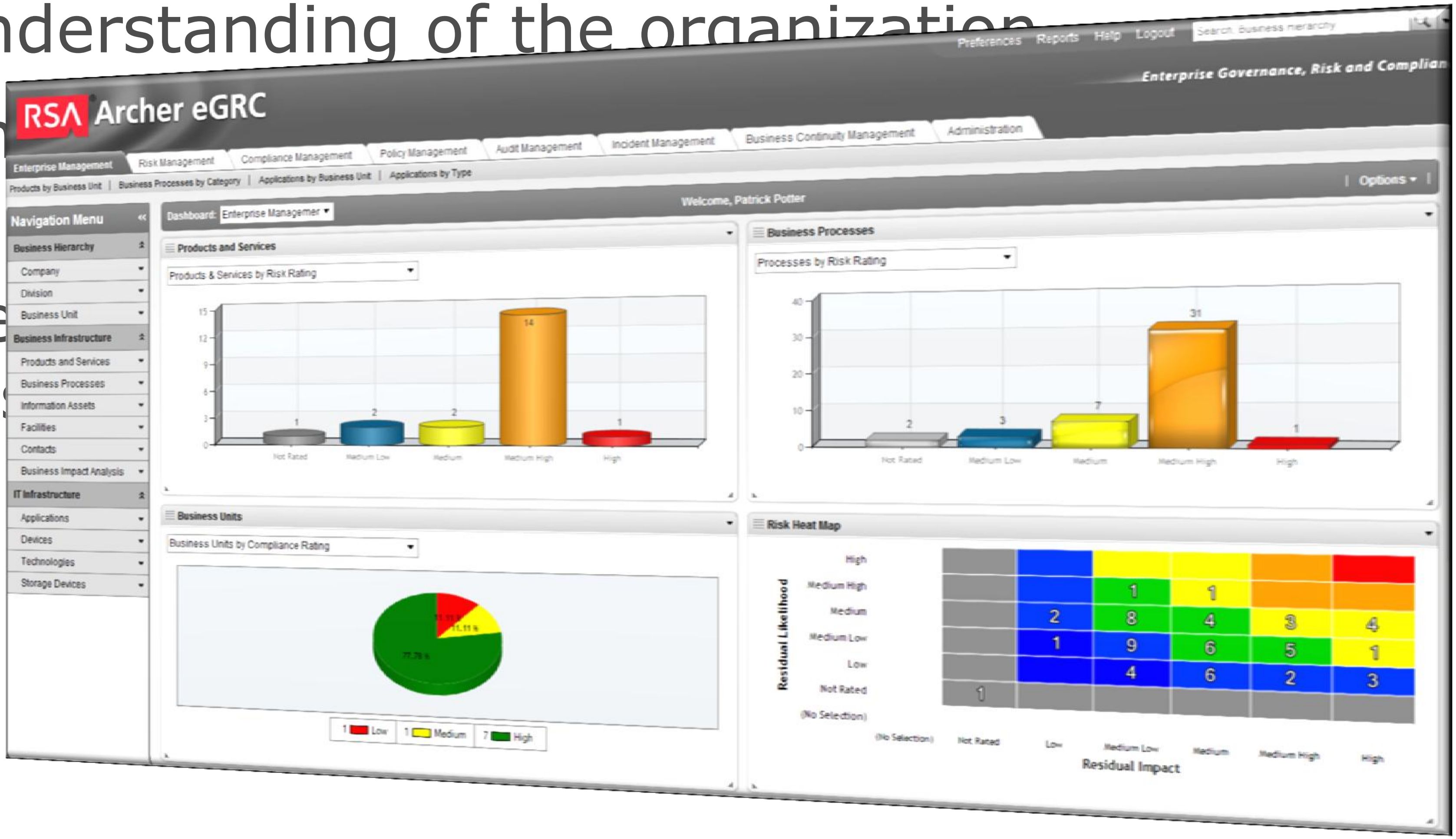


BS ISO 22313:2012
ISO 22313:2012(E)

Contents

4. Context of the organization

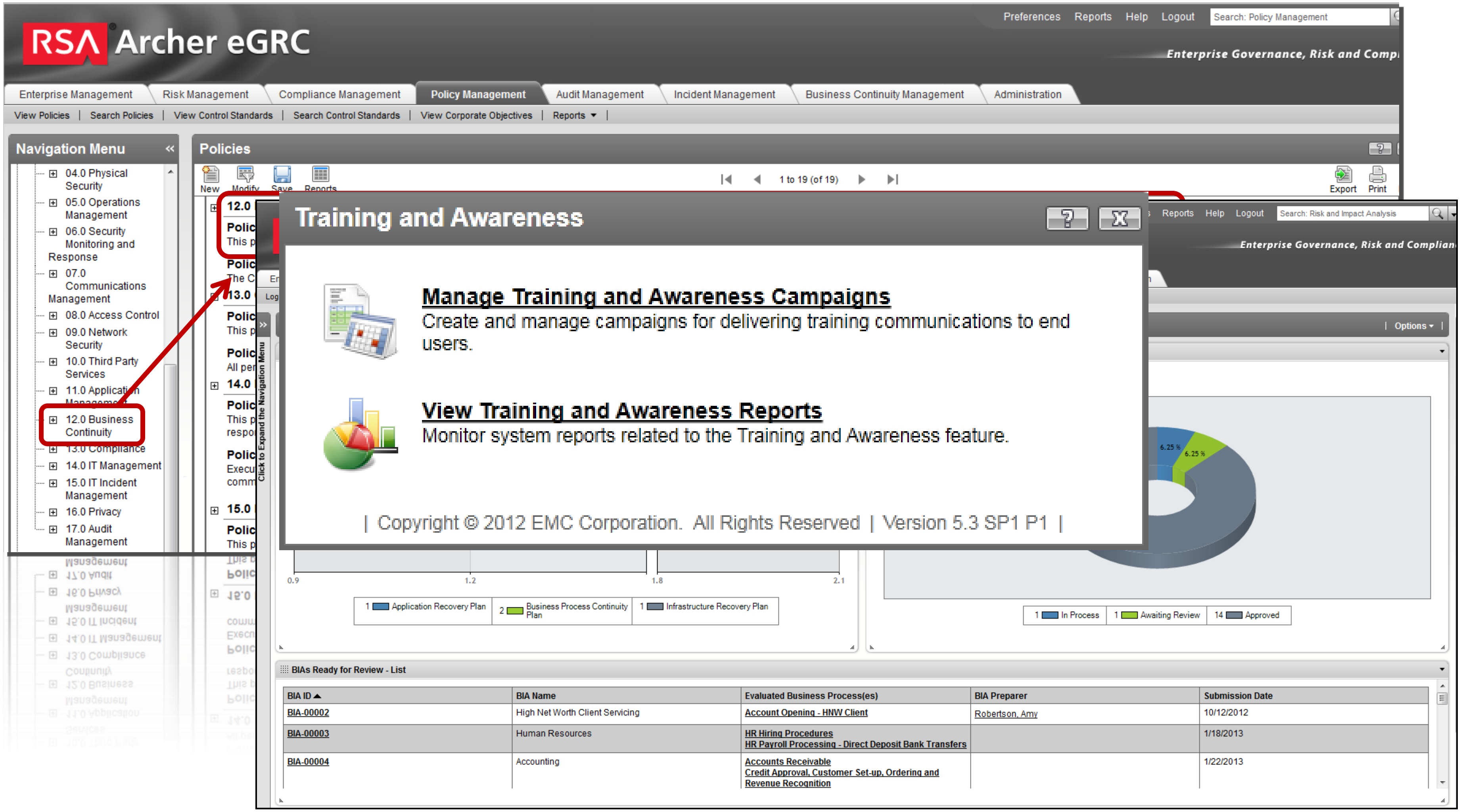
- Understanding of the organization
- Un
  of
- De
  sy



5. Leadership

- Leadership and commitment
- Management commitment
- Policy
- Organizational roles, responsibilities and authorities

Archer: Policy, Awareness and Performance



Training and Awareness

Manage Training and Awareness Campaigns

Create and manage campaigns for delivering training communications to end users.

View Training and Awareness Reports

Monitor system reports related to the Training and Awareness feature.

| Copyright © 2012 EMC Corporation. All Rights Reserved | Version 5.3 SP1 P1 |

BIAs Ready for Review - List

BIA ID ▲	BIA Name	Evaluated Business Process(es)	BIA Preparer	Submission Date
BIA-00002	High Net Worth Client Servicing	Account Opening - HNW Client	Robertson, Amy	10/12/2012
BIA-00003	Human Resources	HR Hiring Procedures HR Payroll Processing - Direct Deposit Bank Transfers		1/18/2013
BIA-00004	Accounting	Accounts Receivable Credit Approval, Customer Set-up, Ordering and Revenue Recognition		1/22/2013

6. Planning

- Actions to address risks and opportunities
- Business continuity objectives and plans to achieve them

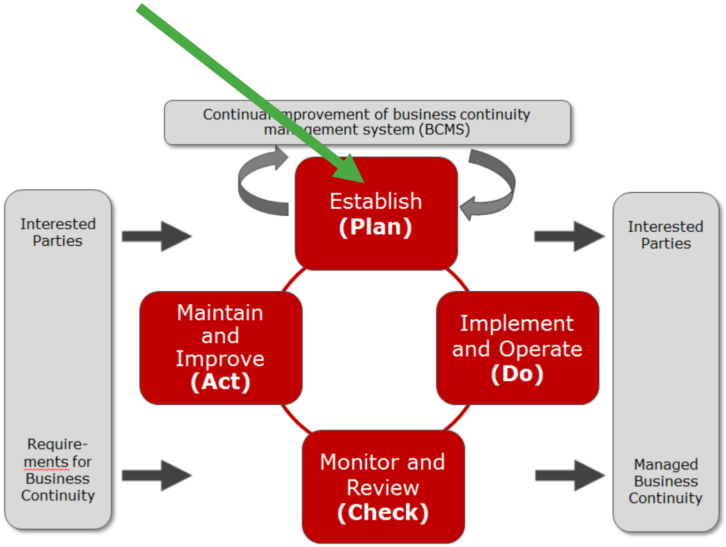
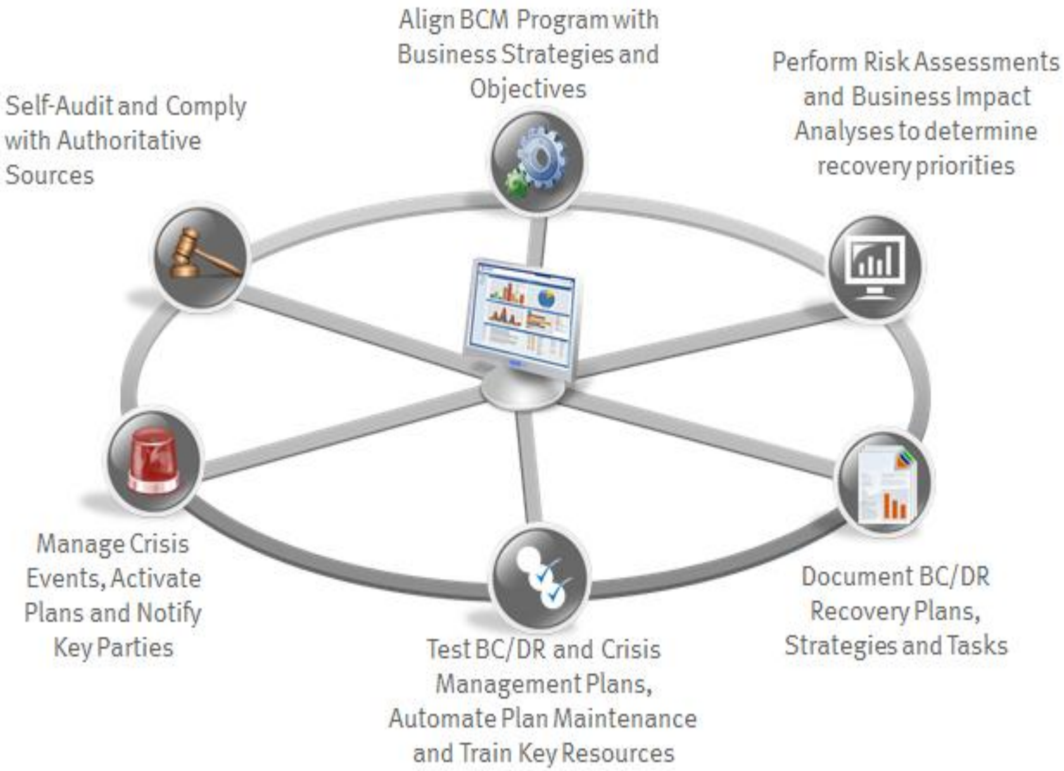

Continual improvement of business continuity management system (BCMS)
Interested Parties
Requirements for Business Continuity
Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check)
Maintain and Improve (Act)
Interested Parties
Managed Business Continuity

Figure 1 – PDCA Model applied to BCMS processes

8.1.1 Elements of BCM

- Operational Planning and Control
- BIA and Risk Assessment
- BC Strategy
- BC Procedures
- Testing


Align BCM Program with Business Strategies and Objectives
Perform Risk Assessments and Business Impact Analyses to determine recovery priorities
Document BC/DR Recovery Plans, Strategies and Tasks
Test BC/DR and Crisis Management Plans, Automate Plan Maintenance and Train Key Resources
Manage Crisis Events, Activate Plans and Notify Key Parties
Self-Audit and Comply with Authoritative Sources

8.1 Operation Planning and Control

8.1.2 Managing the BCM environment

- ensuring the continuing relevance
- promoting and embedding continuity across the organization

8.1.3 Maintaining business continuity

- keeping BCM current through good practice

8.1.4 Measuring effectiveness

- monitoring BCM performance

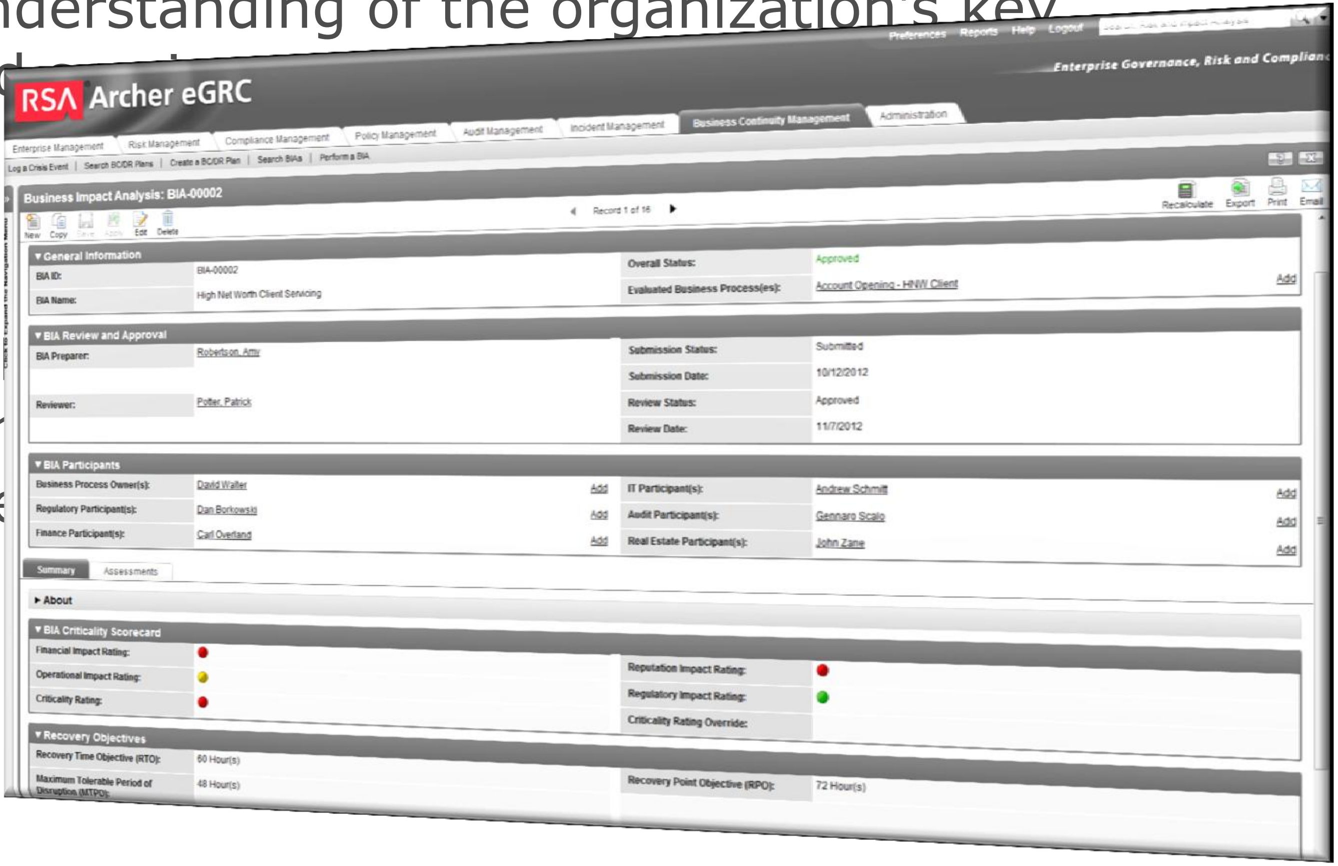
8.1.5 Outcomes

- capability is enabled and provides an effective response

8.2.2 Business Impact Analysis

The purpose of the BIA is to:

- obtain an understanding of the organization’s key products and
  them
- determine p
  activities
- identify the
  continuity ar
- identify depe



Business Impact Analysis: BIA-00002

▾ General Information

BIA ID:	BIA-00002	Overall Status:	Approved
BIA Name:	High Net Worth Client Servicing	Evaluated Business Process(es):	Account Opening - HNW Client

▾ BIA Review and Approval

BIA Preparer:	Robertson, Amy	Submission Status:	Submitted
		Submission Date:	10/12/2012
Reviewer:	Potter, Patrick	Review Status:	Approved
		Review Date:	11/7/2012

▾ BIA Participants

Business Process Owner(s):	David Walter	IT Participant(s):	Andrew Schmitt
Regulatory Participant(s):	Dan Borkowski	Audit Participant(s):	Gennaro Scalo
Finance Participant(s):	Carl Overland	Real Estate Participant(s):	John Zane

▾ BIA Criticality Scorecard

Financial Impact Rating:	🟥	Reputation Impact Rating:	🟥
Operational Impact Rating:	🟨	Regulatory Impact Rating:	🟩
Criticality Rating:	🟥	Criticality Rating Override:	

▾ Recovery Objectives

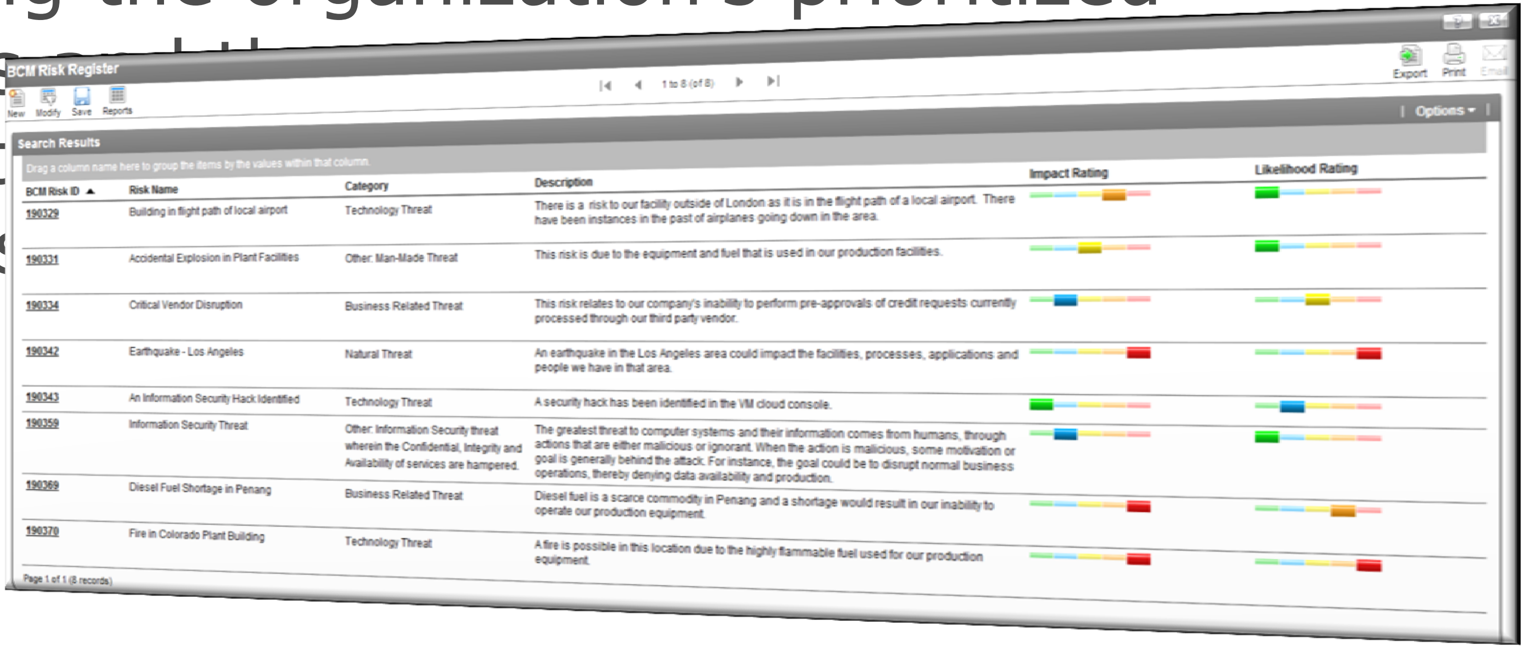
Recovery Time Objective (RTO):	60 Hour(s)		
Maximum Tolerable Period of Disruption (MTPD):	48 Hour(s)	Recovery Point Objective (RPO):	72 Hour(s)

8.2.3 Risk Assessment

The organization should establish a formal risk assessment process that systematically identifies, analyses and evaluates the risk of disrupting the organization’s prioritized activities

informat

other res



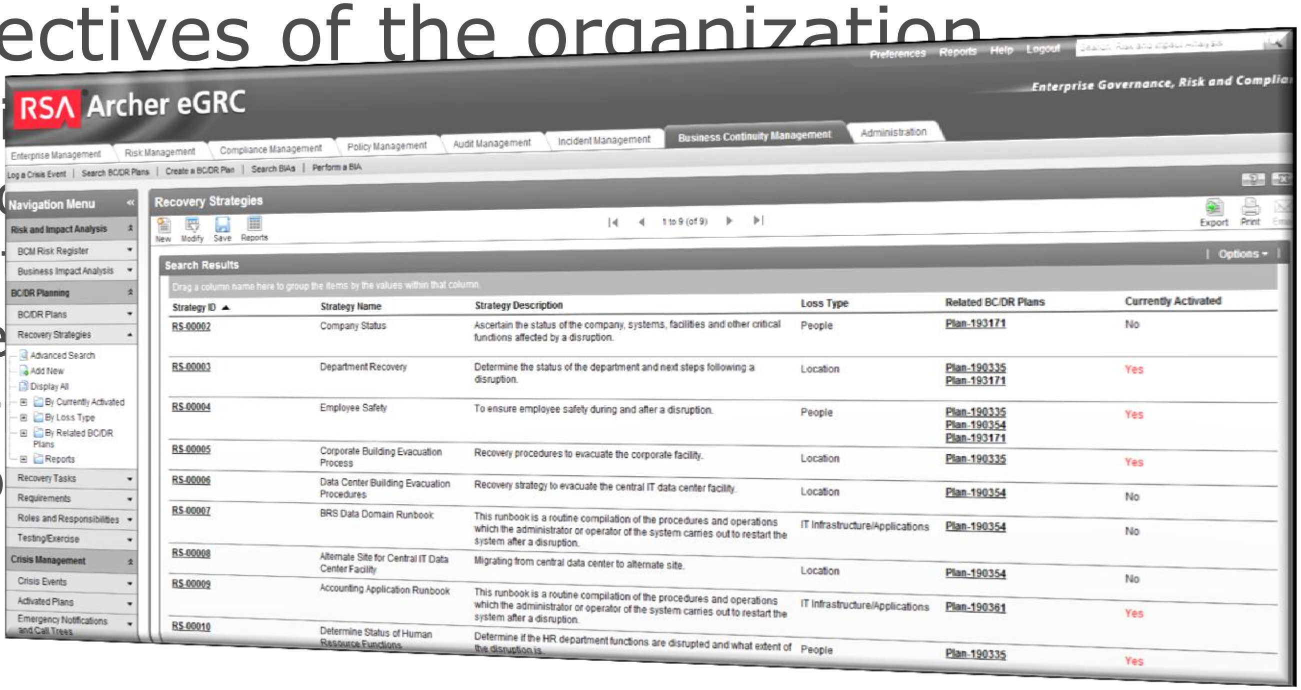
BCM Risk ID ▲	Risk Name	Category	Description	Impact Rating	Likelihood Rating
190329	Building in flight path of local airport	Technology Threat	There is a risk to our facility outside of London as it is in the flight path of a local airport. There have been instances in the past of airplanes going down in the area.	🟧	🟩
190331	Accidental Explosion in Plant Facilities	Other: Man-Made Threat	This risk is due to the equipment and fuel that is used in our production facilities.	🟨	🟩
190334	Critical Vendor Disruption	Business Related Threat	This risk relates to our company's inability to perform pre-approvals of credit requests currently processed through our third party vendor.	🟦	🟨
190342	Earthquake - Los Angeles	Natural Threat	An earthquake in the Los Angeles area could impact the facilities, processes, applications and people we have in that area.	🟥	🟥
190343	An Information Security Hack Identified	Technology Threat	A security hack has been identified in the VM cloud console.	🟩	🟦
190359	Information Security Threat	Other: Information Security threat wherein the Confidential, Integrity and Availability of services are hampered.	The greatest threat to computer systems and their information comes from humans, through actions that are either malicious or ignorant. When the action is malicious, some motivation or goal is generally behind the attack. For instance, the goal could be to disrupt normal business operations, thereby denying data availability and production.	🟦	🟩
190369	Diesel Fuel Shortage in Penang	Business Related Threat	Diesel fuel is a scarce commodity in Penang and a shortage would result in our inability to operate our production equipment.	🟥	🟧
190370	Fire in Colorado Plant Building	Technology Threat	A fire is possible in this location due to the highly flammable fuel used for our production equipment.	🟥	🟥

Page 1 of 1 (8 records)

8.3 Business Continuity Strategy

Identifying the action needed to address the findings from the BIA and risk assessment and in a way that meets the business continuity objectives of the organization

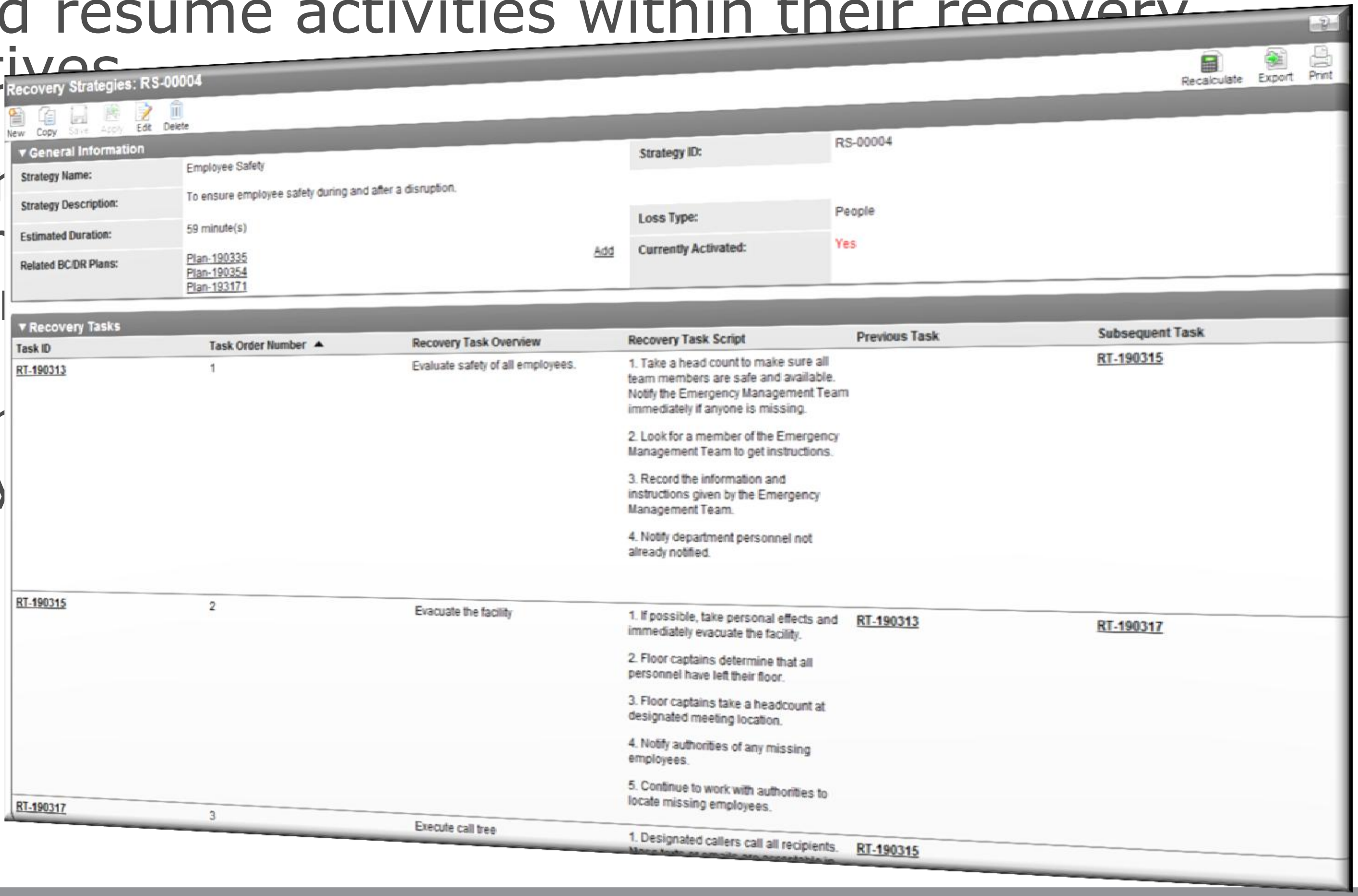
- Protecting pri
- Stabilizing, co prioritized ac
- Mitigating, re
- People; Infor Transportatio



Strategy ID ▲	Strategy Name	Strategy Description	Loss Type	Related BC/DR Plans	Currently Activated
RS-00002	Company Status	Ascertain the status of the company, systems, facilities and other critical functions affected by a disruption.	People	Plan-193171	No
RS-00003	Department Recovery	Determine the status of the department and next steps following a disruption.	Location	Plan-190335 Plan-193171	Yes
RS-00004	Employee Safety	To ensure employee safety during and after a disruption.	People	Plan-190335 Plan-190354 Plan-193171	Yes
RS-00005	Corporate Building Evacuation Process	Recovery procedures to evacuate the corporate facility.	Location	Plan-190335	Yes
RS-00006	Data Center Building Evacuation Procedures	Recovery strategy to evacuate the central IT data center facility.	Location	Plan-190354	No
RS-00007	BRS Data Domain Runbook	This runbook is a routine compilation of the procedures and operations which the administrator or operator of the system carries out to restart the system after a disruption.	IT Infrastructure/Applications	Plan-190354	No
RS-00008	Alternate Site for Central IT Data Center Facility	Migrating from central data center to alternate site.	Location	Plan-190354	No
RS-00009	Accounting Application Runbook	This runbook is a routine compilation of the procedures and operations which the administrator or operator of the system carries out to restart the system after a disruption.	IT Infrastructure/Applications	Plan-190361	Yes
RS-00010	Determine Status of Human Resource Functions	Determine if the HR department functions are disrupted and what extent of the disruption is.	People	Plan-190335	Yes

8.4 Business Continuity Procedures

- Provide overall control of the response to a disruptive incident and resume activities within their recovery time objectives
  - Incident procedur
  - Commur
  - Safety a
  - Salvage
  - Procedur
  - Recovery



Recovery Strategies: RS-00004

▾ General Information

Strategy Name:	Employee Safety	Strategy ID:	RS-00004
Strategy Description:	To ensure employee safety during and after a disruption.	Loss Type:	People
Estimated Duration:	59 minute(s)	Currently Activated:	Yes
Related BC/DR Plans:	Plan-190335 Plan-190354 Plan-193171 Add		

▾ Recovery Tasks

Task ID	Task Order Number ▲	Recovery Task Overview	Recovery Task Script	Previous Task	Subsequent Task
RT-190313	1	Evaluate safety of all employees.	1. Take a head count to make sure all team members are safe and available. Notify the Emergency Management Team immediately if anyone is missing. 2. Look for a member of the Emergency Management Team to get instructions. 3. Record the information and instructions given by the Emergency Management Team. 4. Notify department personnel not already notified.		RT-190315
RT-190315	2	Evacuate the facility	1. If possible, take personal effects and immediately evacuate the facility. 2. Floor captains determine that all personnel have left their floor. 3. Floor captains take a headcount at designated meeting location. 4. Notify authorities of any missing employees. 5. Continue to work with authorities to locate missing employees.	RT-190313	RT-190317
RT-190317	3	Execute call tree	1. Designated callers call all recipients.	RT-190315	

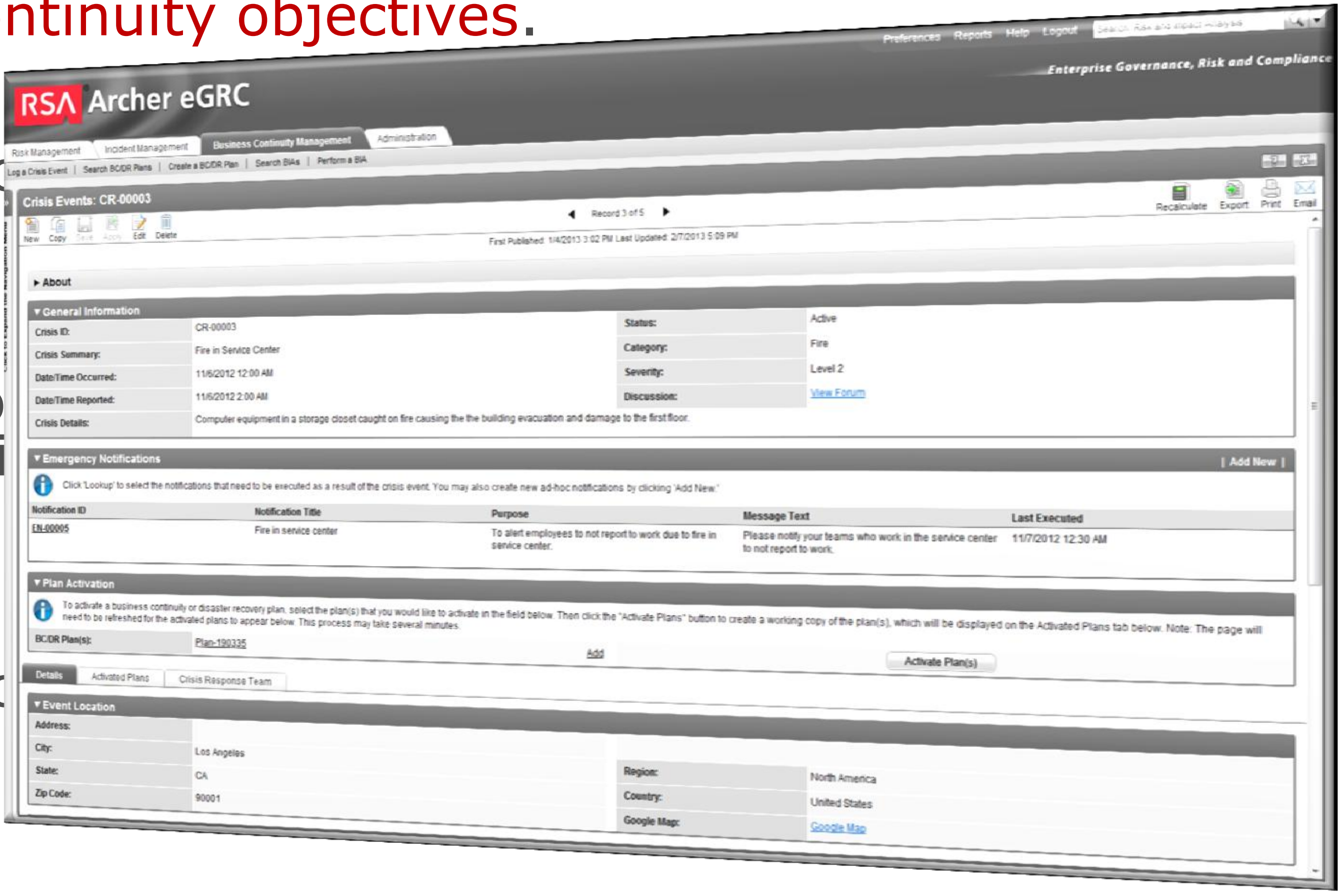
8.5 Testing

Testing is essential to ensure:

- that the strategies, policies, plans and procedures that have been put in place are adequate and meet business continuity objectives.

Testing should

- Technical, lo other opera
- All persons procedures
- Business co (including, i areas)
- Technology the availabi
- Relocation c


RSA Archer eGRC
Preferences
Reports
Help
Logout
Search: Risk and impact analysis
Enterprise Governance, Risk and Compliance
Risk Management
Incident Management
Business Continuity Management
Administration
Log a Crisis Event | Search BC/DR Plans | Create a BC/DR Plan | Search BIAs | Perform a BIA
Click to Expand the Navigation Menu
New
Copy
Save
Apply
Edit
Delete
Recalculate
Export
Print
Email
Details
Activated Plans
Crisis Response Team
Activate Plan(s)

Crisis Events: CR-00003

Record 3 of 5

First Published: 1/4/2013 3:02 PM Last Updated: 2/7/2013 5:09 PM

▸ About

▾ General Information

Crisis ID:	CR-00003	Status:	Active
Crisis Summary:	Fire in Service Center	Category:	Fire
Date/Time Occurred:	11/6/2012 12:00 AM	Severity:	Level 2
Date/Time Reported:	11/6/2012 2:00 AM	Discussion:	View Forum
Crisis Details:	Computer equipment in a storage closet caught on fire causing the the building evacuation and damage to the first floor.		

▾ Emergency Notifications | Add New |

Click 'Lookup' to select the notifications that need to be executed as a result of the crisis event. You may also create new ad-hoc notifications by clicking 'Add New.'

Notification ID	Notification Title	Purpose	Message Text	Last Executed
EN-00005	Fire in service center	To alert employees to not report to work due to fire in service center.	Please notify your teams who work in the service center to not report to work.	11/7/2012 12:30 AM

▾ Plan Activation

To activate a business continuity or disaster recovery plan, select the plan(s) that you would like to activate in the field below. Then click the "Activate Plans" button to create a working copy of the plan(s), which will be displayed on the Activated Plans tab below. Note: The page will need to be refreshed for the activated plans to appear below. This process may take several minutes.

BC/DR Plan(s): Plan-190335 Add

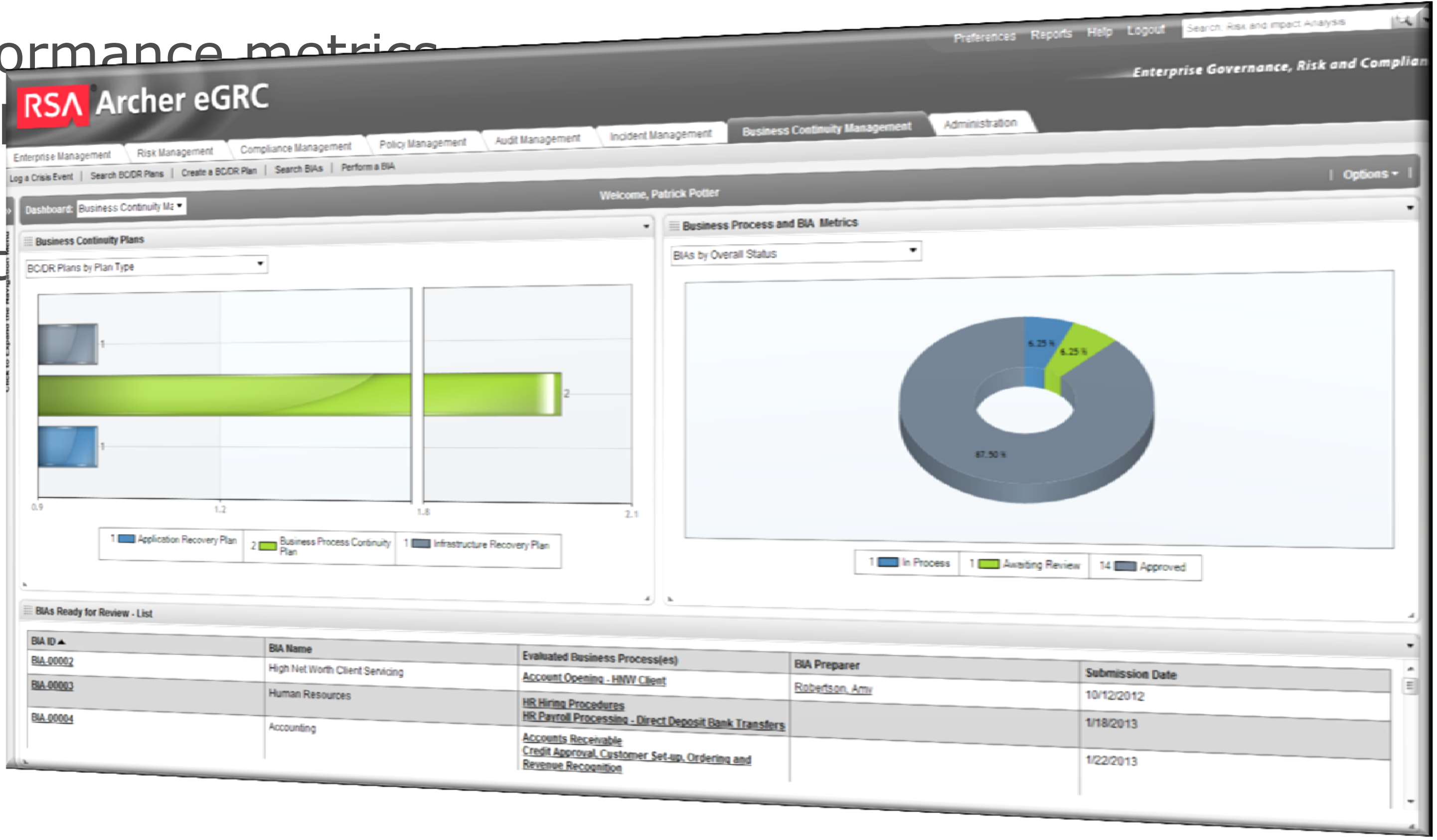
▾ Event Location

Address:			
City:	Los Angeles		
State:	CA	Region:	North America
Zip Code:	90001	Country:	United States
		Google Map:	Google Map

9 Performance Evaluation

To evaluate BCMS performance and effectiveness, programs should:

- Set performance metrics
- Assess t
- Confirm actions t



Preferences
Reports
Help
Logout
Search: Risk and Impact Analysis
RSA Archer eGRC
Enterprise Governance, Risk and Complian
Enterprise Management
Risk Management
Compliance Management
Policy Management
Audit Management
Incident Management
Business Continuity Management
Administration
Log a Crisis Event | Search BC/DR Plans | Create a BC/DR Plan | Search BIAs | Perform a BIA
Options
Dashboard: Business Continuity Ma
Welcome, Patrick Potter
Business Continuity Plans
BC/DR Plans by Plan Type
1
2
1
0.9
1.2
1.8
2.1
1 Application Recovery Plan
2 Business Process Continuity Plan
1 Infrastructure Recovery Plan
Business Process and BIA Metrics
BIAs by Overall Status
6.25 %
6.25 %
87.50 %
1 In Process
1 Awaiting Review
14 Approved

BIAs Ready for Review - List

BIA ID ▲	BIA Name	Evaluated Business Process(es)	BIA Preparer	Submission Date
BIA-00002	High Net Worth Client Servicing	Account Opening - HNW Client	Robertson, Amy	10/12/2012
BIA-00003	Human Resources	HR Hiring Procedures HR Payroll Processing - Direct Deposit Bank Transfers		1/18/2013
BIA-00004	Accounting	Accounts Receivable Credit Approval, Customer Set-up, Ordering and Revenue Recognition		1/22/2013

Recap – Key Points

- Be clear on the organization's key products and services and the activities that deliver them
- Know the priorities for resuming activities and the resources they require
- Have a clear understanding of the threats to these activities, but focus on the impact of disruptions, not the cause
- Have tried and trusted arrangements in place to resume these activities following a disruptive incident
- Make sure that these arrangements are routinely reviewed and updated so that they will be effective in all circumstances

22301 Certification

- Certify your program
- Certify your staff via a professional certification (Implementer, Auditor, Master)

Professional Evaluation and Certification Board
PECB

bsi.

CERTIFICATION EUROPE™

CENTRE FOR ASSESSMENT
Centre for Assessment Ltd.

SGS

RSA Archer

grc summit 2013

A decade of sharing your success

Thank you.