

**RSA Archer eGRC Suite**  
**RSA Archer Business Continuity Management 4**  
**Overview Guide**

Revision 1



## **Contact Information**

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers:

<http://www.emc.com/support/rsa/index.htm>.

## **Trademarks**

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and EMC are either registered trademarks or trademarks of EMC Corporation ("EMC") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to [www.rsa.com/legal/trademarks\\_list.pdf](http://www.rsa.com/legal/trademarks_list.pdf).

## **License agreement**

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

## **Third-party licenses**

This product may include software developed by parties other than RSA.

## **Note on encryption technologies**

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

## **Distribution**

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

# Contents

<b>Preface</b> .....	<b>4</b>
About This Guide .....	4
RSA Archer eGRC Platform Documentation Set .....	4
RSA Archer Business Continuity Management Documentation Set .....	5
RSA Archer Business Continuity Management Data Dictionary .....	5
Support and Service .....	6
<b>Chapter 1: Understand Business Continuity Management</b> .....	<b>7</b>
Introduction .....	7
Business Continuity Management Program .....	7
Business Recovery .....	7
IT Disaster Recovery .....	7
Crisis Management .....	7
Objectives of a Business Continuity Management Program .....	7
<b>Chapter 2: Managing the RSA Archer Business Continuity Management 4 Solution</b> .....	<b>9</b>
Introduction .....	9
Features of the RSA Archer Business Continuity Management Solution .....	9
RSA Archer Business Continuity Management Subsolutions .....	9
Risk and Impact Analysis Subsolution .....	10
BC/DR Planning Subsolution .....	11
Crisis Management Subsolution .....	14
RSA Archer Business Continuity Management Workflow Diagram .....	16
RSA Archer Business Continuity Management Integrated Solutions Diagram .....	17
RSA Archer Business Continuity Management User Groups and Access Roles .....	19
<b>Index</b> .....	<b>20</b>

# Preface

## About This Guide

This guide is for RSA<sup>®</sup> Archer<sup>™</sup> eGRC Suite administrators that need to install the RSA Archer Business Continuity Management 4 solution. It is designed to be used with the *RSA Archer eGRC Platform Administrator Guide* portfolio.

This guide assumes that the reader is knowledgeable about the eGRC industry and the RSA Archer eGRC Suite.

## RSA Archer eGRC Platform Documentation Set

For information about the RSA Archer eGRC Platform 5.3, see the following documentation:

Guide	Description
Administrator Guide	Provides administrators with a system overview, guidelines for navigating, and detailed instructions for key tasks.
Control Panel Guide	Provides administrators with instructions for completing tasks in the release.
Installation Guide	Provides administrators the details of the steps required to plan for, prepare, install, configure, grant access to, and test the release.
Release Notes	Provides administrators a detailed listing of new features, fixed issues, and known issues at the time of the current release.
User Guide	Provides end users with guidelines for navigating, detailed instructions for key tasks, and information about using communication tools.
Web Services API Reference Guide	Provides IT managers and programmers a list of the available web services for programmatically interfacing with the release. This guide provides formatting guidelines for field results, field inputs, and search inputs, and provides sample code for searching, adding and updating users, and updating assets.

Access the documentation from the Documents page on the RSA Archer Community at [https://community.emc.com/community/connect/grc\\_ecosystem/rsa\\_archer](https://community.emc.com/community/connect/grc_ecosystem/rsa_archer).

---

## RSA Archer Business Continuity Management Documentation Set

For information about the RSA Archer Business Continuity Management solution, see the following documentation:

---

Guide	Description
Release Notes	Introduces the RSA Archer Business Continuity Management solution, lists the documentation available, and provides information for obtaining support and service.
Overview Guide	Introduces the RSA Archer Business Continuity Management solution and provides information about the solution, any subsolutions, and the applications.
Installation Guide	Provides administrators with instructions to install the solution.
Practitioner Guide	Provides design information about the solution and a use case highlighting how the solution works.

---

You can access the RSA Archer Business Continuity Management documentation from the Documents page on the RSA Archer Exchange at [https://community.emc.com/community/connect/grc\\_ecosystem/rsa\\_archer\\_exchange](https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange).

---

## RSA Archer Business Continuity Management *Data Dictionary*

The RSA Archer Business Continuity Management *Data Dictionary* contains configuration information for the solution, including the user groups and access roles that must be created.

You can obtain the *Data Dictionary* for the solution by contacting your RSA Archer Account Representative or calling **1-888-539-EGRC**.

---

## Support and Service

---

Customer Support Information	<a href="http://www.emc.com/support/rsa/contact/phone-numbers.htm">http://www.emc.com/support/rsa/contact/phone-numbers.htm</a>
Customer Support E-mail	<a href="mailto:archersupport@rsa.com">archersupport@rsa.com</a>
RSA Archer Community	<a href="https://community.emc.com/community/connect/grc/ecosystem/rsa_archer">https://community.emc.com/community/connect/grc/ecosystem/rsa_archer</a>
RSA Archer Exchange	<a href="https://community.emc.com/community/connect/grc/ecosystem/rsa_archer_exchange">https://community.emc.com/community/connect/grc/ecosystem/rsa_archer_exchange</a>

---

The Community enables collaboration among eGRC clients, partners, and product experts. Members actively share ideas, vote for product enhancements, and discuss trends that help guide the RSA Archer product roadmap.

The Exchange is an online marketplace dedicated to supporting eGRC initiatives. The Exchange brings together on-demand applications along with service, content, and integration providers to fuel the success of RSA Archer clients.

# Chapter 1: Understand Business Continuity Management

---

## Introduction

This chapter contains the following sections:

- [Business Continuity Management Program](#)
  - [Objectives of a Business Continuity Management Program](#)
- 

## Business Continuity Management Program

Business Continuity Management (BCM) is the development of strategies and plans to provide alternative modes of operation for businesses during a catastrophic event, for example, a natural disaster, security breach, or network failure. BCM programs include business continuity, IT disaster recovery, and crisis management.

## Business Recovery

Business recovery identifies crucial aspects of an organization's business processes, such as the people that support the organization, locations at which the processes are performed and supported, and any related vital information. Business recovery helps to prevent or minimize the impact of interruptions to daily business operations.

## IT Disaster Recovery

As part of a BCM strategy, IT disaster recovery ensures the recovery of information technology processes, systems, applications, databases, and network assets used to support critical business operations.

## Crisis Management

Crisis management includes the actions taken to minimize the effects of an interruption and prepare for recovery of important business and IT processes. Emergency notifications alert the appropriate personnel about affected processes, enabling quick responses to events and minimizing potential damage to the business.

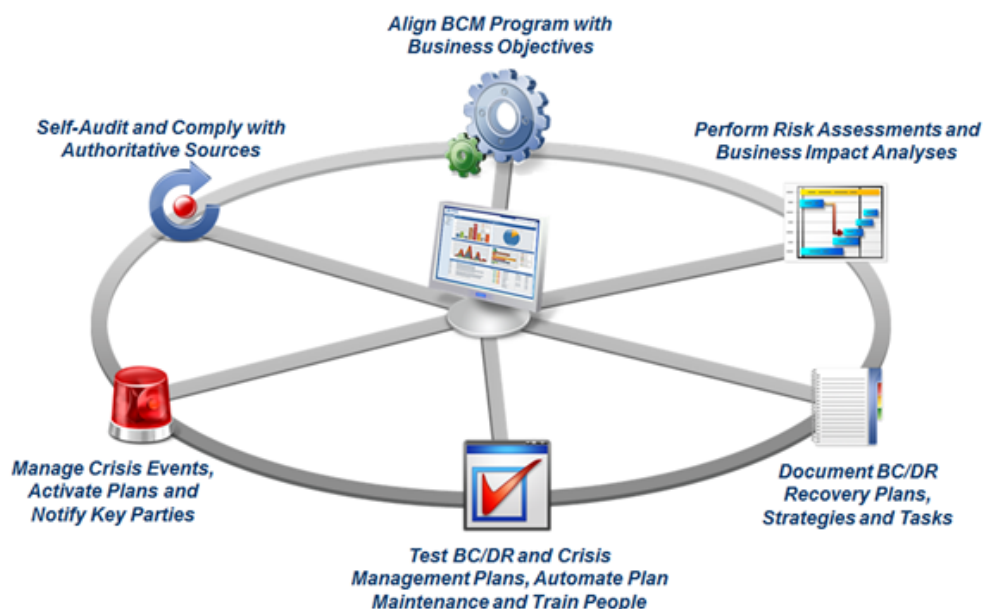
---

## Objectives of a Business Continuity Management Program

An important aspect of a successful Business Continuity Management program is the ability to integrate the following key areas as part of a recovery strategy:

- **Executive Management Support and Sponsorship.** Executive management must support and drive the BCM program alongside other related strategic initiatives.
- **Business Alignment.** Ensure that key components such as RTOs, strategies, and recovery steps align with the strategies, objectives, and operating needs of the business.
- **Risk Assessment and Business Impact Analysis.** Identify and evaluate the risks to critical business processes and determine their Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- **Business Continuity Strategy Design.** Determine the most cost-effective, efficient, and holistic recovery strategies that align with business requirements and other strategic imperatives.
- **Plan Development and Strategy Implementation.** Document the detailed recovery plans and tasks to recover critical business processes and supporting infrastructure.
- **Training and Awareness.** All individuals involved in the business and IT recovery plans must understand their roles and the aspects of recovery strategies and plans relative to the roles.
- **Testing and Maintenance.** Periodically evaluate and update recovery strategies and plans based on realistic and varied disruption scenarios. Tests should become increasingly more difficult and complex.
- **Compliance Monitoring and Auditing.** Ensure that all aspects of the BCM program align with regulatory and audit requirements.

The objectives of a BCM strategy fit into the BCM lifecycle, as shown in the following image.





## Chapter 2: Managing the RSA Archer Business Continuity Management 4 Solution

---

### Introduction

This chapter contains the following sections:

- [Features of the RSA Archer Business Continuity Management Solution](#)
- [RSA Archer Business Continuity Management Subsolutions](#)
- [RSA Archer Business Continuity Management Workflow Diagram](#)
- [RSA Archer Business Continuity Management Integrated Solutions Diagram](#)
- [RSA Archer Business Continuity Management User Groups and Access Roles](#)

---

### Features of the RSA Archer Business Continuity Management Solution

The RSA Archer Business Continuity Management 4 solution allows you to assess the criticality of your business processes and supporting technologies. You can then develop detailed recovery plans using an automated workflow for plan testing and approval. The solution is made up of subsolutions and applications that help you manage plan execution and communication in crisis situations to minimize harm to your employees, customers, reputation, and business operations. The RSA Archer Business Continuity Management 4 solution can help you:

- Centrally manage your business continuity program.
- Perform business impact and risk analysis.
- Test your plan and facilitate periodic reviews.
- Track crisis events in real time.
- Rapidly implement business recovery plans.
- Report on your business continuity program.

---

### RSA Archer Business Continuity Management Subsolutions

The RSA Archer Business Continuity Management 4 solution is composed of three subsolutions that represent the BCM lifecycle:

Subsolution	Description
<b><u>Risk and Impact Analysis</u></b>	Reflects the initial stages of business continuity planning, which consist of identifying risks and determining Recovery Time Objectives (RTOs) in order to set the risk and recovery thresholds for Business Continuity and IT Disaster Recovery Plans.
<b><u>BC/DR Planning</u></b>	Allows users to develop detailed recovery plans for business processes or IT assets, utilizing automated workflow for plan testing and approval.
<b><u>Crisis Management</u></b>	Gives management the ability to document and track crisis events that may lead to a business disruption.

## Risk and Impact Analysis Subsolution

The Risk and Impact Analysis subsolution allows you to identify risks that may exist in a certain location, business process, or technology. Based on these findings, you can determine the amount of time for which a business process can be disrupted before there is a substantial impact on the business. The Risk and Impact Analysis subsolution contains the following applications:

- BCM Risk Register
- Business Impact Analysis

### BCM Risk Register Application

Organizations can use the BCM Risk Register application to identify and evaluate risk by surveying the likelihood and impact of potential disruptions to business operations. Based on these evaluations, organizations can associate the risks to any mitigating controls and add the necessary steps to the BC/DR plans. The BCM Risk Register application allows you to do the following:

- Rate the impact and likelihood of each risk.
- Link to the BC/DR Plans application.
- Categorize risks, for example, **Natural Threat**, **Technology Threat**, or **Business Related Threat**.
- Prompt a periodic review and approval for each risk.
- Associate risks to crisis events.
- Relate the risk to multiple targets in the Enterprise Management solution, such as Business Processes, Applications, Products and Services, Devices, Facilities, and Information Assets.

### Business Impact Analysis Application

The Business Impact Analysis (BIA) application is designed to help organizations determine the criticality of processes with their Recovery Time Objective (RTO) and Recovery Point Objective (RPO). The application allows you to share this information with interdependent teams and enables business leaders to prioritize BC/DR plans, recovery strategies and recovery tasks. Additionally, the BIA application allows you to do the following:

- Link to the Business Processes application and the Facilities application from the RSA Archer Enterprise Management solution.
- Associate BIAs to the BC/DR Plans application.
- Attach supporting documentation for the BIA.
- Perform financial, operational, reputation, and regulatory impact assessments.
- Analyze the BIA Criticality Scorecard that contains the financial, operational, reputation, and regulatory impact assessments. The Criticality Scorecard also contains the criticality ratings, RTOs, RPOs, and Maximum Tolerable Period of Disruption.
- Prompt a periodic review and approval for each BIA.

### BC/DR Planning Subsolution

The BC/DR Planning subsolution allows an organization to develop detailed recovery plans for business processes or IT assets. The subsolution enables companies to manage the maintenance, execution, and activation of a business continuity plan or disaster recovery plan in crisis situations, which helps to minimize the impact to employees, customers, reputation, and business operations. The BC/DR Planning subsolution contains the following applications:

---

**Note:** You cannot edit an active plan. To find out which plans are active, go to the **Currently Activated** field and ensure that **Yes** is not selected for the plan that you want to modify.

---

- BC/DR Plans
- Recovery Strategies
- Recovery Tasks
- Requirements
- Roles and Responsibilities
- Testing/Exercise

### BC/DR Plans Application

The BC/DR Plans application allows you to develop a detailed business process recovery plan or IT disaster recovery plan using an automated workflow for approval and testing. The application helps to manage recovery plan maintenance, execution, and communication in disaster situations. The BC/DR Plans application also contains a centralized repository for components of the plan and links them to risk assessments, impact analysis, and items related to business hierarchy and enterprise infrastructure. The BC/DR Plans application allows you to do the following:

- Distinguishes between business continuity plans and disaster recovery plans.
- Associate multiple recovery strategies to a BC/DR plan.
- Capture steps or transactions that could get backlogged during a disruption.
- Identify the individuals that make up the recovery team for each plan.
- Document requirements, such as equipment, facilities, and vital records that are necessary for the BC/DR plan (reference the Requirements application).
- Connect BC/DR Plans to risks in the BCM Risk Register application and the Business Impact Analysis application.
- View information about plan testing, such as links to all completed tests, test cycles, the date of the last BC/DR plan test, the date of the next BC/DR plan test, and the test status.
- View information about crisis events that resulted in activation of a BC/DR plan, including links to all related crisis events, links to the activated plans, and the results from the last time that the plan was activated.
- Review the plan according to the selected review cycle.
- Attach a copy of the plan for distribution to other employees.

### Recovery Strategies Application

Recovery strategies are high level recovery alternatives and approaches, such as facility evacuations, earthquake response, or alternate site processing. The Recovery Strategies application is designed as a repository where you can document recovery strategies that can be pulled into BC/DR plans and associated with supporting recovery tasks. There can be multiple recovery strategies per BC/DR plan depending on the type, location, and magnitude of the asset being recovered, as well as the risks outlined in each plan. The Recovery Strategies application allows you to do the following:

- Categorize strategies by loss type, for example, **Facilities, Assets, IT, People** and **Third Parties**.
- Associate multiple recovery tasks to a strategy.
- Estimate recovery strategy duration by summing recovery tasks.

- Link to BC/DR plans that use the recovery strategy.
- Link to activated strategies.
- View an execution summary of the recovery strategy that was last activated.

### **Recovery Tasks Application**

Recovery tasks are the detailed steps that execute a recovery strategy. For example, if a recovery strategy is to evacuate the facility, the recovery tasks would include taking a headcount to ensure the safety of all employees, evacuating all employees to a certain location, and transporting employees to work from a remote location. The Recovery Tasks application is designed as a repository in which to document recovery tasks that can then be associated with any recovery strategy and pulled onto BC/DR plans. The application allows you to do the following:

- Capture the order in which to perform each task.
- Store recovery task scripts.
- Designate the role responsible for performing each task (reference the Roles and Responsibilities application).
- Capture the estimated and actual duration of each task.
- Associate recovery tasks with the applicable recovery strategies.
- View an execution summary of the recovery task that was last activated.

### **Requirements Application**

The Requirements application provides a location to document detailed requirements related to each BC/DR plan. For example, the application can include equipment, applications, facilities, and vital records related to each business process. The Requirements application allows you to do the following:

- Set a requirement type and capture relevant information such as quantity, type, and location.
- Link requirements to BC/DR plans.
- Attach supporting documentation to requirements.

### **Roles and Responsibilities Application**

You can use the Roles and Responsibilities application to document key roles within the BCM program. These roles can include a BCM Program Leader, a BCM Plan Owner, or a Security Manager. The application uses roles instead of individuals because individuals may change positions frequently in an organization, whereas roles needed to perform recovery tasks do not change as often. These roles are then pulled into BC/DR plans and associated with the appropriate recovery tasks. The Roles and Responsibilities application allows you to do the following:

- Capture the primary, secondary, and tertiary contacts responsible for performing the responsibilities of a role.

- Link to the risks and recovery tasks that each role is responsible for performing.

### **Testing/Exercise Application**

The Testing/Exercise application allows organizations to maintain a repository of tests related to their BCM and IT disaster recovery programs. Using these tests, organizations can evaluate the effectiveness of their BC/DR plans and gain insight into areas of the process that need additional attention. The application allows you to do the following:

- Select a test type.
- Select a BC/DR plan to activate from the BC/DR Plans application and copy the selected plans for testing.
- Select loss types (Facilities, Assets, IT, People or Third Parties) that are impacted in the test scenario.
- View scenario details, including description, compliance information, and related BCM risks, with mitigating controls.
- Determine if the exercise identified gaps in strategies, tasks, or the ability to achieve RTOs or RPOs.
- Track metrics on the completion of the tasks in the Activated Plans application, including the number of tasks completed, the number of tasks remaining, the duration of the recovery strategies and tasks, and the number of tasks that exceed the estimated duration.
- View whether the test passed or failed and the justification of the results.
- Sends the results of the test to a reviewer for approval.

## **Crisis Management Subsolution**

The Crisis Management subsolution gives management the ability to document and track crisis events, track notifications to all key individuals and groups (inside and outside the organization), and manage activated BC/DR plans. The Crisis Management subsolution contains the following applications:

- Crisis Events
- Emergency Notifications and Call Trees
- Activated Plans
- Notification History

### **Crisis Events Application**

The Crisis Events application allows customers to report and manage crisis events. They can track summary information, assign investigators, track legal involvement, and record information about the data, loss, recovery, and results of the incident. You can log reports as attachments within the crisis record and identify related incidents for trend analysis. The Crisis Events application allows you to do the following:

- Provide specific details about each crisis event, such as the date and location of the event, the severity rating, and the impacted business unit.
- Capture whether law enforcement or insurance companies are involved in the crisis event.
- Perform a cost analysis and select the loss types that are impacted by the crisis event.
- Set the crisis response team and select a notification template to execute or add a new notification (call tree).
- Activate a BC/DR plan from the BC/DR Plans application and track the completion of recovery tasks.
- Track metrics on the completion of tasks in the Activated Plans application.
- Use a discussion forum to talk about the crisis event.

### **Emergency Notifications and Call Trees Application**

The Emergency Notifications and Call Trees application enables organizations to manually manage notifications by using a call tree (a network of people organized in such a way that they can quickly and easily spread information amongst each other). The Emergency Notifications and Call Trees application allows you to do the following:

- Capture the call initiator and call recipient (references the Contacts application).
- Create custom messages to send to recipients.
- Link to BC/DR plans that utilize the call tree.
- Link to the Crisis Events application from which a notification may have originated.

### **Activated Plans Application**

The Activated Plans application documents BC/DR plans and the associated recovery strategies and tasks that have been activated as the result of a crisis event or a test scenario. By creating unique copies of the activated plan, organizations can select the specific strategies of the plan that need to be executed based on the impacted assets and can also track the completion of the required tasks. The Activated Plans application allows you to do the following:

- View information about your BC/DR plans, for example, the name, category, purpose, scope, type, backlog, assumptions, recovery team, call trees, and requirements.
- View information about the status of the executed plans, for example, the total number of recovery strategies and tasks completed, the progress, and task duration.
- Link to the Recovery Strategies application and the Recovery Tasks application.

- View information about the completed tasks, for example, the name of the individual performing the task, the status of the task, and the duration of the task.

### Notification History Application

The Notification History application is used to document the manual execution of call trees associated with BC/DR plans. The application captures the number of people contacted, the number of people reached, and the duration of the activity. An execution of the call tree can be tied to a specific crisis event or BC/DR test to show why the call tree was executed. The Notification History application allows you to do the following:

- Link to the Emergency Notifications and Call Trees application.
- Capture information about the status of an executed call tree.
- Link to the Crisis Events application to view more information about each executed call tree.

---

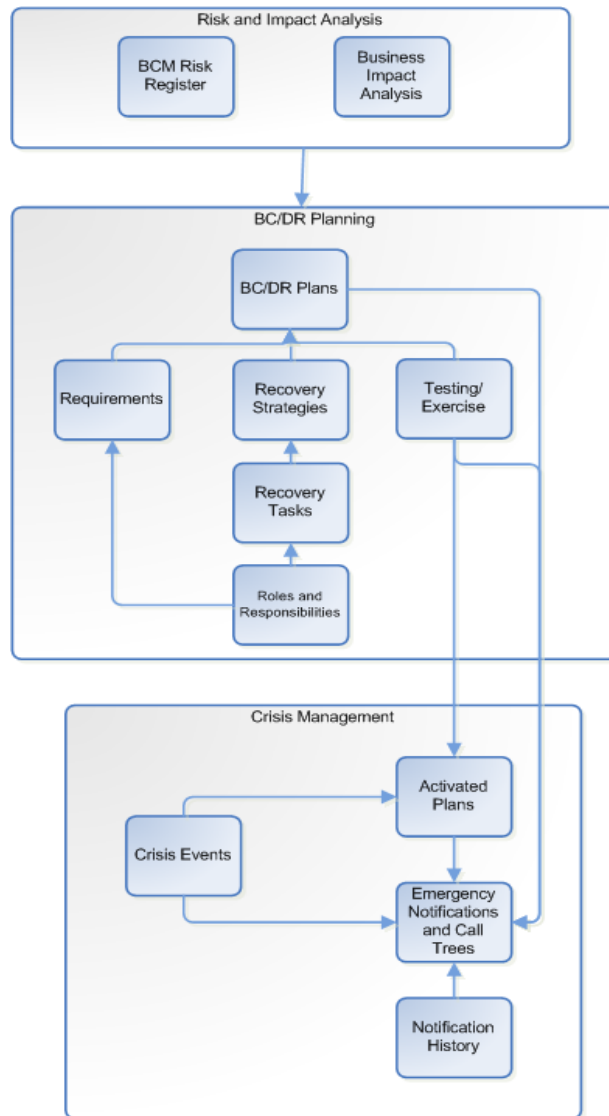
## RSA Archer Business Continuity Management Workflow Diagram

The workflow for the RSA Archer Business Continuity Management 4 solution is as follows:

1. Use the Risk and Impact Analysis subsolution to:
  - a. Align your BCM program with your business objectives.
  - b. Measure the value of your business processes and IT assets.
  - c. Rate the impact that a disruption to business operations would have on revenue, reputation, customers, and regulatory compliance.
2. Use the BC/DR Planning subsolution to:
  - a. Assign roles and responsibilities to members of the BCM team.
  - b. Document the recovery strategies, detailed recovery plans, and the tasks necessary to recover critical business processes.
  - c. Manage the maintenance, testing, execution, and activation of each plan during a crisis situation.
3. Use the Crisis Management subsolution to:
  - a. Set specific tasks to perform during a crisis event, including sending notifications to key members of the Business Continuity Management team.
  - b. Analyze trends by logging reports and identifying related crisis incidents.
  - c. Run self-audits on your BCM program to comply with regulations and authoritative sources.

The following diagram demonstrates the relationship between each subsolution and application in the RSA Archer Business Continuity Management 4 solution.

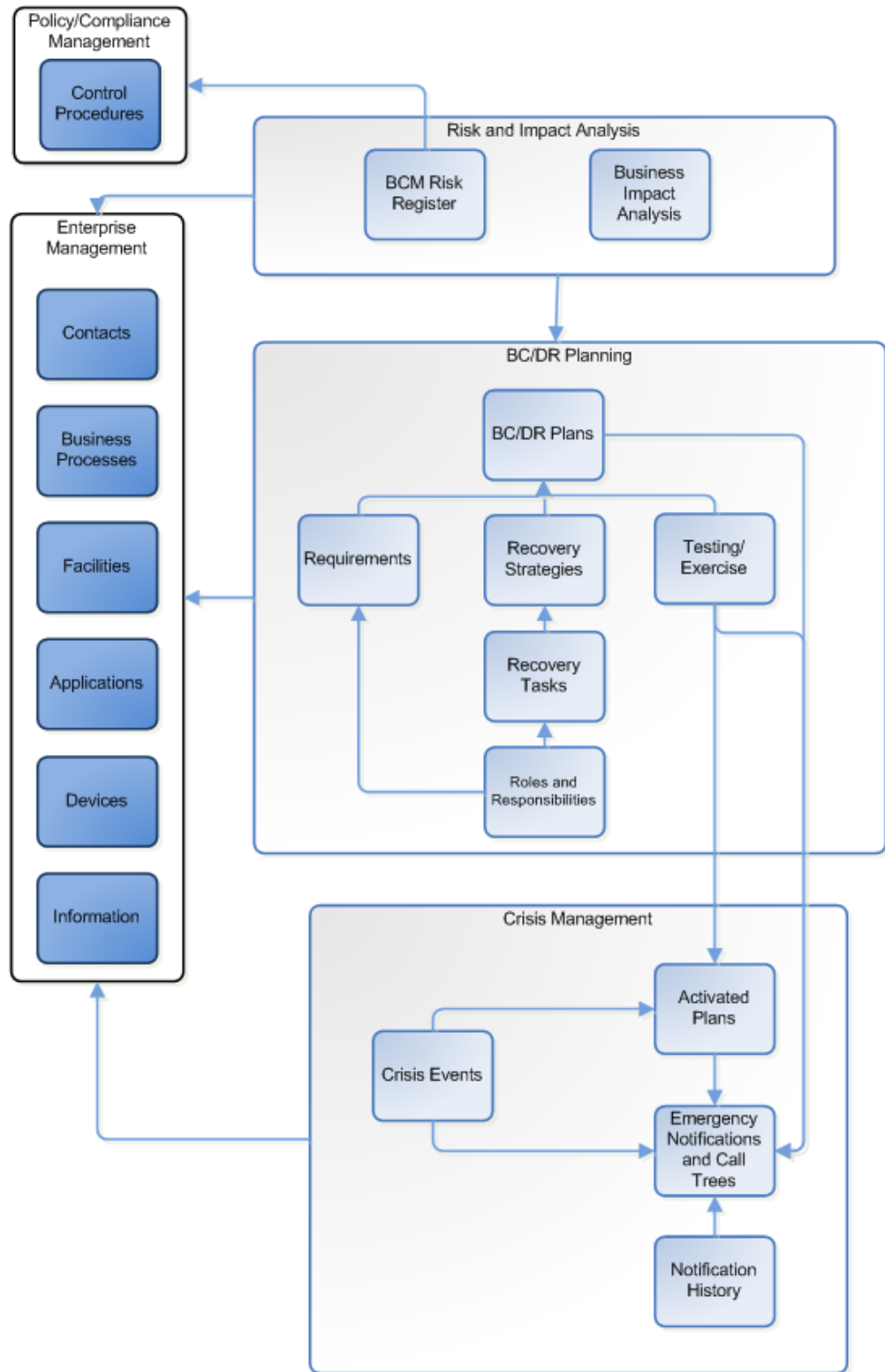




## RSA Archer Business Continuity Management Integrated Solutions Diagram

To function properly, the RSA Archer Business Continuity Management 4 solution references applications from the Enterprise Management solution and the Policy/Compliance Management solution. The referenced applications are the following: Contacts, Business Processes, Facilities, Applications, Devices, Information, and Control Procedures.

The image below demonstrates how the RSA Archer Business Continuity Management 4 solution integrates with the Archer eGRC Suite.



---

## **RSA Archer Business Continuity Management User Groups and Access Roles**

The RSA Archer Business Continuity Management 4 solution uses pre-defined user groups and access roles.

See the *Data Dictionary* for the list of groups and roles needed for the RSA Archer Business Continuity Management 4 solution.

For instructions, see "Add an Access Role" and "Add a Group" in the Access Control section of the *RSA Archer eGRC Platform Administrator Guide* portfolio.

# Index

## A

Activated Plans application 15

## B

BC/DR Planning subsolution

BC/DR Plans 12

described 11

Recovery Strategies 12

Recovery Tasks 13

Requirements 13

Roles and Responsibilities 13

Testing/Exercise 14

BC/DR Plans application 12

BCM

see Business Continuity

Management 7

BCM Risk Register application 10

Business Continuity Management

business recovery 7

crisis management 7

described 7

IT disaster recovery 7

objectives 7

Business Impact Analysis application 11

business recovery 7

## C

Crisis Event application 14

crisis management 7

Crisis Management subsolution

Activated Plans 15

Crisis Events 14

described 14

Emergency Notifications and Call

Trees 15

Notification History 16

customer support 6

## D

documentation

RSA Archer Business Continuity

Management 5

RSA Archer eGRC Platform 4

## E

Emergency Notifications and Call Trees

application 15

## I

integrated solutions diagram 17

IT disaster recovery 7

## N

Notification History application 16

## R

Recovery Strategies application 12

Recovery Tasks application 13

Requirements application 13

Risk and Impact Analysis subsolution

BCM Risk Register 10

Business Impact Analysis 11

described 10

Roles and Responsibilities

application 13

RSA Archer Business Continuity

Management 9

diagram 16

integrated solutions diagram 17

subsolutions 9

user roles 19

## S

solution

see RSA Archer Business Continuity

Management 9

subsolution

BC/DRPlanning 11

Crisis Management 14

Risk and Impact Analysis 10

support, technical 6

## T

Testing/Exercise application 14

## U

user roles  
described 19