# RSA Archer
# Security Operations Management - Co3
# Implementation Guide

**RSA Archer GRC Platform version 5.4 SP1 or 5.5**

**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**.

**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

# Preface

## About This Guide

This guide is for RSA$^{®}$ Archer$^{®}$ GRC administrators who need to install the RSA Archer Security Operations Management - Co3 solution. For more information, see the RSA Archer GRC Help.

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

## RSA Archer Documentation

You can access the RSA Archer documentation from the RSA Archer Exchange and RSA Archer Community.

| Documentation | Location |
| --- | --- |
| Platform | On the RSA Archer Community at: **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer** |
| Solutions, Applications, and Content | On Content tab on the RSA Archer Exchange at: **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange** |

RSA continues to assess and improve the documentation. Check the RSA Archer Community and RSA Archer Exchange for the latest documentation.

## Support and Service

| | |
| --- | --- |
| Customer Support Information | **www.emc.com/support/rsa/index.htm** |
| Customer Support E-mail | **archersupport@rsa.com** |

## Other Resources

RSA Archer Community enables collaboration among GRC clients, partners, and product experts. Members actively share ideas, vote for product enhancements, and discuss trends that help guide RSA Archer product roadmap. **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer**

RSA Archer Exchange is an online marketplace dedicated to supporting GRC initiatives that delivers on-demand applications with service, content, and integration providers to drive the success of RSA Archer clients.
**https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_ exchange**

RSA Solution Gallery provides information about third-party hardware and software products that have been certified to work with RSA products. The gallery includes Secured by RSA Implementation Guides with instructions and other information about interoperation of RSA products with these third-party products.
**https://gallery.emc.com/community/marketplace/**

RSA SecurCare Online (SCOL) provides unlimited access to a wealth of resources on the Web, 24 hours a day. The secure system provides members access to a support knowledgebase, to download current platform patches and bug fixes, to sign up for notifications, to manage your support cases and more.
**https://knowledge.rsasecurity.com/cleartrust/ct_ logon.asp?CTAuthMode=BASIC&language=en&CT_ORIG_ URL=https%3A%2F%2Fknowledge.rsasecurity.com%3A443%2F&ct_orig_ uri=%2F**

# Chapter 1: Integration Overview

## Introduction

- **RSA Archer Security Operations Management - Co3 Integration**
- **RSA Archer Security Operations Management - Co3 Integration Architecture**
- **RSA Archer Security Operations Management - Co3 Integration Files**
- **RSA Archer Security Operations Management - Co3 Integration Requirements**

## RSA Archer Security Operations Management - Co3 Integration

The RSA Archer Security Operations Management - Co3 integration allows you to leverage Co3 breach response procedures as part of your overall data breach response process in RSA Archer Security Operations Management. The integration can help you do the following:

- Determine the deadline for particular breach tasks.
- Identify the financial impact of a breach.
- Understand whether a certain breach task is mandatory or optional, and the order in which a particular task must be performed.

### RSA Archer Security Operations Management

The RSA Archer Security Operations Management solution enables you to aggregate all actionable security alerts, allowing you to become more effective, proactive, and targeted in your incident response and SOC management.

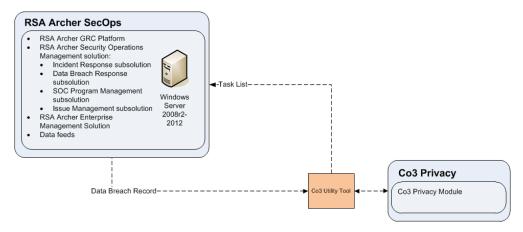RSA Archer Security Operations Management helps you do the following:

- Prioritize and respond faster to security incidents by leveraging business context and actionable threat intelligence.
- Engage key business and IT stakeholders in the incident management process.
- Simplify incident investigation and breach response procedures through industry best practice methodologies and response procedures.
- Optimize SOC investments through SOC KPI (key performance indicators) monitoring and staff time management tracking.

### Co3 Privacy

The Co3 Privacy module analyzes data breach information to identify the laws and regulations associated with each type of data breach, and generates a detailed breach response procedures task list based on these findings.

## RSA Archer Security Operations Management - Co3 Integration Architecture

The following figure provides a high level overview of the integration between RSA Archer Security Operations Management and the Co3 Privacy module.



## RSA Archer Security Operations Management - Co3 Integration Files

The RSA Archer Security Operations Management - Co3 integration package file, co3-tools.zip, includes the following files:

- co3.bat (This is the Co3 Utility Tool)
- co3-incident-builder.jar
- config.properties
- example files
- incident-builder.cmd
- templates

## Requirements

Before using the RSA Archer Security Operations Management - Co3 Integration, your system must meet the following requirements:

| Requirement | Details |
|---|---|
| RSA Archer Security Operations Management 1.1 | This guide assumes that you have installed RSA Archer Security Operations Management 1.1. For installation instructions, see the *RSA Archer Security Operations Management 1.1 Installation Guide*. |
| Co3 Privacy Module | This integration supports Co3 Privacy 16.0.144 and previous releases. |
| Co3 logon credentials | A user name and password are required to access the Co3 Privacy module. |
| Java SE Runtime Environment 7 and higher | This integration requires that Java is installed on your system. |

# Chapter 2: Using the RSA Archer Security Operations Management - Co3 Integration

## Use the RSA Archer Security Operations Management - Co3 Integration

**Procedure**

1. **Download the RSA Archer Security Operations Management - Co3 Files**
2. **Export Co3 Breach Response Report**
3. **Run the Co3 Utility Tool**
4. **Import Co3 Results into RSA Archer Security Operations Management**
5. **View Breach Tasks**

## Download the RSA Archer Security Operations Management - Co3 Integration Files

**Procedure**

1. Download the RSA Archer Security Operations Management - Co3 file, co3-tools.zip, from the Applications Exchange page on the RSA Archer Exchange at **https://community.emc.com/community/connect/grc_ecosystem/rsa_ archer_exchange**.
2. Extract co3-tools.zip, and save the files to a location on your local drive.

## Export Co3 Breach Response Report

The Co3 Breach Response - Generate Export File report pulls data from your existing breach records. For instructions about creating a breach record, see Chapter 4 of the *RSA Archer Security Operations Management 1.1 Practitioner Guide*.

**Procedure**

1. From the Navigation Menu, select Data Breaches > Reports > Co3 Breach Response - Generate Export File report.
2. Verify that only the breaches that you want to export are displayed in the report.
3. If necessary, modify the fields to display to include the fields required for Co3. For a complete list, see **Required Fields for Co3**.

     a. Click Modify.

     b. In the Fields To Display section, add or remove fields.

     c. Click Search.

4. Click Export.

5. Select XML File.

6. Select Exclude all HTML formatting tags, and click OK.

7. To access the file, click the Click Here link.

8. Save the file to the Co3-Tools folder.

### Required Fields for Co3

The following input fields should be included in your report to provide Co3 with the necessary breach information for analysis.

| Input Field | Required | Recommended |
| --- | --- | --- |
| Breach ID | X | |
| Impacted Regulations | X | |
| Date of Discovery | | X |
| Data Encrypted | | X |
| Data Format | | X |
| Data type | X | |
| Region | X | |
| Number of Records Disclosed per Region | X | |
| Is harm to individuals foreseeable? | | X |

## Run the Co3 Utility

The Co3 utility tool scans your exported breach data records against a database of laws and regulations and compiles a task list based on the number of violations that occurred during the breach.

**Procedure**

1. Open the folder where you extracted the co3-tools.zip files.

2. Click the co3.bat file.

3. For the input file, type:
   ```
   input.xml
   ```

   where *input.xml* is the XML file you saved in **Export Co3 Breach Reponse Report**.

4. For the output file name, type:
   ```
   output.csv
   ```

   where *output.csv* is the name of the .csv file that you want the Co3 utility to create.

5. When prompted, enter your Co3 logon credentials.

   **Note:** You can store your user names in the config.properties file if you do not want to type in your user name each time you log on.

6. Wait for the Co3 utility command screen to close automatically. This indicates that the scan has completed and that a list of tasks has been compiled.

## Co3 Output Fields

The Co3 utility tool generates a .csv file with the following fields.

- Related Breach (Breach ID)
- Task Name
- Required/Optional
- Task Status
- Task Owner
- Task Due Date
- Instructions
- Co3 Unique ID (This ensures duplicate tasks are not generated during data import)
- Sources
- Estimated Financial Impact (Figures in dollar amount on overall financial impact)
- Breach Task Source
- Order (This prioritizes the tasks in the order in which they should be completed)
- Co3 Response Generated

# Import Co3 Results into RSA Archer Security Operations Management

Once you have a list of breach tasks from Co3, you can import them into your Breach Tasks application.

**Procedure**

1.  From the Navigation Menu, select Data Breach Response > Breach Tasks > Data Import.

2.  In the General Information section, click Browse, and select your *output.csv* file.

3.  Click Next.

4.  In the Import Type field, select Update Existing Records.

5.  In the Application Field, select Co3 Unique ID.

6.  Click Next.

7.  Click Import. When the import has completed, you will see a Successful Completion notification.

    **Note:** The data import will complete depending on the schedule set by your administrator. For example, if the job queue is set to run immediately, the results will be generated immediately.

# View Breach Tasks

After you import the list of breach tasks from Co3, you can view a list of tasks associated with a breach, in order to facilitate a timely and thorough breach response.

**Procedure**

1.  Open the Data Breaches application and select the Breach ID.

2.  Select the Breach Tasks tab. Tasks associated with that breach ID are listed in the order in which they need to be completed.

**Note:** By default all new tasks have a status of New and are assigned to the System Administrator. You can manually assign tasks to specific individuals within your organization. For instructions, see the *RSA Archer Security Operations Management 1.1 Practitioner Guide*.

## Update Impacted Breach Regulations

If you need to change the impacted regulations for a breach, you must export and run the breach report through the Co3 utility tool to update the related breach task list.

**Note:** Tasks that are no longer applicable will be moved to the Not Applicable section of the Breach Tasks tab.

**Procedure**

1. **Export Co3 Breach Response Report**
2. **Run the Co3 Utility**
3. **Import Co3 Results into RSA Archer Security Operations Management**
4. **View Breach Tasks**