Rsam SSRS Report Installation Requirements and Administration Guide

Vendor Summary Report

Document Version: 2017.01 | December 2017

Contents

About this Guide

Each Rsam SSRS report has a unique set of steps for installing the report and ensuring that all the required configurations for the report are met. This guide provides a walk through of all the items to consider when installing the **Vendor Object Summary Report** and executing it for the first time.

For general information about integrating SSRS with your Rsam environment, refer the document *RSAM Reporting - SSRS Integration*.

For information on building your own SSRS reports, refer the document *Rsam Platform Step-by-Step Tutorial - Building SSRS Reports*.

Overview

This guide provides details around the installation artifacts and configuration dependencies required to run the Vendor Summary Report.

Minimum Rsam Version

The minimum version of Rsam required to execute this report is **9.2.2126.2**.

Required Modules

This report requires that you have licensed and installed the **Vendor Risk Management** baseline module.

Required SSRS Artifacts

This section provides information about the required SSRS artifacts for the Vendor Object Summary Report.

Report-Specific SSRS Artifacts

The following Report Definition Language files and Stored Procedures must be applied in your Rsam environment.

Report Definition Language (RDL) Files

The following table lists the Report Definition Language files that must be applied in your Rsam environment.

If your Rsam instance is on premise, then add the RDL files to your report server using SSRS Report Manager.

If your Rsam instance is in the Rsam Cloud, then contact support to have the RDL files added to your environment.

RDL File Name	Description
Vendor_Object_Summary.rdl	This is the primary RDL file for the Vendor Object Summary Report.
Domain_Graph_Subreport.rdl	This is the RDL file for the Compliance percentage sub report.
Questionnaire Findings Burn-Down_SubReport.rdl	This is the RDL file for the Burndown sub report.
Questionnaire Findings Burn-Down_Target by Domain_SubReport.rdl	This is the RDL file for the Burndown by Domain type sub report.
RiskFactorsSummary_SubReport	This is the RDL file for the Riskfactor Summary sub report.
StackedCharts_SubReport	This is the RDL file for the Stacked Summary sub report.
VOS_Subreport_BitSight	This is the RDL file for BitSight sub report.
VOS_Subreport_RiskRating	This is the RDL file for Riskrating sub report.
VOS_Subreport_SSC	This is the RDL file for SecurityScoreCard sub report.

Stored Procedures

The following table lists the Stored Procedures that must be applied in your Rsam environment. These procedures are included in the file called **Vendor Summary Report – Stored Procedures.sql**, which is included in the report installation package.

If your Rsam instance is on premise, have a database administrator execute this script against your database.

If your Rsam instance is hosted in the Rsam Cloud, please work with Rsam Support to have this script applied to your Rsam database.

Stored Procedure Name	Description
reportdata_Compliance_Percentage_Multiple	Fetches the data required for the **Compliance %** chart.
reportdata_object_objectdetail_SSRS	Fetches the data required for the **Compliance % Chart By Domain Type** chart.
reportdata_Vendor_ObjectSummary	Fetches the data for **Attributes of the given Vendor**.
reportdata_sub_object_special_policies	Fetches the data for **Questionnaire in Scope**.
reportdata_QS_FINDING_BURNDOWN_Multiple	Fetches the data for the **Questionnaire Burndown** chart.
reportdata_QS_FINDING_BURNDOWN_COMPLIANCE_DOMAINTYPE	Fetches the data for the **Questionnaire Burndown chart by Domain Type** chart.
reportdata_RiskFactor_Summary	Fetches the data for **Summary of RiskFactors** sub report.
reportdata_StackedChart	Fetches the data for the **Stacked Chart**.
reportdata_SSC_Gauge	Fetches the data for the **SSC Gauge Chart**.
reportdata_SSC_Line	Fetches the data for **SSC Line Chart**.
reportparam_DomainTYpe	Fetches the data for the **Domain Type** parameter.
reportParam_FindingType	Fetches the data for the **Finding Type** parameter.
reportdata_Compliance_Percentage	Fetches compliance percentage based on gaps

Configuration Dependencies

Before executing the report, you must ensure that your Rsam environment includes all the configuration elements on which the report depends. This section details the attributes, searches, and other elements that must be available in the environment before executing the report. New Rsam customers will have these items included in the databases by default, but existing customers who want to add SSRS reports to their existing Rsam environments may need to obtain these items from Rsam in the form of environment migration files.

Attribute Types

The attribute types listed in the following table must be present in your Rsam environment for the report to execute successfully. They are available in the optional environment migration script - **Vendor Summary Report – Attributes Main**.

Note: If you are an existing Rsam customer, applying these attribute types to your environment through an environment migration script may overwrite configuration changes that you have made to those attribute types.

Attribute Type Admin Name	Rsam ID
U: Open / Closed	RSAM01-00000861-033032A0D51F4743A243FBA49B4B70C2
U: Universal Severity / Risk	RSAM-00209
VEN: OGM - Execution Date	RSAMA6-00002010-A3A01096B9C44FF2A7ADD1E191D69A60

In addition to the preceding core VRM attributes, if you have licensed the SecurityScorecard or BitSight connectors, you should ensure that the following attributes are also included in your environment. They are included in supplemental environment migration scripts - **Vendor Summary Report – Attributes SSC** and **Vendor Summary Report – Attributes BST**.

SecurityScorecard Attributes

The migration package file for the SecurityScorecard attributes is **Vendor Summary Report – Attributes SSC**. The following table lists the attributes for the SecurityScorecard Connector.

Attribute Type Admin Name	Rsam ID
VEN: SSC: Application Security Grade	RSAMA6-00003133-2A027DCB78B94543A4356DC74C512850
VEN: SSC: Application Security Grade Previous	RSAMA6-00003153-4A02C009F9284BB783DEDC260F1E2650
VEN: SSC: Cubit Score Grade	RSAMA6-00003134-413E654EC9334E1F87CDF98A5D44C2EA
VEN: SSC: Cubit Score Grade Previous	RSAMA6-00003144-C2CB329F64964327826423C3B0E1CF3C
VEN: SSC: DNS Health Grade	RSAMA6-00003135-DD764688B0FB4A4FA4122A87433BE307
VEN: SSC: DNS Health Grade Previous	RSAMA6-00003145-2D1B22D977C94E1A9D03A7D313D85A35

Attribute Type Admin Name	Rsam ID
VEN: SSC: Endpoint Security Grade	RSAMA6-00003137-E71AC381B81547E9BC0659B6DE6CF730
VEN: SSC: Endpoint Security Grade Previous	RSAMA6-00003147-BA2AD90F4961468DB5E5049FBCF9731A
VEN: SSC: Hacker Chatter Grade	RSAMA6-00003136-7DF5187B244944A2BC570698C252A35D
VEN: SSC: Hacker Chatter Grade Previous	RSAMA6-00003146-9316EF5D9AAE4E2CBEDFC3E59CBB2468
VEN: SSC: Information Leak Grade	RSAMA6-00003140-A260434F55284BCA943388EF52E2A648
VEN: SSC: IP Reputation Grade	RSAMA6-00003148-B1F20DB0A50B48508273890D9A586276
VEN: SSC: IP Reputation Grade Previous	RSAMA6-00003138-DACF69214FEF4A1C9B08EC363933B3AA
VEN: SSC: Network Security Grade	RSAMA6-00003130-E13D44C10E584A1DB2C9A7619294C521
VEN: SSC: Network Security Grade Previous	RSAMA6-00003131-3E5354EC1EE04F73ADF473BB8E5EE0AD
VEN: SSC: Overall Grade	RSAMA6-00003150-C8302F00DFD74023AAB63DC8F5C6E49A
VEN: SSC: Overall Grade Previous	RSAMA6-00003151-C697875E65704167950C5D0E6B259F58
VEN: SSC: Patching Cadence Grade	RSAMA6-00003139-07029299EE54452C877209BDE74B1C8A
VEN: SSC: Patching Cadence Grade Previous	RSAMA6-00003142-98325F45741645868E421596AA117CD1
VEN: SSC: Security Scorecard Vendor Domain	RSAMA6-00003154-8936F06C95E047F6BC121F764719B8EB
VEN: SSC: Social Engineering Grade	RSAMA6-00003132-1CEA4DCD5448412EBF37F1777E51FAED
VEN: SSC: Social Engineering Grade Previous	RSAMA6-00003143-4828EF3D856D40FF839F95BAB55783D4

BitSight Attributes

The migration package file for the BitSight attributes is **Vendor Summary Report – Attributes BST**. The following table lists the attributes for the BitSight Connector.

Attribute Type Admin Name	Rsam ID
VEN: BST - Application Security Grade	RSAMR6-00002573-4719FAC52A1C434ABF4067FA3AAB5D11
VEN: BST - Botnet Infections Grade	RSAMR6-00002561-FD828A44AAC94FA69267574118BC1D7E
VEN: BST - Company GUID	RSAMR6-00002557-09743002DEA8420C84382E72E91D922F
VEN: BST - Data Breaches Grade	RSAMR6-00002572-FB4783570CA74D2590AE3BA750145B49
VEN: BST - DKIM Records Grade	RSAMR6-00002567-C59B6750D3614ADE842F966746447C1E
VEN: BST - DNSSEC Records Grade	RSAMR6-00002571-3AC9CD487AE64801AAABD3ADCBFED202
VEN: BST - File Sharing Grade	RSAMR6-00002565-9B8FBA367DDE4EA58F60BC68C26A88CF
VEN: BST - Malware Servers Grade	RSAMR6-00002562-DA6692B675CA4784BAE20F67B166B89C
VEN: BST - Open Ports Grade	RSAMR6-00002570-096967547AE047A5A8B9E72EC7E7FA63

Attribute Type Admin Name	Rsam ID
VEN: BST - Overall Company Rating	RSAMR6-00002558-AA84A7DEFB864A819B1AA02ECDE16804
VEN: BST - Overall Rating Tier	RSAMR6-00002983-E7BAD2ADAC954A1C8BED2F2863189F94
VEN: BST - Patch Cadence Grade	RSAMR6-00002560-A3D2D492614B4A39B09F1080B18AFCCE
VEN: BST - Potentially Exploited Grade	RSAMR6-00002564-9A26F4D7C57F48D78D27DDDF0979CFDC
VEN: BST - Spam Prop Grade	RSAMR6-00002559-F43C60C7CE8543898AE7ACED598BB90D
VEN: BST - SPF Domains Grade	RSAMR6-00002566-6F8584C267E14A7D8996FACB42D93CB7
VEN: BST - TLS/SSL Certificates Grade	RSAMR6-00002568-5ED6283ED1B04B2B89A6E9C2A19C534F
VEN: BST - TLS/SSL Configurations Grade	RSAMR6-00002569-CE8D00C403B647DBB2228058B4D04BD2
VEN: BST - Unsolicited Communication Grade	RSAMR6-00002563-4965F0EBA78D4DA48405359E2E7512B2

Searches

A set of searches must be present in your Rsam environment for the report to execute successfully. These searches have been created specifically for use with the SSRS report (note the naming convention). These searches should not be modified for use within other parts of Rsam (navigators, charts, etc.). If you want to use these searches throughout other areas of Rsam, it is recommended that you create copies of these searches and modify the searches for the required purposes.

The following table lists the search that must be present in your Rsam environment for the Vendor Object Summary Report to execute successfully.

Search Name	Rsam ID	Migration Package File Name
VEN: Record Types for Universal Severity (SSRS)	RSAMA6-00003949-59E1FE03F3914BE1BC55300A46903C55	Vendor Summary Report – Searches Main

To add these searches to your environment, import the environment migration script, **Vendor Summary Report - Searches Main**.

In addition to the preceding searches, if you have licensed the SecurityScorecard or BitSight connectors, ensure that the following additional searches are also present in the environment. These searches are contained in the migration files **Vendor Summary Report – Searches SSC** and **Vendor Summary Report – Searches BST**.

Search Name	Rsam ID	Migration Package File Name
VEN: SSC - Overall Grade Gauge (SSRS)	RSAMA6-00003831-90A9F38E2A124666B503FE476318F60B	Vendor Summary Report – Searches

Search Name	Rsam ID	Migration Package File Name
VEN: SSC - Overall Grade Trend (single) (SSRS)	RSAMA6-00003837-A7566719ADE844FFAA0AB8739CFB0020	SSC
VEN: BST - BitSight Overall Rating Gauge (SSRS)	RSAMA6-00003827-9DE505E4CE0C4415BB298631EDC371BD	Vendor Summary Report – Searches BST
VEN: BST - BitSight Overall Rating Trend (SSRS)	RSAMA6-00003829-2B1DFDB3A43F48FC9D5DD064391DB0EC	

Report, Buttons, and Handlers

The items mentioned in this section are all contained in the migration package - **Vendor Summary Report – Report and Workflow Items.**

To access the report from the **Report** menu in Rsam, you must apply the report through the provided migration script. The following table lists the name and ID of the report.

Report Name	Rsam ID
Vendor Summary Report	RSAMA6-00000247-54442EA945854D43841809F31C35D729
Vendor Summary SSRS (Report Category)	RSAMA6-00000246-EA6ED79BDC934B40A9ABC8EB56AF2A6D
Object (Report Type)	RSAM-10

To access the report from an object in Rsam, ensure that you have the following button and handler present in your environment and that it is associated with the correct Object Type. These are available in the environment migration package.

Type	Name	Rsam ID
Handler	**VEN: Run Vendor Summary SSRS Report**	RSAMA6-00001501-164DC70259004F11871F158E5E31BB99
Button	**VEN: View Vendor Summary SSRS Report**	RSAMA6-00000824-5EC726FB39534943970435E2AC10D072

Record Types

The record types mentioned in the following tables are included as part of the VRM baseline module in Rsam and for most customers. These serve as the record types that are presented in the Vendor Object Summary Report.

If you have created custom events or incident record types, those will be included in the report if the following criteria are met:

- You have included your custom record category types in the SSRS-specific searches
- You have associated your record types with the required attribute types

Note: If you are an existing Rsam customer, applying these record types to your environment through an environment migration script may overwrite configuration changes that you have made to those record types.

The following table lists the Record Types for the Vendor Object Summary report.

Record Type Admin Name	Rsam ID
QF: Questionnaire Finding	RSAM-00001
RR: Risk	RSAM-00200

In addition to the preceding core VRM record types, the Vendor Object Summary Report can also include information on record types associated with the SecurityScorecard or BitSight connectors. If you have licensed either of the connectors, you should ensure that the appropriate connector-specific record types are also included in your environment.

The following table lists the Record Types.

Record Type Admin Name	Rsam ID
VEN: SSC - Ongoing Monitoring Snapshot	RSAMA6-00000625-BCCC9553094B4C9093A1AB0476C762EB
VEN: BST - Ongoing Monitoring Snapshot	RSAMR6-00000608-E3E6F4101C3348559351D6A1CB876341

Object Types

The following table lists the Object Type required for the Vendor Object Summary Report.

Object Type	Rsam ID
Vendor / Service Provider	RSAM-00114