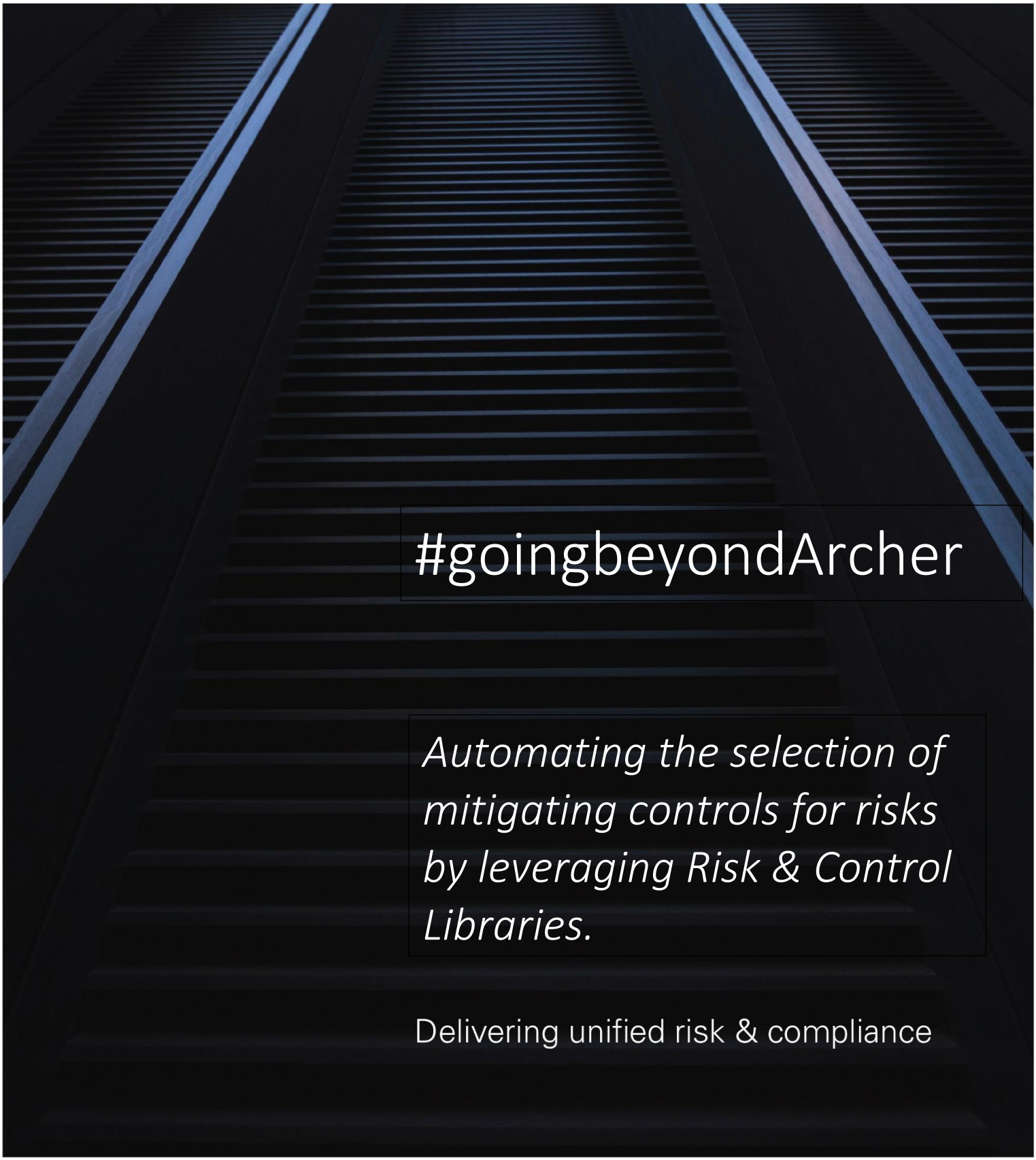
BOWMEN GROUP



#goingbeyondArcher

Automating the selection of mitigating controls for risks by leveraging Risk & Control Libraries.

Delivering unified risk & compliance

RISK &CONTROL LIBRARY

Introduction

This document details the Bowmen Group Limited (BGL) approach to implementing a Risk & Control library within the RSA Archer eGRC product. This approach has been used successfully with multiple customers and is currently in use in production environments. The example screens shown are included only as indicators of layouts taken previously; future engagements can use different screen and field configurations successfully with the underlying principles of this approach.
For further details and to discuss using this approach please speak to your BGL representative or e-mail info@bowmengroup.com.

Use Case

To achieve an advanced level of maturity to the Risk Identification & Management and Control Definition portion of eGRC it is often seen as desirable to centrally develop and maintain a Risk and associated Controls library within an organisation. This library can then be used for the business as a starting point to the identification and management of Risk as well as providing current best practice for Controls definition against those Risks.
Key points to make this workable are:

- The Risks should be copied from the library based on matching patterns against different Business Units / Processes / Teams (or any other granularity choice)
- The Controls should be copied, along with the Risks, with perhaps further filtering being applied
- If the library is updated, any real-world copies of Risks and Controls should (in some way) reflect these updates
- The library should be plastic rather than defined once and never touched again

Approach

Library Concept

The central idea behind the concept of a Risk & Control library is to introduce 2 new Applications (RSA Archer terminology, see

Glossary):

- Risk Library: holds the basic, generic definition of a Risk Register item; includes links to the Risk Hierarchy or other way of classifying the library item for matching where to copy it
- Control Library: holds the basic, generic definition of a Control Procedure item; includes links to the Risk Library to know where to copy this out as well as (potentially) further classification on where to apply this item in the business

The maintenance (creation of new items, updating of existing items and retirement of existing items) of these library applications is (usually, but not exclusively) performed by a central team of risk experts within the company. Changes to the library based on business feedback are dealt with outside of the system, although automated ways of doing this can be discussed.

Classification

A central tenant of the library is that the Risks (and, potentially, the Controls) are categorised in some way so that the system knows where they should be copied out within the business based on the Business Units also being categorised in a matching way. The most common, but not exclusive, way of doing this is to use the existing Risk Hierarchy application; in this way, a Risk in the library is linked to a single Risk Hierarchy item, the Business Units are each linked to as many Risk Hierarchy items as they would normally encounter in their daily business and the system then publishes out copies of the appropriate Risk Library records to each Business Unit (see the sections below on publishing methodologies for details on when and how this happens). The associated Control Library records are taken as part of this publish and copied out to the business also.
While it is common to use the Risk Hierarchy for this classification approach it can also be done in other ways – classification by Business Processes, simple fields or other ODAs are also feasible. Equally, this approach discusses publishing out per Business Unit, but Risks could be published out to Facilities, Business Processes or any other Application.

Publishing

Once the library has been defined and each item classified, the system needs to be told when to publish the new Risks & Controls to the Business.
Individual Risk & Control records within the library can be marked as 'Draft' so that they aren't published until they are ready.

Post-Publishing

Once the publishing has happened, the copies of the Risks & Controls in the wild should remain linked to the Library to allow for easier identification and updating in future as well as to easily allow for centralised (or localised) reporting of performance of library Risks & Controls.
The system also caters for the ability of the business to mark Controls as duplicates of existing Controls they already have in place by linking both the library copy and the parent Risk to the pre-existing Control they have.
There are two main ways to cater for future updates from the library to the business Risks:

- Automatically updated fields (calculated fields) on the object, utilising the linkages between the Risks & Controls and the library entries
  AND / OR
- An overwrite from the library out to the business copy of the Risks & Controls

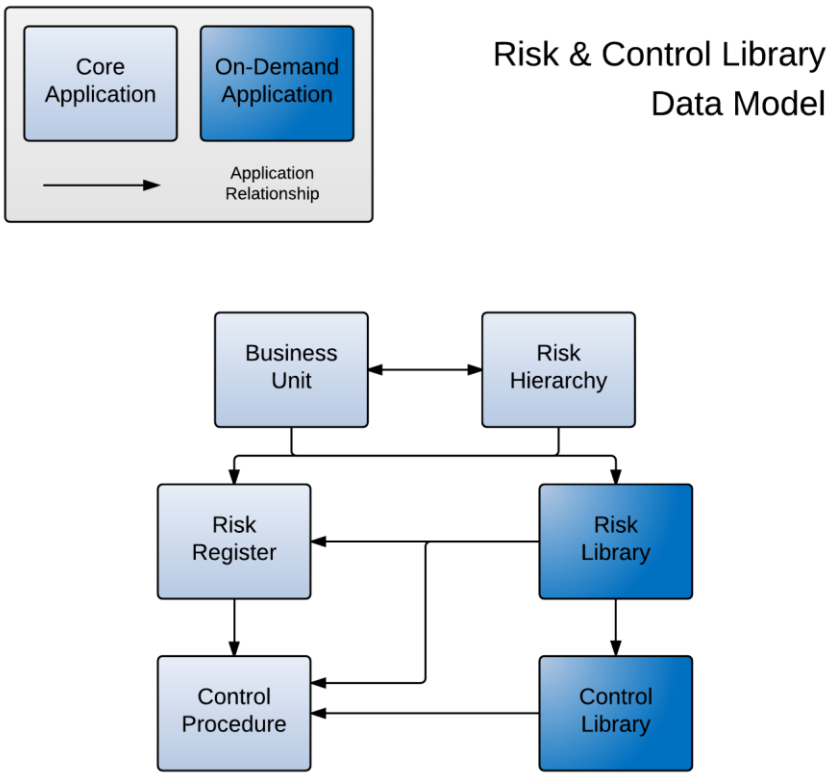
Shared Controls

Truly shared Controls differ from shared Control Templates and Control Standards – truly shared Controls are Controls operated by a single Business Unit / team / function which mitigate Risks held in other areas of the Business, whereas a Control Template or Control Standard is a standard methodology for Controlling a Risk used in multiple areas of the Business. The key point to differentiate them is that if a shared Control instance fails then **all** Risks controlled by it are impacted – an example of this might be a firewall device that is patched by a central IT team and behind which sit multiple systems used by different Business Units; if the firewall patching isn't performed then Risks managed by the Business against those systems will all be potentially impacted

.

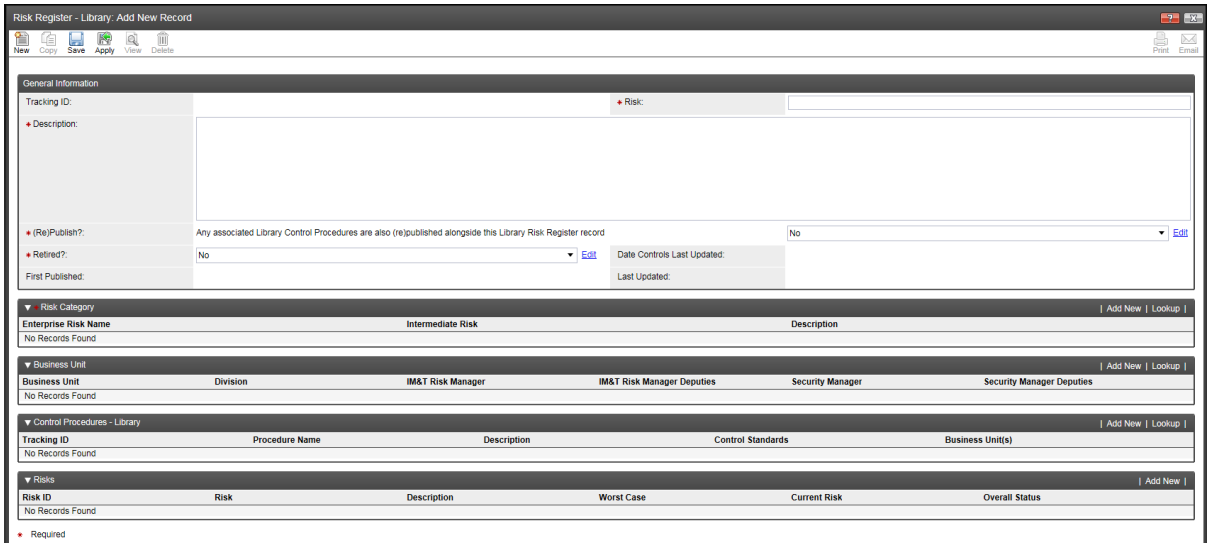
The library methodology described above only talks about Control Templates / Standards; if you wish to utilise shared Controls as well then the publishing can be customised to allow for this – a Risk in the library can then be attached to both library Controls as well as actual shared Control Procedures. Any published copies of the Risk will then pull along copies of the library Controls (unique instances per Business Unit) as well as maintaining links to the shared Control Procedures already in place.

Example Object Model

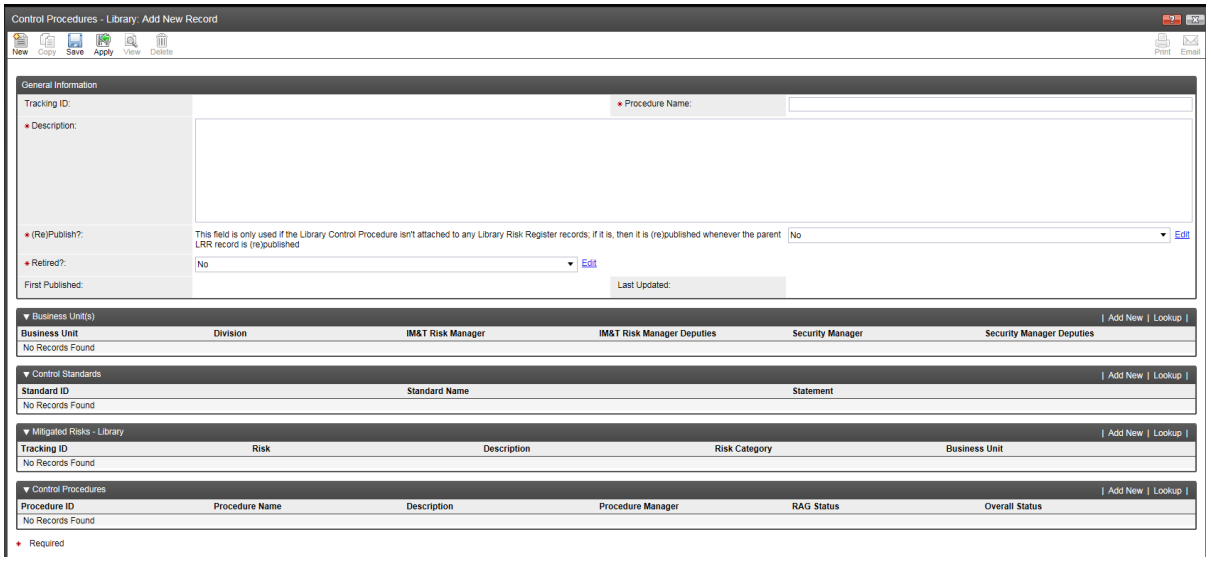


Example Screens

Example Risk Library Screen



Example Control Library Screen



Technical Requirements

For the system described above, the following are the necessary requirements:

i. A working RSA Archer system
ii. At least 2 available Datafeed slots (more may be needed depending on the complexity of the filtering involved for the publishing side)
iii. At least 2 available ODAs (more may be needed depending on the complexity of the filtering involved)

For quotes and pricing of BGL time to implement the solution please contact your BGL representative or info@bowmengroup.com.

Glossary

TERM	DEFINITION
Application	Within RSA Archer, an Application is the term used for a form / data screen / 'bucket' for a particular type of data; i.e. the Risk Register is held in an Application, the Control Procedures are held in a separate Application
Datafeed	Within RSA Archer, a Datafeed is an automated, scheduled process that manipulates data in the system (or imports data from external systems).
ODA	Within RSA Archer, an ODA is an On-Demand Application; this is an Application (see above) that is a blank sheet in terms of starting point and can be configured to capture any kind of data. These are purchased from RSA.