**Risk Management Practionner Guide:**

**Chapter 1: Risk Management Overview**

**Definition**:

Risk is the effect of uncertainty on an organization’s objectives. Risk is the product of the probability of an event and its consequence. Risk events are commonly considered to be negative outcomes that result in hard and soft costs.

Risk management is the process of identifying, analyzing, and either accepting or treating the

uncertainty in your company. Proper treatment procedures involve mitigation by reporting upon and monitoring the uncertainty. The practice of risk management is pervasive across all geographies and industries, although the degree to which the practice is formalized and operates varies by geography, industry, and organization

**Benefits of Archer Risk Management:**

Higher customer retention and growth

l Improved loss control

l Lower cost of capital and borrowing costs

l More efficient capital utilization

l Higher stock price and increased shareholder value

l Lower risk transfer costs

l Enhanced reputation and brand value

l Greater job security and success of management

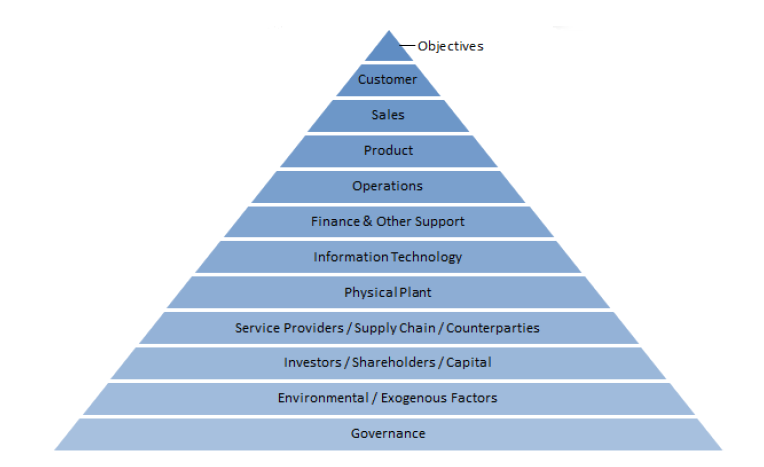
l More accurate product pricing

l Consistency with regulatory expectations

l Protection of directors and officers from shareholder suits

l Improved corporate governance and efficiency

**Organizational Dependencies**



Each layer and its associated people, processes, and technologies are necessary to achieve the organization’s objectives and to successfully deliver the product to customers. To maximize

Objectives, Governance manages each layer within constraints set by Management, the Board of Directors, and Regulators. However, risks may arise within any one or more of these layers that threaten the organization’s ability to achieve its objectives. For example, some of these risks include:

l Human errors

l Internal or external fraud

l Information security breaches

l Disaster or Business Interruption

l Violations of law and regulation

l Product liability claims

l Employee injuries

l Employee litigation claims

l Supply chain interruption

l Third-party non-performance, error, or fraud

Property damage

l Customer credit default

l Inability to effectively market product

l Manufacturing defects

l Poorly designed processes and technologies

l Failed M&A integration

l Inadequate capital or inability to raise capital

l Political risk, domestic & foreign

l Terrorism, civil unrest, war

l Inadequate liquidity

l Environmental damage

l Inability to attract and retain qualified employees

l Competition

l Foreign currency fluctuation

l Income deterioration from interest rate changes

l Deterioration in investment values

l Inflation

l Sub-optimal execution

l Product obsolescence

l Insufficient market demand

**Risk Management Standards**

AAIRM, l BASEL II/III, COBIT 5, COSO ERM, ISO 27001 / 27005, ISO 31000 / 31010, M\_o\_R, NIST SP 800-30, 37, 39 & 53, PMI Practice Standard for Project Risk Management, Solvency II

Organizations building a risk management program will typically adopt pieces of one or more

standards and tailor them to fulfill their specific risk management requirements. RSA Archer

solutions are designed to accommodate whatever standard or hybrid standard that an organization may select. The out-of-the-box RSA Archer Risk Management solution addresses the broad principles outlined in ISO 31000 and the OCEG GRC Capability Model. If needed, through configuration, organizations may tailor their RSA Archer solutions to accommodate most unique requirements not addressed out-of-the-box, including turning on and off features if and when needed.

**Chapter 2: Program Considerations**

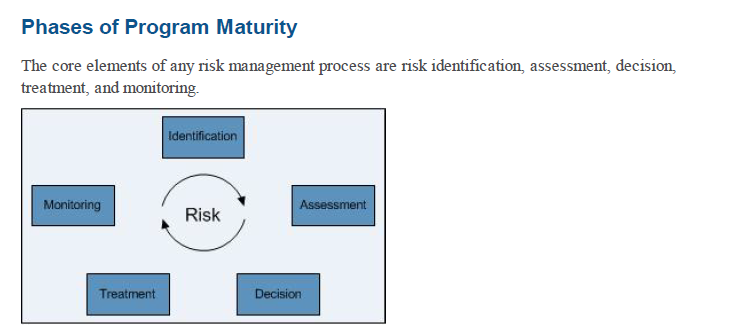
There are several important considerations that influence the level of maturity of an organization’s risk management program. Carefully evaluate each of these considerations prior to implementing a risk management program to ensure that there is a clear understanding of the organization’s current approach to risk management, and the preferred end-state program. While it is not necessary that all of the following considerations be fully resolved prior to implementing the RSA Archer Risk Management solution and its related solutions, RSA recommends that they be evaluated with respect to the organization’s risk management roadmap, timeline, and their impact on the overall success, effectiveness, and efficiency of the organization’s risk management program

**Program Scope:**

Organizations that take an enterprise view of risk management face more challenges when initiating a program, but the long-term benefits are much more significant. Risk management programs that are targeted to specific pain points without first establishing a holistic enterprise perspective may foster silos of inconsistent risk identification and assessment, inconsistent risk treatment, and risk decisions that are not aligned from one part of the organization to the next. This will also make it much more difficult in the future for an organization to bring together the various risk management approaches into one harmonized, consistent approach.

Typically, organizations just starting a risk management program establish a multi-year roadmap to move from the current state to the desired end-state. Organizations that have a more mature program may not require a multi-year roadmap; simply migrating their existing program to RSA Archer solutions may fulfill their objective. In any case, a necessary first step is to identify the target and scope of the risk management program within their organization.

Will the use of the RSA Archer Risk Management solution and any related solutions be targeted to a specific area of the organization or business process, such as IT-GRC, business continuity, vendor, SOX, etc., or will the program be deployed to eventually encompass the entire organization? It is important to answer this question because it significantly impacts decisions that should be made to ensure that a successful long-term program is efficiently implemented with the fewest possible miscues.



Risk management program maturity can be characterized in at least three phases across each risk management process. It may be helpful to a practitioner in assessing their program and developing their roadmap to evaluate each of these phases.

**Risk Identification Maturity**

**Phase1**: Identification of risks limited to auditors and executive management

l Risks may not be broadly identified and well documented

**Phase2:** Risks are assigned to owners, l Owners are educated about what risk is, its relationship to other framework elements, and how to identify it l A formal risk register exists l Classification of risks by category l ERM framework documentation in process l Primary focus on risks of something going wrong

**Phase3:** Good (strategy and opportunity) and bad risks included in risk identification l RM framework substantially documented and change control implemented l Defined risk universe is routinely reaffirmed up and down the organization typically through Risk & Control Self-Assessments completed by 1st Line of Defense Managers l New and emerging risks regularly solicited and evaluated l Root cause analysis of near misses and external loss events

**Risk Assessment Maturity**

**Phase1:** Ad-hoc assessment of risk l No consistent risk vocabulary l No consistent assessment

Methodology l No consistent definition of when risks would be considered significant

**Phase2:** Agreed upon risk measurement approach l Standardized risk rating scales used throughout the organization l substantially qualitative assessments l some metric based assessments

**Phase3:** Assessment approach consistent enterprise-wide l Significant risk quantified wherever possible using non-subjective metrics l Awareness of interdependent risks l Risks assessments are harmonized l Evaluating actual losses and near misses against expected losses & external data l Use of Key Risk Indicators and loss root cause analysis in risk assessments

**Risk Decision Maturity**

**Phase1:** Line managers not explicitly aware of risk ownership l Risk appetite and tolerance not defined l Authority to take risk is not clearly defined and delegated l Risk decisions are ad-hoc and inconsistent l Many risk decisions are heavily influenced by auditors

**Phase2:** Some delegated authorities are formally approved and communicated l Delegated authorities may be inconsistent across processes, risks, risk impacts, and management levels

l Process of escalating and documenting risk decisions not handled consistently

**Phase3:** Risk appetite and tolerance formally and consistently defined for all major risk categories l Managers understand their risk taking authority l Systems enforce authorities where

Appropriate l Systems escalate exceptions to managers with appropriate authority and decisions are formally documented

**Risk Treatment Maturity**

**Phase1:** Internal controls may be documented by auditors l The relationship between controls and the risks they mitigate may not be clear

**Phase2:** Controls are assigned to owners l Owners are educated about controls, why they are important, and how to identify and describe them l A formal control register exists that is linked to risks, policies, and regulations l Owners periodically attest to the operation of controls l Control design and effectiveness assessments and tests are captured

**Phase3:** Consideration of all risk treatment types, not just controls (insurance and hedging) l Remediation plans to bring risks and risk drivers within tolerances are formalized and actively managed l Total cost of risk is considered, where significant and risk treatment adjusted when not justified.

**Risk Monitoring Maturity**

**Phase1:** Limited use of metrics l Reporting is burdensome and mostly manually compiled l Some risk reporting is ad-hoc and focused on the risk du jour l Risk & control gap reports are not available or easily compiled l No central repository of remediation plans.

**Phase2:** Some metrics (primarily loss monitoring) used within the organization l Risk and control register reporting exists that may rollup into summary and executive level reports l Gaps, outstanding issues, and remediation plans are centrally compiled and monitored

**Phase3:** Metrics widely implemented and monitored around significant RM framework elements

l Robust, actionable, reporting is in place at all levels of the organization l RM framework elements that deviate from specified tolerances are automatically reported to key stakeholders

l Gaps and issues that are not remediated within agreed upon timeframes are automatically

escalated.

**Governance Considerations**

Creating a risk management culture, establishing consistent risk management practices across

business processes, and operationalizing those practices on a day-to-day basis requires the

commitment of management at all levels, especially that of senior management. Without adequate senior management commitment, competing management priorities will crowd out risk management initiatives.

The broader the scope of the program, the higher up in the organization the commitment

should be voiced. For example, commitment to an IT GRC program should be formally

communicated by the CTO or COO while commitment for an Enterprise Risk management program should be voiced by the CEO, Chairman, or the Board of Directors

commitment to strong risk management governance include:

A statement issued by executive management regarding the importance of risk management and the expectation that all managers embrace risk management practices

l Formalized risk management practices approved by executive management, a risk management committee, and/or the board of directors that are periodically reaffirmed and communicated to every manager

l At least annual affirmation by all managers that they understand their role in risk management.

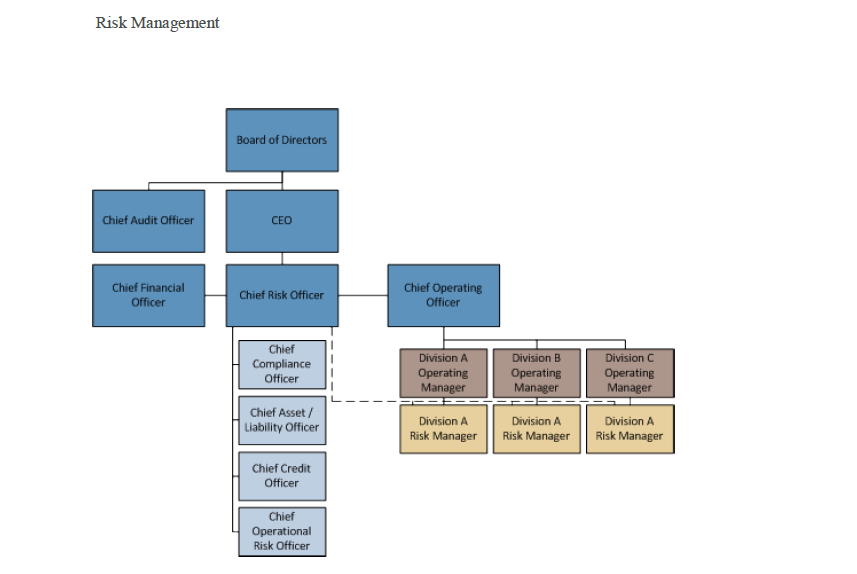
This goal may be achieved through periodic business unit manager reaffirmation of their risks and controls and/or by way of a periodic affirmation of the organization’s code of conduct

l Addition of a formal management objective related to the practice of sound risk management

l Formalized compensation claw-back provisions for risk taking that materially deviates from

approved practices.

**Risk Management Organization**



Regardless of the governance structure selected, the structure should establish the following:

Every organizational entity is assigned an owner

l Every risk is assigned an owner

l Every internal control is assigned an owner

l A documented process exists as to when a risk decision will be escalated and to whom the decision will be escalated

**Risk Identification Considerations**

Practitioners should consider the following issues around the identification of risk when establishing their risk management program in the RSA Archer Risk Management solution:

**Determining the scope of the risk management** framework to be documented: Risk Management related framework elements that may be documented include organizational objectives, products and services, business processes, risks, controls, policies, and regulations. The more framework elements that are associated to one another, the greater the business context within which risk can be assessed, decided, treated, and monitored. Initially, some organizations may choose to limit the framework elements they wish to document in order to get the program up and running while other organizations may choose to document the relationship of all of the framework elements at the same time.

**Establishing the Risk Register**: Organizations that have already identified their risks should load them into the Risk Register. These risks may currently reside in spreadsheets maintained by auditors or imported from legacy GRC systems. Organizations that do not have an established risk register will need to compile their risks. Typically, risks are compiled through interviews with affected managers throughout the organization and through formal Risk and Control Assessments (RCSAs) like those supported in the Archer Operational Risk Management solution

**Establishing the Risk Hierarchy**: Organizations that want to roll risks up from very granular

business unit-focused risk statements to a handful of enterprise level risk statements should agree on the wording of the more summary level risk statements. For organizations that have not identified their business unit level risks, it is helpful to have a list of enterprise-level risk

statements in place before meeting with business unit managers in order to prompt discussions

around whether the business unit has related risks. Inevitably, the process of identifying risk

requires iteration.

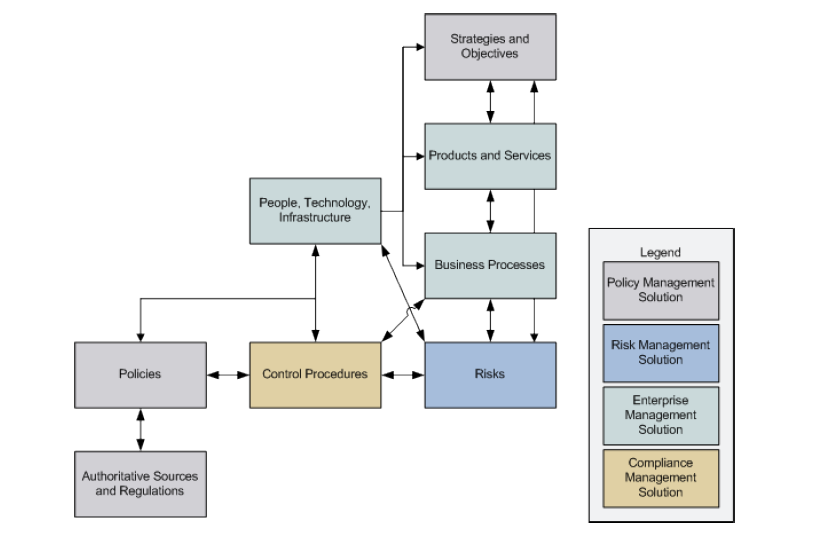
**Establishing risk-related framework ownership**: To create the accountability necessary for a risk management program, owners must be established for documented objectives, products and services, business processes, risks, control procedures, and associated policies. Generally,

owners should be established based on their domain of responsibility related to the framework

element.

l **Reaffirming the Risk Register**: Once the risk register is compiled, the frequency of reaffirmation should be decided. In order to monitor changes in risk profile and to reinforce risk ownership, practitioners should consider reaffirming risk with their owners on quarterly basis.

Conceptually, typical framework elements that can be documented across RSA Archer solutions are depicted as follows:



**Risk Assessment Considerations**

There are two approaches to risk assessment enabled in the RSA Archer Risk Management solution: **top down** and **bottom up.**

**The top down** approach focuses on the assessment by management of risks identified in the risk register through scenario discussions and risk and control self-assessments. Top down assessments validate existing risks and may also result in the identification of new risks to be

added to the risk register.

**The bottom up approach** focuses on assessing the risk of specific projects such as the introduction of new products and services and other ventures and on assessing risk to

infrastructure elements such as IT applications, systems, devices, and facilities. Most organizations will utilize both approaches.

* To ensure consistency across the risk management program, both approaches require management agreement on the following:
* Under what circumstances will qualitative risk assessments be performed?
* l Under what circumstances will quantitative risk assessments be performed?
* l What rating scale will be used for qualitative and quantitative risk assessments?
* What qualitative and quantitative factors will define the scale? In other words, what defines a
* high risk qualitatively and what is the monetary level that defines a high risk rating?
* Under what circumstances if any ,will externally modeled risk score be brought into RSA
* Archer Risk Management solution?
* l Who will perform risk assessments?
* l How frequently will risk assessments be performed and reaffirmed?
* l When will the use of metrics and loss reporting be enabled to inform decisions regarding risk assessment?

**Risk Decision Considerations:**

Risk management is about making risk decisions. Decisions about any particular risk may include one or more of the following decisions:

Accept the risk

l Accept more risk to achieve an objective

l Reject the risk entirely

l Reduce the risk through mitigating control activities

l Reduce the risk through risk transfer

l Reduce the risk by accepting less of the activity that is creating the risk

Efficient and effective risk management programs explicitly articulate each manager’s authority for making risk decisions, which types of risk decisions can be made by whom, and when risk decisions must be escalated to higher authorities based on the type or size of the risk. These items directly impact the way in which an organization will want to set up workflow, notifications, and reporting in the RSA Archer Risk Management solution

Specific examples to consider when creating workflow around risk decisions include:

* At what level of inherent risk (Orange, Red, > $1,000,000, etc.) must a risk be decided?
* l What is an acceptable level of residual risk (Gray, Green, and < $100,000) where no further action is required to mitigate, transfer, or reduce the risk taking activity?
* How much authority does a business unit manager have to accept a risk (such as any risk up to a yellow or $500,000)?
* Who decides risk that exceeds a business unit manager’s delegated authority?
* l Are there certain types of risk that cannot be decided by a business unit manager but must be decided by a risk management specialist (such as litigation risk being decided by the Chief Legal Counsel or M&A strategy being approved by the CEO)?
* How frequently and to whom will stale and outstanding risk decisions be communicated?
* l How frequently will accepted risks or approved risk exceptions be reaffirmed?

**Risk Treatment Considerations:**

Risk treatment includes mitigating control procedures, insurance, and other risk transfer

When documenting control procedures in the Compliance Management solution, it is very important to assign specific management ownership to each record in order to establish management accountability. In order to make use of Risk Management solution reports that depict the impact of inherent risk vs. the cost to mitigate the risk, practitioners should also populate control procedures with an estimate of the cost to maintain the control.

**Monitoring Considerations:**

* Aligning risk management reporting with the organization’s internal financial reporting structure
* Determine those reports and frequency of reporting that risk management specialists and risk management control functions will receive
* Determine the extent to which the organization will implement metrics (KRIs, KCIs, KPIs), the timing of implementation, frequency metrics will be refreshed, frequency by which metrics will be reevaluated for appropriateness and revision, and how the metrics program will be administered.
* Identify those risk management reports that should be routinely provided to different levels of management, and the frequency of such reporting.

**Socialization:**

Organizations that manage risk best are characterized not just by the fact that they have risk

Management programs, but that the programs are socialized throughout their organization so that all employees embrace it. Developing this kind of risk culture requires things such as:

* Formalized risk management practices that are broadly and routinely communicated to

Stakeholder.

* l Risk management education for new and existing managers
* l Operationalizing risk management terminology, reporting, and workflow using RSA Archer solutions
* l Clear accountability for risks, controls, metrics, and exception remediation
* l Tone at the top

**Setup, Change Management, and Administration:**

* Who will oversee that the various aspects of the risk management program are being executed like: Everyone is participating, Reports are generated and distributed properly, Risk and control exceptions are cleared, Risks are identified and assessed consistent with policy, Changes in risk profile are captured and addressed by appropriate management and risk management specialists.
* To what extent should business unit management be allowed to change objectives, products and services, business processes, risk, control, and policy and authoritative source records? Many organizations choose to require changes be approved by dedicated risk managers before the changes are accepted into production.
* Are field names, values lists, and scales used in the RSA Archer Risk Management solution consistent with the organization’s terminology and rating scales?
* Will all field changes be logged, and which ones?
* l To what extent should records be readable and editable?
* Have all circumstances been identified where the organization wants notifications, workflows, and escalations to be triggered?
* Have all desired reports been created for management reporting and administration
* Who will control and approve changes to global risk management reports
* Will any information be archived for historical reporting purposes?

**Chapter 3: RSA Archer Risk Management Solution**

**Architecture**

**RSA Archer Risk Management Solution Architecture**

The following depiction illustrates the applications and associated cross references of the

RSA Archer Risk Management solution.



**RSA Archer Risk Management Solution Integration with Other RSA**

**Archer Solutions**

The RSA Archer Risk Management solution is designed to directly interface with the following

other RSA Archer solutions:

**Solutio**

**Application**

**Name Primary Purpose(s) of the Relationship**

**Enterprise Management** ->

**Contacts**: Establishes individual ownership of the various RSA Archer Risk Management solution records

**Enterprise Management -> Business Unit:**

* l Establishes organizational ownership of the various Risk Management solution records by business unit including risks, loss events, metrics, projects, and assessments
* l Risks by business unit are displayed along with counts of the risk ratings of each risk
* l Risk Levels are displayed by business unit, tolerances can be set by business unit, and monitored against risk levels
* l Key Risk indicators by business unit can be monitored against tolerances
* l Business Units can be monitored using indicators created within the Metrics application
* l Losses by business unit can be monitored against tolerances
* l Threshold for escalation of Losses to various levels of management can be set
* l Business Unit serves as the target for the Business Unit Risk Review application to periodically reaffirm and capture changes in risk profile
* l Business Unit serves as a target for Fraud Assessments

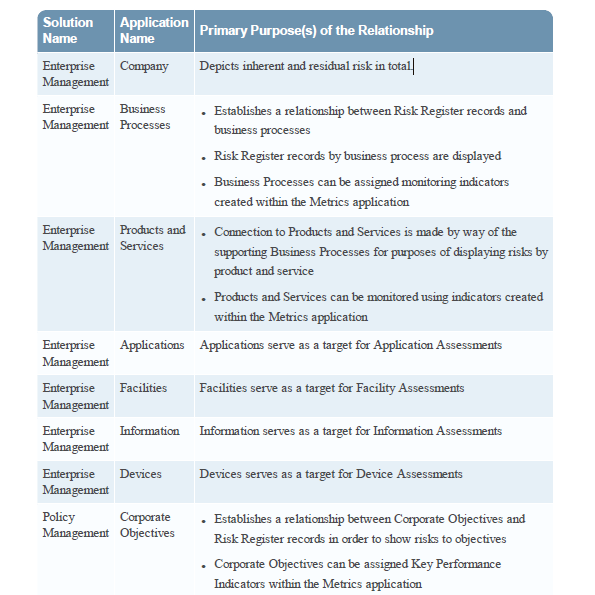
**Enterprise Management -> Division** l :

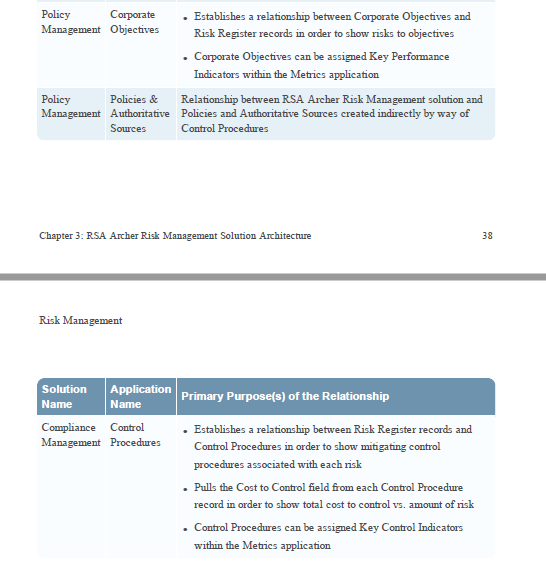
Establishes organizational ownership of the various Risk Management solution records by Division including risks, loss events, metrics, projects, and assessments

l Risks by Division are displayed

l Risk Levels are displayed by Division, tolerances can be set by Division, and monitored against risk levels

l Losses by Division are displayed





**Chapter 4: RSA Archer Risk Management Solution**

The RSA Archer Risk Management solution is designed to provide an organization with a

consolidated view of their risk. Solution allows for top-down and bottom-up risk assessments

that can be performed qualitatively and quantitatively, the ability to assign metrics to risks and other framework elements, track and manage losses, evaluate insurance risk transfer, reaffirm and collect changes in the organization’s risk profile, and monitor risks and metrics against targets, tolerances, and trend expectations.

**RSA Archer Risk Management Solution Component Overview**

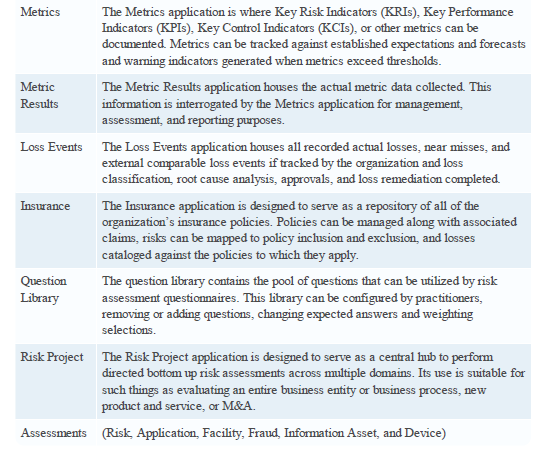
The RSA Archer Risk Management solution contains the following components:

**Risk Hierarchy:** The Risk Hierarchy application contains enterprise risk statements and

intermediate-level risk statements. By linking intermediate risk statements to risk register records and to enterprise risk statements, organizations are able to provide a three level roll-up of risk statements and ratings from the most granular risk register level to the most summary-level enterprise statements.

**Risk Register**: Risk Register application is the container to house the most detailed level of

risk that an organization wishes to track. It is at the risk register level that risks are associated to risk owners, business units, business processes, and risks are assessed from a top-down perspective.

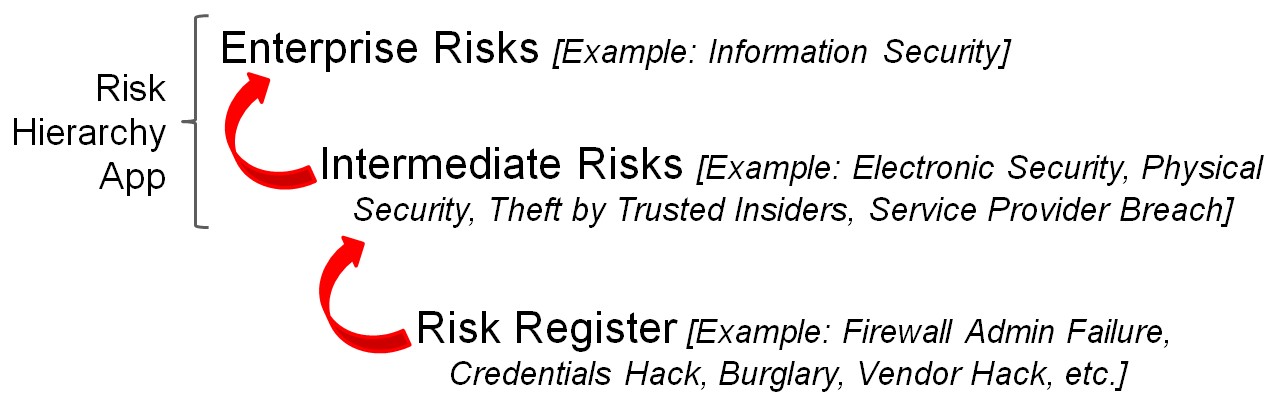


## Risk Management Sub-Solution

The Risk Management sub-solution allows you to identify risks, evaluate their likelihood and impact, relate them to mitigating controls and track their resolution. You can build a repository of reputational, financial, operational, and IT risks; tie those risks to corporate objectives, supporting metrics, and loss events; and deliver targeted risk assessments to evaluate identified risks within your environment. Additionally, you can manage the remediation or acceptance of assessment findings.

## Risk Hierarchy

The Risk Hierarchy application is a two-level application that contains Enterprise Level Risk statements and Intermediate Level Risk statements. In many organizations, Enterprise Level Risk statements are those statements that are reported in public filings such as 10-Ks and 10-Qs(orm **10**-**Q**, (also known as a **10**-**Q** or **10Q**) is a quarterly report mandated by the United States federal Securities and Exchange Commission, to be filed by publicly traded corporations. ... Information for the final quarter of a firm's fiscal year is included in the **10**-**K**, so only three **10**-**Q** filings are made each year.) filed with the Securities and Exchange Commission.



In the Risk Hierarchy application, Enterprise Level Risk statements can be linked to Intermediate

Level Risk statements, and Intermediate Level Risk statements can be cross-referenced to Risk

Register application records. This enables a three-level roll-up of risks from the most granular Risk Register level to the most summary enterprise level and allows a risk manager to traverse the organization’s risk from the top down or bottom up.

By utilizing the Risk Hierarchy application, organizations can: Provide positive assurance regarding published risk statements.

More easily understand the breadth and amount of risk, the drivers of risk, and the associated control framework. Monitor and manage risks against established risk tolerances.

### **Enterprise Level**

### Enterprise: Enterprise Risk Level

The Enterprise Risk level provides the location where you can enter the highest summary level risk. In this level you may assign an enterprise risk owner.

Enterprise: Risk Status

The Enterprise Risk Status tab contains **two sections**: **Risk Levels** and **Risk Tolerances.** It is followed by the Intermediate Risk Level section, which displays all of the intermediate risks associated with the enterprise level risk statement.

The primary **purpose** of the **Risk Levels** section is to provide an understanding of the **average and maximum** amount of the **enterprise level risk**.

* The average risk levels calculated in the Risk Levels section are derived by averaging the same named values from each of the intermediate risks associated with the enterprise level risk record.
* The maximum risk levels calculated in the Risk Levels section are derived by selecting the maximum values across all associated Intermediate Level records.

The primary **purpose** of the **Risk Tolerances** section is to **produce warning indicators**. Warning indicators turn red if one of the following user supplied tolerances is exceeded at the Enterprise Level risk:

* Average Calculated Risk Maximum Calculated Risk
* l Percentage of Failed Controls across all control procedures mitigating risks that roll-up to the enterprise level risk record
* Percentage of Failed KRIs across all metrics associated to risks that roll-up to the enterprise level risk record
* Aggregate loss events over the past twelve months that are associated with risks that roll-up to the enterprise level risk record
* Enterprise: Risk Analytics

The **Risk Analytics tab** of **an Enterprise Risk level record** contains two sections: **Risk Analytics** and **Loss Event Analysis.**

The purpose of the Risk Analytics section is to provide information regarding the distribution of **average and maximum risk ratings across all Intermediate Level risk records** associated with the Enterprise Level risk. Also recorded in this section are the average and maximum percentages of failed controls and Key Risk Indicators (KRIs).

The **average percentage**s of failed controls and KRIs are **calculated from** the **associated Intermediate** Level risk record that is associated with the Enterprise Level risk.

The **maximum percentages** of failed controls and KRIs are calculated from **Metrics** that are associated **with Risk Register** records that are associated with the Intermediate Level risk record.

The purpose of the **Loss Event Analysis section** is to provide information regarding expected and actual loss events across all associated Intermediate Level risk records.

The value displayed in the Total Annual Loss Expectancy field is derived by calculating the sum of all Annual Loss Expectancy values across all Intermediate Risk records associated with the Enterprise Level record. The value displayed in the Total of Loss Events (last 12 months) field is derived by calculating the sum of all Loss Events in the past 12 months that are associated with all Intermediate Risk records associated with the Enterprise Level record.

**Enterprise: Content Provider**

The Content Provider Information tab on Enterprise level application can be used to document and track the source and version of enterprise level taxonomy that may have been acquired from a third party (such as Risk Business International) or sourced internally.

### **Intermediate Level**

**Intermediate: General Information**

The Intermediate Risk field provides the location where you can input intermediate summary level risk statements. In this level, you can associate the Intermediate Risk statement to an Enterprise Risk statement, and to an Intermediate Risk Owner

**Intermediate: Risk Status**

The Intermediate Risk Status tab contains two sections: Risk Levels and Risk Tolerances. These are followed by the Risk Register section, which shows all of the Risk Register records associated with the intermediate level risk statement.

The primary purpose of the Risk Levels section is to provide an understanding of the **average and maximum** amount of the Intermediate Level risk.

* The **average** risk levels calculated in the Risk Levels section are derived by averaging the same named values from each of the risk register records associated with the intermediate level risk record.
* The **maximum** risk levels calculated in the Risk Levels section are derived by selecting the maximum value across all associated Risk Register records.

The values displayed in the Maximum Qualitative Inherent Risk and Maximum Quantitative Residual Risk fields are derived by examining the quantitative risk assessments across all associated Risk Register records and returning the maximum values.

The primary purpose of **the Risk Tolerances** section is to produce warning indicators. Warning indicators turn red whenever one of the following user supplied tolerances is exceeded at the Intermediate Level:

* Average Calculated Risk Maximum Calculated Risk Percentage of Failed Controls across all control procedures mitigating risks that roll-up to the intermediate level risk record
* Percentage of Failed KRIs across all metrics associated to risks that roll-up to the intermediate level risk record
* Aggregate loss events over the past twelve months that are associated with risks that roll-up to

intermediate level risk record

**Intermediate: Risk Analytics**

The Risk Analytics tab of an **intermediate risk level record** contains two **sections**: **Risk Analytics and Loss Event Analysis**. These are followed by the **Risk Register section**, which shows all of the Risk Register records associated with the intermediate level risk statement.

The **Risk Analytics section** provides a **count of each Risk Response** Type indicated on all associated Risk Register records. It also provides a count of all of the Inherent Risk, Residual Risk, and Calculated Risk ratings across all associated Risk Register records.

The values displayed in the **Average** % of Failed Controls and Average % of Failed KRIs are calculated from Control Procedures that are associated with Risk Register records that are associated with the Intermediate Level risk record.

The values displayed in the **Maximum** % of Failed Controls and Maximum % of Failed KRIs are calculated from Metrics that are associated with Risk Register records that are associated with the Intermediate Level risk record.

The **Loss Event Analysis section** provides information about **annual and average losses**. The **Total Annual Loss** Expectancy is derived by calculating **the sum of all Annual Loss Expectancy values across all Risk Register Records** associated with the Intermediate Level Risk record. The Total of Loss Events (last 12 months) is derived by calculating the sum of all Loss Events in the past 12 months associated with all Risk Register Records that are **associated with an Intermediate Level Risk record**. The Average Amount of Loss Events is derived by calculating the average of all Annual Loss Events across all Risk Register Records associated with an Intermediate Level Risk record.

**Intermediate: Content Provider**

The Content Provider Information tab can be used to document and track the source and version of enterprise level taxonomy that may have been acquired from a third party.

## Risk Register

It is the repository where risks are stored, cataloged, assigned to risk owners, and associated to other ERM framework elements. Organizations also use the Risk Register application to document mitigating controls and insurance, and to relate losses and KRIs to monitor risks. The Risk Register application can then inform an organization about their risks and provides the necessary transparency to react to risks that exceed acceptable levels.

The following sections are found within the Risk Register application.

Risk Register: General Information

The General Information section of a Risk Register record is the area where an organization documents their most granular risk statements, assigns those statements to the business unit where the risk resides, assigns the accountable risk owner, and the accountable risk manager.

The Status field indicates if the record is In Development, Active, or Inactive (not in production). Only risk register records that are in Active status are scored for reporting purposes.

The Assessment Approach field indicates which type of risk assessment (Qualitative Survey or Quantitative Survey) will be utilized in scoring and rolling-up risk register record scores.

**Risk Register: Overall Risk**

* Inherent, Residual, and Calculated Residual risks are derived from other areas of the Risk Register record. Their values are carried up from the qualitative or quantitative assessment survey. Calculated Residual Risk field displays information dependent on the selected assessment approach.
* Volatility (the speed at which the risk may arise or how rapidly the risk may change), Likelihood and impact direction on an inherent risk basis (absence of risk treatment) and on a residual risk basis (considering the design and operation of current risk treatments) are supplied by the subject matter expert.
* Annual Loss Expectancy field displays Annual Residual risk from the Quantitative Risk assessment.
* The Calculated Risk Override field and Calculated Risk Override Justification field may be utilized by a practitioner to document any circumstances where the subject matter expert disagrees with the system generated Calculated Residual Risk value.
* The Warning Indicator field generates a red status whenever the Calculated Residual Risk field value is greater than the Residual Risk value. Calculated Residual risk bumps the value of the subject matter expert’s Residual Risk score based on the existence of open findings, actual losses that exceed expected losses, failed key risk indicator metrics, and controls that are not operating. So, when the Warning Indicator is red, it means that something is going wrong with the associated risk treatments that may warrant attention.

### **Risk Analysis**

**Risk Analysis: Qualitative Survey**

The Qualitative Survey section of a Risk Register record provides **one of two ways** that a risk register record can be assessed using a **top-down approach**. In a **qualitative assessment**, a **subject matter** expert provides an **assessment of the risk likelihood and impact on an inherent risk** basis (in the absence of risk treatment) and on a residual risk basis (after considering the existence of risk treatments in place). The **values that appear in the Inherent Risk - Qual and Residual Risk - Qual sections** are derived by multiplying the likelihood of the risk with its impact.

While **qualitative** assessments can provide a quick and dirty idea of the significance of a risk, there are some inherent **weaknesses** with a qualitative assessment approach that should be considered:

* Qualitative scales can be **subject to broad interpretation** unless all assessors are operating from **well-defined explanations of the risk rating scales used for likelihood and impact**. It is important to be as explicit as possible in defining the meaning of likelihood and impact scales, to make the definitions as easy as possible to interpret, and make the definitions understood and used by all assessors.
* Qualitative likelihood scales, if defined as a probability of 0 to 100%, obscure risk events that occur multiple times during **the specific period being a**ssessed.
* Qualitative impact scales obscure the significance of high risks. For example, if high risk is defined as anything over $10 million, risks that have an inherent impact of $100 million will appear as significant as a $10 million risk
* Risks that have been qualitatively assessed are much more difficult to aggregate. If aggregation is an objective, practitioners must consider questions such as: What is the value of two low risks – a medium? Or, how high are two high risks – super high?

Because of these limitations, practitioners should consider the role that qualitative assessments will take in their risk management programs. A good balance between the simplicity and speed of qualitative assessments and the more complex and time consuming quantitative or modeled assessments may be found by taking an iterative risk assessment approach.

**Risk Analysis: Quantitative Survey (Important!!)**

Quantitative Survey section of a Risk Register record provides an alternative approach to a top-down risk assessment that requires the subject matter expert to estimate risk impact in monetary terms, and risk likelihood in terms of the frequency of occurrence. Like the qualitative approach, this assessment is performed on an inherent basis, and on a residual risk basis. Instead of assessing the risk in one overall assessment of impact and likelihood a quantitative assessment requires the assessor to consider how the risk manifests itself over multiple risk categories.

Evaluating risk using risk categories better enables an assessor to consider all ramifications of a risk. It is very common that a risk will manifest itself across more than one risk category, and the impact associated with each risk category will vary. **For example**, an information security breach involving customer records creates operational risk as well as reputation risk. The operational risk component includes the cost to remediate the breach, fraud loss customer reimbursements, and the cost to provide required notifications. The reputation risk component represents customer runoff and slow on-boarding of new customers due to publicized poor information security practices.

Risk category-related assessments are supplied by the subject matter experts in **Quantitative Survey Risk Category Sub-Forms**. The monetary values across all completed Risk Category Sub-Forms populate the Worst Case and Typical Case Exposure category fields, and these fields are summed to produce the Worst Case Total Financial Exposure and Typical Case Total Financial Exposure fields.

Subject matter experts provide estimates of the Frequency of Occurrence **Without Controls** and Frequency of Occurrence **With Controls** by selecting from drop down lists populated with the following time periods: Daily, Weekly, Monthly, Quarterly, Once a year, Once every 1-5 years, Once every 5-10 years, and Highly Unlikely.

The Annual Inherent Risk field is derived by multiplying the Worst Case Total Financial Exposure by the Frequency of Occurrence Without Controls field and the Annual Residual Risk field is derived by multiplying the Typical Case Total Financial Exposure by the Frequency of Occurrence With Controls field.

The Overall Risk section of a Risk Register record contains the fields Inherent Risk and Residual Risk. care should be exercised to ensure that the qualitative and quantitative scales are harmonized as much as possible.

**Risk Analysis: Quantitative Survey Risk Category Sub-Form**

The Quantitative Survey Risk Category Sub-Form is used to capture each category of risk included in a quantitative assessment.

In the **Risk Category field**, the subject matter expert selects one of the following options:

Compliance/Litigation, Credit, Financial, Liquidity, Market, Operational, Reputation, or Strategic. Organizations should tailor this value list to match **the risk categories** that they use. With each risk category sub-form added, one risk category is selected, and a **description** is provided in the Description field to explain how the risk arises related to the category selected.

In the **Worst Case section**, the subject matter expert provides a description of the scenario that would produce the worst case outcome of the risk, and the estimated monetary value. The Worst Case Likelihood may be indicated qualitatively, or this field may be removed from the form layout if relying solely on the Frequency of Occurrence Without Controls field on the Quantitative Survey to reflect the likelihood of occurrence.

In the Typical section, same but difference is, A typical scenario is analogous to a residual risk estimate, The Typical Case Likelihood may be indicated qualitatively, or this field may be removed from the form layout if relying solely on the Frequency of Occurrence With Controls field on the Quantitative Survey to reflect the likelihood of occurrence.

**Risk Analysis: Monte Carlo Simulation**

Using the RSA Archer Risk Management solution and Palisade @Risk allows you to perform risk analysis by running Monte Carlo simulations on your Risk Register application records, and calculating inherent and residual risk. The Monte Carlo method takes randomly sampled input data and runs a risk analysis simulation hundreds or thousands of times in order to give you a probability distribution of all possible outcomes.

The integration supports two different calculation methods: Expert Elicitation and Historical Loss Data. The Expert Elicitation method is based on expert predictions, whereas the Historical Loss Data method is based on actual previous values.

### **Risk Response and Treatment**

The Risk Response and Treatment sections of a Risk Register record are described as follows:

For each assessed risk in the Overall Response section, the risk Response Type (Avoid, Accept,

Reduce, or Share), Response Description, and Expected Response Date are assigned. The Response Status is indicated as Not Started, In Process, or Completed, as appropriate. Response Status fields that are not Completed can be monitored and managed against Expected Response Dates and individual tasks established and assigned through the Task Manager. A reviewer or sign-off field could be added to this section to be completed by an independent party validating that the response is indeed completed properly.

If the Response Type selected is Reduce, one or more control procedures must be established to mitigate the inherent risk. The Mitigating Control Procedures section provides a cross-reference to Control Procedure records contained in the RSA Archer Compliance Management solution. The Residual Risk Analysis section provides summary details regarding all of the control procedures assigned to the risk, including the cost of maintaining these controls, provided those costs have been recorded on the Control Procedure records in the RSA Archer Compliance Management solution.

If the Response Type selected is Share, and the sharing is achieved by transferring risk under an insurance contract, the applicable insurance policy is cross-referenced from the Insurance application in the RSA Archer Risk Management solution.

### **Risk Monitoring**

The sections of a **Risk Register** record that appear under the **Risk Monitoring** tab include Create Key

Risk Indicators (**KRIs**), Key Risk Indicators, and **Related Loss Events.** A Key Risk Indicator is a qualitative or quantitative **metric that describes a risk, providing an indication** of the impact, likelihood, or direction of the Risk Register record.

The Create Key Risk Indicators section enables you to create risk-specific KRIs using the Metrics Library. This section is disabled if there is no Business Unit Risk Owner assigned to the record. **KRIs are stored in the Metrics application.**

The **relevance of KRIs** appearing in this section is to provide practitioners with an understanding of the drivers of the risk and whether the drivers are outside desired specifications and management attention is warranted.

**Loss Events** are actual losses, near misses, and harmonized external loss events (if applicable), and in this section, Risk Register records are associated with their related Loss Events. Loss Events are important to monitor in order to understand the impact and likelihood of a risk; to determine the accuracy of management assessments; and to analyze the root cause of losses. Proper analysis of the root cause of losses enables practitioners to accurately understand the associated risk, and to effectively design and operate the risk treatments.

### **Calculated Risk**

Calculated Risk tab derive an Adjusted Qualitative Residual Risk or Adjusted Quantitative Residual Risk depending on the risk assessment type being performed on the Risk Register record (Qualitative or Quantitative).

The two sections of a Risk Register record that appear under the Calculated Risk tab include **Calculated Risk Factors** and **Calculated Risk Levels.**

The **Calculated Risk Factors** section contains information about **KRIs and Control Factors**. The KRI

Scorecard field contains counts of statuses of all of the Metrics (KRIs) associated with the Risk Register record. The value displayed in the **Percentage of Non-Compliant Controls** field is derived from all Control Procedures associated with **the Risk Register record**. The value displayed in the **Percentage of Open Findings field** is derived from all the Findings associated with the **Risk Register record**. The value displayed in the Percentage of Failed Metrics is derived by dividing the Current Status Fall Metrics by the sum of the Current Status Pass Metrics and the Current Status Fail Metrics

The Calculated Risk Factors section also contains information regarding **Loss Events** and **Impact Analysis**. The value displayed in the **Total Loss Amount** field is derived by calculating the s**um of the net loss** of all loss records associated with **the Risk Register record**. The value displayed in the **Average L**oss Amount field is derived by calculating the **average o**f the net loss of all loss records associated with the Risk Register item. The value displayed in the **Actual Annualized** Loss Amount field is derived by calculating the **sum of the net loss of** all approved losses that have occurred within 365 days of the current date.

The **Calculated Risk Levels** section contains information about Adjusted Qualitative Risk Levels and the Adjusted Quantitative Risk Level.

The value in the Adjusted Qualitative Risk Impact field evaluates expected losses against the actual loss events occurring in the previous 365 days. If **Actual Net Losses exceed Expected Losses**, the qualitative residual risk impact is increased by one risk level.

The **Adjusted Qualitative Residual Risk** field provides an estimation of **the overall risk** to the organization taking into account the **Qualitative assessment and any failed metrics, non-compliant controls, open findings, and variance between annual expected losses and actual losses.** This field visually displays the sum of the Adjusted Qualitative Risk Impact and the Adjusted Qualitative Risk Likelihood.

The **Adjusted Quantitative** **Residual Risk** field provides an estimation of the overall risk to the organization taking into account the Quantitative assessment and any failed metrics, non-compliant controls, open findings, and variance between annual expected losses actual losses. **This field visually displays Residual Risk -** Quant adjusted upward by 1 if the percentage of failed metrics, open findings, and non-compliant controls is greater than 0 or if the actual loss amount is greater than the annual expected losses, or it is adjusted upward by 2 values if both the percentage of failed metrics is greater than 0 and the actual loss amount is greater than annual expected losses.

The **Calculated Residual Risk field appearing in the Overall Risk section** of a risk register record equals the Adjusted Qualitative Residual Risk field if the Assessment Approach is Qualitative Survey, or it equals the Adjusted Quantitative Residual Risk field if the Assessment Approach is Quantitative Survey

### **Mappings**

The Mappings tab of a Risk Register record contains two sections: Company Objectives and

Business Processes.

**Risk Metrics**

An important component of effective risk management involves the identification and monitoring of relevant metrics associated with ERM framework elements. Metrics, often referred to as Key Risk Indicators (**KRIs**), Key Compliance Indicators (**KCIs**), and Key Performance Indicators (**KPIs**), are core to the measurement and monitoring of risk, opportunity, and performance optimization. Through the RSA Archer Risk Management solution, metrics can be cataloged, associated with ERM framework elements, and monitored against expectations and tolerances on an ongoing basis.

The RSA Archer Operational Risk Management application provides a KRI framework through the creation of a KRI library where each KRI is linked to risks and controls. The framework captures the attributes of those KRIs to support an Operational Risk Management program. In addition, organizations are able to set thresholds to monitor the evolution of those KRI.

All Risk Metrics records contain the following global sections:

**Risk Metrics General Information**

A metric is given a name, a description, and is assigned to a metric owner. In addition, the measurement frequency of the metric is indicated and a type of monitoring.

If Type of Monitoring equals:

Threshold then Pass/Fail status determined by the Threshold Status field Trend Alignment then Pass/Fail status determined by the Trend Status field Banding then Pass/Fail status determined by the Banding Status field

In the Targets section, a metric can be targeted to one or more ERM framework elements, and serve as a Key Risk Indicator (KRI), Key Control Indicator (KCI), or Key Performance Indicator (KPI).

### **Risk Metrics Description**

The Description tab of a Metrics record contains the following sections: Metric Information, Collection and Calculation, Advanced Attributes, and Related Metrics. The sections are made up of more than 25 fields, which describe a metric, how it's used, calculated, and its relationship to other metrics.

In the Related Metrics section, Dependent and Prerequisite Metric inter-relationships can be documented.

### **Metrics Analysis**

The Metrics Analysis tab of a Metrics record contains the following sections: Threshold Monitoring, Trending, Banding, and Aggregated Statistics.

**Threshold Monitoring:**

The Threshold Monitoring section includes some configuration fields required to implement monitoring of a value against a threshold. Threshold Monitoring examines a defined value of the metric, compares that value to a specified threshold and returns a status based on the configuration. Threshold Monitoring can be enabled for one of the following: Current Value – The current/last reported value of the Metric.

* Percentage Change – The percentage of change between the Current Value and the Previous Value.
* Average Value – The average value of all Metric Results. Forecasted Value – The forecasted value of the next reporting period.
* Projected Growth – The forecasted percentage of change between the Current Value and the Forecasted Value.

Threshold Monitoring is enabled for one value, but each value is also calculated for the Metric owner to review.

**Trending:** The Trending section contains fields related to the trend of the Metric Results. The fields examine the set of all Metric Results and determine the trend based on the slope of the line plotted using the Metric Date and Metric Result Value. All fields are calculated and require no configuration.

The Trend Alignment field then compares the Trend Analysis and the Trend Expectation set by the Metric owner and determines if the actual trend and the expected trend are aligned. The direction of the arrow indicates the Trend Analysis, and the color of the arrow indicates if the expectation and trend are aligned.

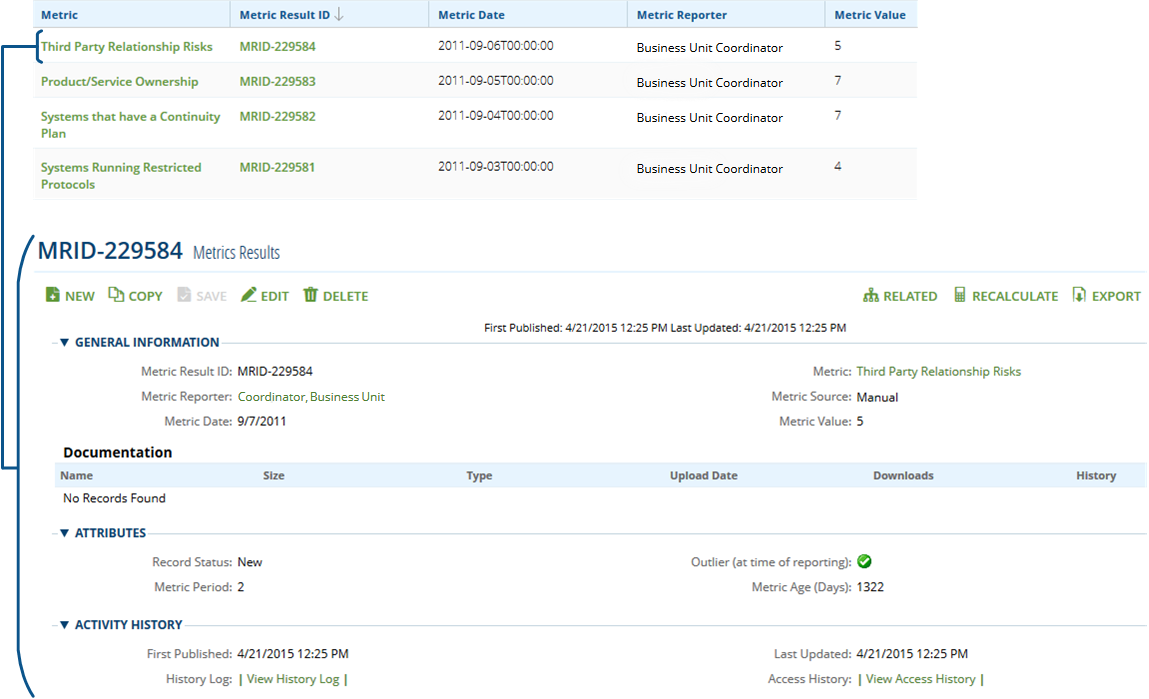
A Negative (or red arrow) means that the trend is opposite of the expected trend. A Positive (or green arrow) means that the trend is the same as the expected trend. A Marginal (or yellow arrow) is used to denote that the trend is one-step away from the expectation.

**Banding**: The Banding section contains fields related to comparing the current value against a range of values as determined by the Average Value and Standard Deviation of the set of Metric Results. All fields are calculated and require no configuration.

The **Aggregated** Statistics section provides Minimum, Maximum and Median values that are calculated from the entire set of Metric Results.

**Metric Results**

The Metric Results section and an example of a Metric Results record is depicted below:



The Metric Results tab includes the cross reference to the Metric Results application. In the Metrics application, the Metric Results tab includes each individual result captured for the metric.

The Metric Results application can capture: Metric Reporter – The person reporting the metric.

* Metric Source – Manual or automated.
* Metric Date – Default Current Day

### **Risk Metrics: Forecast Analysis**

The Forecast Analysis tab of a Metrics record includes a set of up to 5 forecasted values for the metric, based on the entire set of previously reported Metric Results. The forecasted projections are calculated using a Linear Progression based on the existing Metrics Results, and calculated using the FORECAST function. The FORECAST function calculates, or predicts, a future value by using existing values. The predicted value is a y-value for a given x-value.

**Loss Events**

An essential component of an organization’s Operational Risk Management program is the ability to record loss events as they arise, to categorize them to the various categories of operational risk, and to track them to closure. This allows the organization to have a better understanding of the scenario in which the event occurred, implement changes to the control environment to better manage the risk, and ultimately improve the ability to assess risk in the future given the complexities of the operating environments. The latter two tie loss events into the operational risk framework, especially scenario analysis, and risk and control self-assessments (RCSA).

From a regulatory view, a loss database is required, and should be both comprehensive and contain several years’ worth of data. Basel II specifically requires a minimum of 3 years of data initially, and 5 years for the Advanced Measurement Approach (AMA).

RSA Archer Risk Management provides loss event management capabilities within the solution for managing and analyzing internal and external operational events. The Loss Event application has an out-of-the-box workflow that practitioners can configure to better reflect the approach that they want to implement within their organization.

The primary use case around Loss Events is the management of losses to acceptable levels. Capturing and analyzing losses provides management with additional insight into the scope of risks facing the organization, the size and frequency of risk events, the points of failure contributing to losses, and the remedial actions necessary to prevent similar losses in the future.

**Event Classification Section:**

where new loss events are first recorded, including the name, description, amount, affected part of the organization, and various classifications of the source and type of risk. Event type (Actual Loss, Near Miss, or Pending Loss). In addition, it is very important that the loss records maintained in the Loss Events application reconcile to the organization’s general ledger system of record and that the business hierarchy used to classify loss events is consistent with the general ledger classification.

The **advantages of using** the same business hierarchy classifications and reconciling loss events to the general ledger include:

* Avoiding questions between what the income statement is showing for losses and what the Loss Events application is showing for losses. Discrepancies undermine the integrity of this important risk management practice and, perhaps, the practitioners responsible for maintaining the Loss Events application.
* Reconciling the general ledger to loss events ensures that all losses are being captured within the Loss Events application. If losses are loaded directly into the Loss Events application from the general ledger, it is a straight forward process to identify missing or duplicate Loss Event forms.
* Loss Event reporting is usually much more detailed than total losses reported on a business unit’s income statement. Aligning Loss Event reporting to the same business unit structure as the income statement, loss event reporting can complement the income statement reporting on at least the same cadence as income statements are being distributed to management and the board of directors.

Organizations that model capital requirements based on loss information need as complete and accurate a listing of losses as possible.

**Additionally:**

While reconciling the general ledger to the Loss Events application is strongly recommended, most organizations certainly do not want to create and analyze a Loss Event form for small monetary losses. Each organization must establish a minimum monetary threshold above which Loss Event forms are required. General ledger entries below the established threshold can be loaded in total as one record, indicating the number of entries that compose the loss entry. If small losses combine them add them and create one record in system for loss event.

**Event Details Section:**

The sections related to describing event details associated with a Loss Event record include Event Details, Grouped Loss Events, Related Loss Events, Comments, Associated Business Process(es), and Associated Risks.

For Group Losses, you can use the Related Loss Events section to look-up and attach all related loss events, and the system aggregates the total value in the Total Calculated Gross Loss Amount field for the group.

### **Remediation**

The Remediation tab allows you to add new Findings records that can assist with your remediation plans.

### **Root Cause Analysis**

Sections related to the Root Cause Analysis of a Loss Event record include Policy Analysis and Risk Assessments.

Typically, root cause analysis is performed by the affected business unit manager, their delegate, or a risk management specialist. Completing these sections is very straight-forward and brings to light the underlying cause of the loss.

* In the Policy Analysis sub-tab, the Violated Policies section, references are made to any policy documented
* In the Policy Analysis sub-tab, the Failed Control Procedures section, references are made to any control procedures documented.
* In the Risk Assessments section, Applications, Facilities, Devices, and Information Assets associated with the loss can be targeted for assessment.

Following the evaluation of violated policies, failed controls, and completed risk assessments, the Root Cause Analysis Narrative field should be completed indicating the summary reason(s) for the loss. The Impact Evaluation and Likelihood Evaluation can be scored to indicate the qualitative scale of the loss, or the fields may be removed from the form if this type of information is deemed unnecessary and redundant to the loss amount.

The Detection Evaluation field provides a classification around how timely the loss was detected. This classification may help organizations to focus on losses with slow detection rates in order to identify how loss detection can be improved.

Lastly, deficiencies in policies and procedures that have been identified in root cause analysis should be remediated. Findings and tasks can be established, assigned to responsible individuals, and monitored until completed.

### **Recovery Tracking**

Sections of the Loss Event record which relate to loss recovery tracking include Financial Valuation, Insurance Claims, Financial Recovery Summary, Offset Transactions, and Recovery Tasks/Activities.

The **Financial Valuation** section can be used to track the status of the recording of loss entries, if the entries originate after the form is completed. Or, this section can be removed from the layout if transaction preparation, submission, and approval is tracked through the general ledger.

**The Financial Recovery Summary** provides a calculation of the Net Loss Amount. See the Risk Management Data Dictionary for the calculation.

Losses that are covered by insurance can be related to the appropriate insurance policy in the Insurance application. Claim notes can also be managed by the insurance administrator until the claim is paid. **Tying losses to the insurance policy** to which they relate helps insurance purchasers make better decisions about the reasonableness of insurance policy premiums versus losses incurred

The **Offset Transactions** section represents any offsetting, related transactions that should be removed from this transaction.

The **Recovery Tasks/Activities section** provides a location where recoveries captured against the loss can be recorded and tracked.

### **Reporting and Approvals**

Sections that relate to the reporting and approval of a Loss Event record include Reporting Requirements and Approvals.

The Reporting and Approvals section is used to manage all necessary reporting, to attach any additional documentation about the loss event, and to capture required approvals. RSA recommends that you configure specific reporting requirements and approvers to fit your organization.

**ORX**

The Operational Risk Exchange tab provides organizational context to the Loss Events record

### **Loss Event Thresholds:**

Loss event thresholds determine when certain people need to get involved in a loss event incident. The greater the loss event, the more people need to sign-off on the workflow.

* Loss Event Controller
* CFO
* CEO

**Insurance**

The Insurance application is designed to assist risk practitioners with the following tasks: Managing their corporate insurance programs by tracking insurance applications, insurance policies, premiums, deductibles, brokers, underwriters, underwriter financial strength, and expiration dates.

* Identifying gaps associated with uninsured risks and analyzing over and under insured risks by mapping insurance policies to risk register items. Analyzing losses incurred vs. insurance premiums paid (loss ratios).
* Perform basic insurance claims management via Loss Events.
* Rationalizing the corporate insurance risk transfer program in terms of the organization’s overall risk profile.

The following questions are clearly framed by mapping an organization’s risk register and losses to its insurance policies,

Are all of the risks facing the organization that must be insured, in fact, insured?

Are the insurance limits in place on each policy consistent with the amount of risk faced by the organization? Is the organization sustaining losses that are not covered by insurance? Are loss amounts consistent with policy deductibles? Does loss history justify the premiums being paid on each policy.

**Archer Insurance application is around the evaluation of the adequacy of insurance in place vs. the risks facing the organization.**

### **Insurance Form**

An insurance application record would typically be completed by someone in the organization’s insurance administration function. The General Information section lists details about each insurance policy that the organization has in place, including the broker name, carrier name, underlying carrier strength, policy limits and deductibles, premium, and expiration date. In addition, copies of the policy and application can be attached.

The Exclusions and Included Risks tabs provide sections that allow practitioners to cross reference the policy to Risk Register risks that are included and excluded from coverage under the insurance policy contract and endorsements. The purpose of mapping including risks is to better understand the degree to which policy limits cover the inherent risk covered by the policy. The purpose of mapping excluded risks is not to map all other risks in the risk register, but those risks that would be expected to be covered by such a policy, but are excluded by contract provision or endorsement. This helps risk managers clearly understand what is and isn’t covered by insurance.

The Associated Losses tab allows practitioners to associate Loss Event records to the insurance policy to which they relate. This information is useful to understand the insurance policy loss ratio to negotiate with the underwriter.

## Risk Register Library

The RSA Archer Risk Register Library is a place where risk managers can document a standardized pool of risk statements that can later be drawn upon when building a business unit’s Risk Register, or when adding risks to Risk self-assessments. Use of the library is intended to expedite building out registers and completing assessments while also ensuring continuity and completeness of new risk statements.

## Metrics Library

The RSA Archer Metrics Register Library is a list of generic metrics that you can import, maintain, and add to.

These metrics library records can be used in the Metrics application to quickly create new Metrics. You can use Metrics Library records as is, or modify them to better reflect your organization’s specifications.

RSA Archer also maintains a partnership with Risk Business International. RBI provides libraries of Key Risk Indicators that you can import into your RSA Archer Risk Management-related solutions.

### **Risk Assessments Sub-Solution**

The Risk Assessments sub-solution contains the pre-built Risk Assessment questionnaires that are included as part of the RSA Archer Risk Management solution.

## Risk Project