5 software AG

IT Governance, Risk and Compliance

Alfabet Reference Manual

Documentation Version Alfabet 10.9.1

CONVENTIONS USED IN THE DOCUMENTATION

Convention	Meaning
Bold	Used for all elements displayed in the Alfabet interface including, for example, menu items, tabs, buttons, dialog boxes, page view names, and commands. Example: Click Finish when setup is completed.
Italics	Used for emphasis, titles of chapters and manuals. this Example: see the *Administration* reference manual.
Initial Capitals	Used for attribute or property values. Example: The object state Active describes...
All Capitals	Keyboard keys Example: CTRL+SHIFT
File > Open	Used for menu actions that are to be performed by the user. Example: To exit an application, select File > Exit
< >	Variable user input Example: Create a new user and enter <User Name>. (Replace < > with variable data.)
	This is a note providing additional information.
	This is a note providing procedural information.
	This is a note providing an example.
	This is a note providing warning information.

TABLE OF CONTENTS

Chapter 1:   Introduction to IT Governance, Risk and Compliance

Enterprises need to evaluate, plan and manage IT strategies, architectures and processes effectively by understanding possible vulnerabilities, threats, and risks to their IT. The evaluation of threats as well as compliance with various requirements is necessary at every level of planning to reduce risk to your enterprise IT environment. IT risk management should not be a one-off project, but a continuous process targeting constantly changing IT risk and business environments and ensuring that risks are continually monitored and the risk management strategy is adjusted accordingly.

The IT Governance, Risk and Compliance sales package allows you to realize your enterprises requirements in terms of understanding and mitigating risks as well as fulfilling compliance requirements. Finding the right policies for IT risk, compliance and security is a balancing act between the enterprise's need for agility and continuity and the requirement to comply with regulations. The capabilities available in the IT Governance, Risk, and Compliance sales package enable you to understand the most current and relevant IT vulnerabilities affecting the organization, and effectively plan and monitor the actions needed to mitigate the impact of the risks posed by them and offset the cost and effort of assessing and managing compliance and risk.

The IT Governance, Risk and Compliance package is used by enterprise architects, compliance officers, risk managers and auditors to:

- assess applications, data, and projects and other (IT) objects according to their degree of risk exposure

- stipulate threat, risk, and risk mitigation catalogs that are applicable to specific sets of applications, technologies, projects, etc.

- automate the assessment of threats and risks and manage and plan their mitigation

- establish automated processes to drive risk assessments based on ever-evolving threats in the market

- refine data retention policies at a more granular scale

- perform and manage compliance evaluations

- define a centralized framework to make compliance checks more efficient

- audit for adherence to the control structure and correctness of the evaluated objects

To understand the potential pain points in the IT and implement projects to alleviate these, Alfabet provides a Risk Management and Compliance Management as well as the implementation of configurable surveys to initiate complex data collection tasks. The Risk Management functionalities in Alfabet support risk assessment that allows objects such as applications, business, data, projects, etc. in the enterprise to be evaluated for risk as well as for mitigations to be defined and planned to prevent or reduce the risks. The Risk Management functionalities available in Alfabet can be implemented for the Application Risk Management, Information Risk Management, and Project Risk Management capabilities. Assessments can be automated with workflows, reducing manual effort drastically. Further, you can define the IT controls necessary to mitigate risk and to fulfill regulatory and corporate compliance obligations. The Compliance Management functionalities in Alfabet provide support for the definition of compliance inquiries, management of compliance projects, evaluation of target objects in the context of a compliance project as well as the auditing of compliance projects

The table below provides an overview of the features of each of these options:

Functionality	Assessment Method	Identifying Users to Make Assessment	Configuration Requirements
Risk Management	Users evaluate the base risk exposure of objects in order to prioritize and focus on the objects that require detailed risk assessment. Risk mitigations may be defined that can later be realized by means of a project.	Users are explicitly assigned to a risk management group.	Evaluation types and indicator types must be configured.
Compliance Management	Users evaluate on an object-by-object basis via a compliance evaluation wizard. A disadvantage to this method is that the same metric must be used to answer all questions.	Users are found via a query configured for a compliance policy.	Several queries must be configured and an indicator type must be specified.
Surveys	Complex data capture forms are available to users in configured wizards. Workflows ensure that the data collection tasks are distributed to the responsible users and that all data collection tasks are completed by their specified deadlines.	Users are found via a query configured for a workflow.	Surveys are very flexible in their conceptualization but typically require complex configuration including the configuration of custom classes, custom properties, custom editors/wizards, and workflows. Surveys are configured by a solution designer in the configuration tool Alfabet Expand and are not described here. For more information, see the section *Configuring Surveys for Data Capture Campaigns* in the reference manual *Configuring Alfabet with Alfabet Expand*.

The following information is available:

- [Introduction to IT Governance, Risk and Compliance](#)

- [Application Risk Management](#)

- [Information Risk Management](#)

- [Project Risk Management](#)

- [Compliance Management](#)

Chapter 2: Application Risk Management

Enterprises need to plan and manage strategies, architectures, and processes with an understanding of all possible relevant threats and vulnerabilities in order to minimize risk. Alfabet provides an Application Risk Management capability that allows you to evaluate and analyze applications in order to understand the relevant threats and risks to the application architecture.

A risk refers to the likelihood that a particular object in the enterprise's IT landscape is exposed to a given threat and potentially targeted by a given attack. The definition of a risk includes the assessment of the potential damage caused by the risk, the potential probability that the risk could occur, and ideally a mitigation of the risk that can be planned and implemented in the enterprise. The assessment of applications for risk allows you to understand which applications are to be tolerated in the landscape but need observation and which applications have risks that must be mitigated. Attaining answers to these questions is critical to the maintenance of a healthy and cost-effective architecture as well as planning future operating models.

The following functionalities constitute the Risk Management capability:

- The *Configuring Risk Management Templates for the Risk Management Functionality* allows risk projects to be configured that focus on different parts of the IT

- The *Risk Mitigation Templates Explorer* allows a catalog of risk mitigations to be defined in order to support the standardization of mitigations

- The *Threat Management Functionality* allows a catalog of threats to be defined in order to couple threats and vulnerabilities with risks to actual applications in the IT

- The *Risk Management Functionality* allows risk management groups to be defined with the applications to be targeted by the risk project

- The *Risk Documentation Functionality* allows applications to be surveyed for base risk exposure and evaluated for risk by the user responsible for the risk assessment.

> Before you can begin to evaluate the risk to the application architecture, information on the organization's application landscape must already be captured and maintained. The activities around information gathering are done at the level of individual applications and are typically coordinated by an application owner or other responsible staff. Ideally, all relevant applications in your enterprise have already been captured in the inventory. Information about the applications, such as the business data that is transferred by them, the technical context required to run the application, the business processes that the application supports, and the functional domains that own the application should also be documented and up-to-date. For detailed information about capturing application data, see the reference manual *Enterprise Architecture Management*.

The following information is available regarding the Application Risk Management capability:

- [Methodology: Understanding Risk Management](#)

- [Prerequisite: Configuration Requirements for Risk Management](#)

- [Understanding Governance and Responsibilities in Application Risk Management](#)

- [Capturing Threats and Defining Risk Mitigation Templates](#)

    - [Defining Threat Groups and Capturing Threats](#)

    - [Specifying Risk Mitigation Templates for the Threat Catalog](#)

    - [Understanding Application Risks Based on Existing Threats](#)

> ⓘ Please note that a context-sensitive Help is available for each view available in the Application Risk Management capability. You should refer to the Help if you require an explanation about the functionalities and information available in a specific view.

Methodology: Understanding Risk Management

In order to assess applications for risk using the Risk Management capability, your enterprise's applications must be captured in Alfabet as part of your enterprise's IT inventory. Ideally, the various layers of the IT are documented including the application and information architectures as well as the business layer. Responsibilities for the applications should be defined and the relationships of the applications to other aspects of the IT architecture should be modelled.

> For more information about documenting the scope of the IT inventory, see the reference manual *Enterprise Architecture Management*.

The following roles are typically responsible for the risk evaluation and assessment:

- IT Compliance Manager

- Chief Information Security Officer

- Application owners

- Process owners and contributors

The Risk Management capability in Alfabet typically consists of four activities that focus on understanding the threats to your enterprise's IT architecture, evaluating and prioritizing the vulnerability of applications, assessing the risks and potential damage to the applications considered most at risk, and specifying and implementing mitigations for the risks. This methodology allows the enterprise to streamline the risk evaluation process and specifically target the relevant objects that are considered most at risk in the enterprise. A catalog of standard threats including templates describing risks and risk mitigations can be reused for regular assessments of the IT.
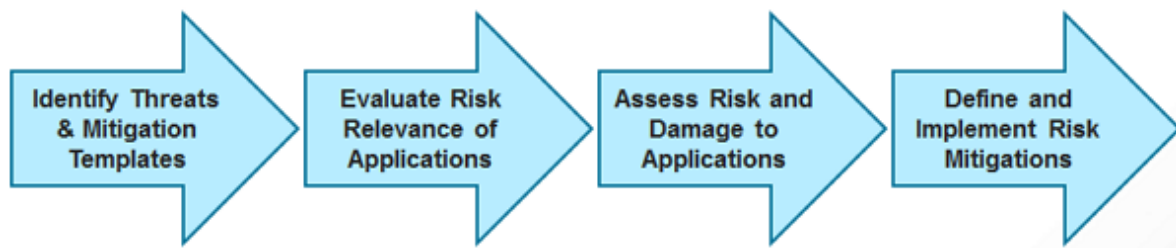
FIGURE: Recommended processes for risk management

The following methodology is recommended for risk management in Alfabet:

- **Identify Threats and Specify Risk Mitigation Templates:** For each business area that is to be assessed, a relevant user who is a risk specialist for that area (for example, for trading risks, etc.) should assess the threats to the applications for that business area. Threats can be manually captured in Alfabet as well as imported via the Alfabet Data Integration Framework (ADIF) functionality from a repository containing a catalog of standard threats. For each threat defined, one or more risk mitigation templates can be defined that are targeted to avoid, reduce or contain the risk derived from the potential threat. The definition of a catalog of risk mitigation templates will reduce the effort during the risk assessment phase and will support the standardization of the mitigation strategy in the enterprise.

- **Evaluate Risk Relevance of Applications:** To streamline the process of capturing the risks and their mitigations for the enterprise's application architecture, the base risk exposure of the applications in the enterprise should be evaluated. Evaluating the risk relevance allows the applications to be screened in order to determine whether potential risks exist and the significance of those risks. For each application targeted by the risk evaluation, questions must be answered in order to evaluate the level of risk to the application. All risk relevance scores above the specified threshold will thus be considered relevant to enter the next phase in which the risks to the application are defined in more detail.

- **Assess Risk and Damage to Applications**: This stage of the risk assessment targets only the objects that have been evaluated for risk relevance and determined to warrant risk assessment. The specification of the risk includes the potential cost of damage to the application and the probability of damage to the application as well as suggestions to mitigate the risk. The potential cost of damage to the application and the probability of damage to the application if the suggested mitigation is implemented can also be documented. The suggested mitigation is informational only. Mitigations that can be planned and made operational are captured in the next stage of risk management.

- **Define and Implement Risk Mitigations**: Once risks have been defined for the application, risk mitigations can be defined that can be tracked and implemented to avoid, reduce or contain the risk. The risk mitigation may be based on a predefined risk mitigation template. For each risk mitigation, the architecture elements that might be impacted by the risk mitigation can be documented. Furthermore, a demand can be created to express the need to address the risk mitigation in the IT architecture. Once a demand has been articulated to address the risk mitigation, a project can be created to implement the risk mitigation.

> To capture demands, you must have access to the Demand Management capability and to capture projects you must have access to the Project Portfolio Governance capability, both of which are part of the IT Planning Advanced sales package.

Prerequisite: Configuration Requirements for Risk Management

To implement the **Risk Management** capability in Alfabet, you should configure the following:

- Risk management templates must be configured in order to specify the object classes that are the target of the risk evaluation. The risk management template includes the evaluation types that represent the questions to use for the **Risk Evaluation** phase, the indicator types to define the risk damage and probability of risk damage to the risk object in the **Risk Assessment** phase, and a risk portfolio for the analysis of the risk evaluation. Risk management templates are defined in the *Configuring Risk Management Templates for the Risk Management Functionality*.

  > ⓘ It is highly recommended that the user designing the risk project pursues a pragmatic qualitative approach that is directed at the relevant stakeholders. The evaluation questions should be a compact set of questions with simple answers and the answers should be mapped to numeric values for easy analysis.

- Risk templates may be configured in order to group a standard set of risks as well as suggested mitigations. A risk can be defined explicitly for a specific risk object or it can be added to the risk object by means of a configured risk template. A risk template is defined via the *Risk Templates Page View* available for a class-based risk management template.

- Risk mitigation templates may be configured in order to capture a predefined risk mitigation for a specific threat in order to articulate how to avoid, reduce or contain the risk derived from the potential threat. The risk mitigation template includes the name of the risk mitigation, the target date when the risk mitigation should be implemented, and a number to prioritize the risk mitigation. The risk mitigation can then be defined for a risk object in the context of a risk assessment. Risk mitigation templates are configured via the *Risk Mitigation Templates Explorer*.

  > ⓘ For a detailed description of the configuration of risk management templates, risk templates, and risk mitigation templates, see the section *Configuring the Risk Management Capability* in the reference manual *IT Governance, Risk and Compliance*.

Understanding Governance and Responsibilities in Application Risk Management

A number of governance concepts are implemented in the Application Risk Management capability:

- **Risk Object**: Each application assigned to a risk management group is considered a risk object. The risk evaluation and assessment of the application is specified for the risk object only. The risk object has its own **Authorized User** definition which may differ from the **Authorized User** definition of the application that the risk object is based on. The risk assessment is therefore only visible to users in the user community who have authorization to the risk object.

- **Roles**: A role defines the functional relationship or responsibility that a user or organization has to an application (for example, the Risk Manager or Architect of an application) or to a risk object. The risk object has its own role definition which may differ from the role definition of the application that the risk object is based on Roles describe responsibilities but they do not authorize access permissions to the application in Alfabet.

- **Mandates**: Risk management groups may be managed in a federated architecture. By means of a federated architecture, it is possible to specify the visibility of individual risk management groups in the Alfabet interface for specific users.

Capturing Threats and Defining Risk Mitigation Templates

A **Threat Management** capability allows you to identify, plan for, and reduce risk to the enterprise's IT. The assessment of threats supports the enterprise to understand the value of the application portfolio, effectively assess and mitigate risks to the application architecture, and plan associated risk-mitigating projects.

For each business area that is to be assessed, a relevant user who is a risk specialist for that area (for example, project risks, trading risks, etc.) should assess the threats that pose risks to that area. A threat refers to the source of a particular type of risk and can be associated with one or more specific risk objects in the enterprise's IT landscape. Threats can be manually captured in Alfabet as well as imported via the Alfabet Data Integration Framework (ADIF) functionality from a repository such as the National Vulnerability Database (NVD) made available by the National Institute of Standards and Technology (NIST).

> The import of threats from a repository or other database requires the Alfabet Data Integration Framework (ADIF) functionality available via the configuration tool Alfabet Expand. For more information about ADIF, see the reference manual *Alfabet Data Integration Framework*.

In Alfabet, a threat refers to the source of a particular type of risk to the enterprise's IT. The threats can be organized and assessed in the context of hierarchically structured threat groups. For each threat defined, one or more risk mitigation templates can be defined that are targeted to avoid, reduce or contain the risk derived from the potential threat. The risk mitigation template can be used later by users when defining specific mitigations for actual risks. When a risk is assessed for an application, the risk may be based on an existing threat that has already been documented in Alfabet. The risk will inherit the risk mitigation based on the risk mitigation template defined for the threat that the risk is derived from.

The definition of a catalog of risk mitigation templates will reduce the effort during the risk assessment phase and will support the standardization of the mitigation strategy in the enterprise.

The following information is available:

- [Defining Threat Groups and Capturing Threats](#)

- [Specifying Risk Mitigation Templates for the Threat Catalog](#)

- [Understanding Application Risks Based on Existing Threats](#)

Defining Threat Groups and Capturing Threats

Threat groups bundle a set of threats. Threat groups should be defined based on the risk assessment methodology used in your enterprise. Threats can either be manually defined or a catalog of standardized threat groups and threats may be imported via ADIF.

FIGURE: Threat group hierarchy with threats at the leaf level

The example above displays a threat group hierarchy for Microsoft® Internet Explorer®. The subordinate threat groups represent each IE version and the threats for an IE version are displayed at the leaf level of the subordinate threat group. In this case, the threats were imported from a repository. The **Description** attribute in the object profile of the threat captures the information about the threat. Please note the following:

- The threat group hierarchy can be manually created in the *Threat Management Functionality*.

- Threats can be captured in the *Threats Page View* for any threat group in the hierarchy. The threat should have a name, release status, and description defined.

Specifying Risk Mitigation Templates for the Threat Catalog

Risk mitigations may be planned and implemented in order to address potential threats as well as avoid, reduce, or contain risks to the IT landscape. By means of risk mitigation templates, risk mitigations may be standardized and consistent data can be captured for a set of risk objects.
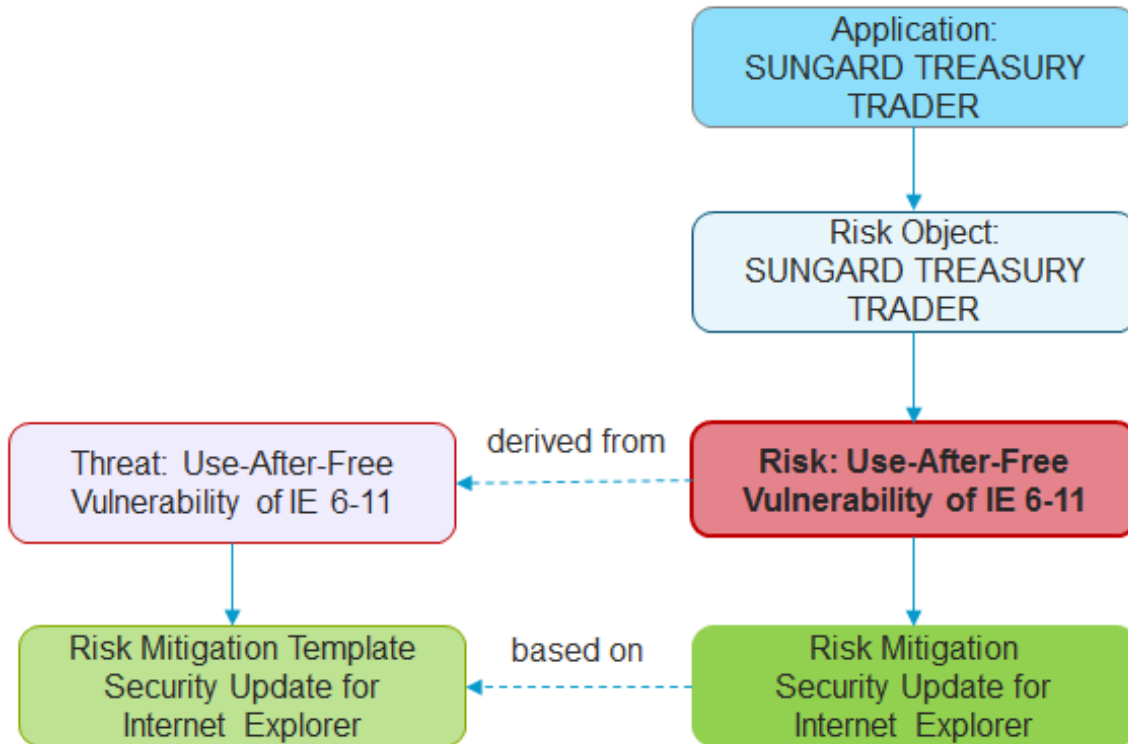
FIGURE: Risk mitigation based on risk mitigation template defined for threat

When a risk is assessed for an application, the risk may be based on an existing threat that has already been documented in Alfabet. The risk will inherit the risk mitigation based on the risk mitigation template defined for the threat that the risk is derived from. The definition of a catalog of risk mitigation templates will re-duce the effort during the risk assessment phase and will support the standardization of the mitigation strategy in the enterprise.

A risk mitigation template captures a preconfigured definition of a mitigation that applies to a specific threat. The definition of the risk mitigation template includes the name of the risk mitigation, the target date when the risk mitigation should be implemented, and a number used to prioritize the risk mitigation. When a risk is specified for an application in the context of a risk assessment, the risk can be based on an existing threat that is part of the enterprise's catalog of threats and vulnerabilities. The risk mitigation tem-plate is then copied as a risk mitigation to the risk. The definition of the risk mitigation can be modified as needed.

Risk mitigation templates are defined for a threat in the *Risk Mitigation Templates Page View* of the rele-vant threat.

Understanding Application Risks Based on Existing Threats
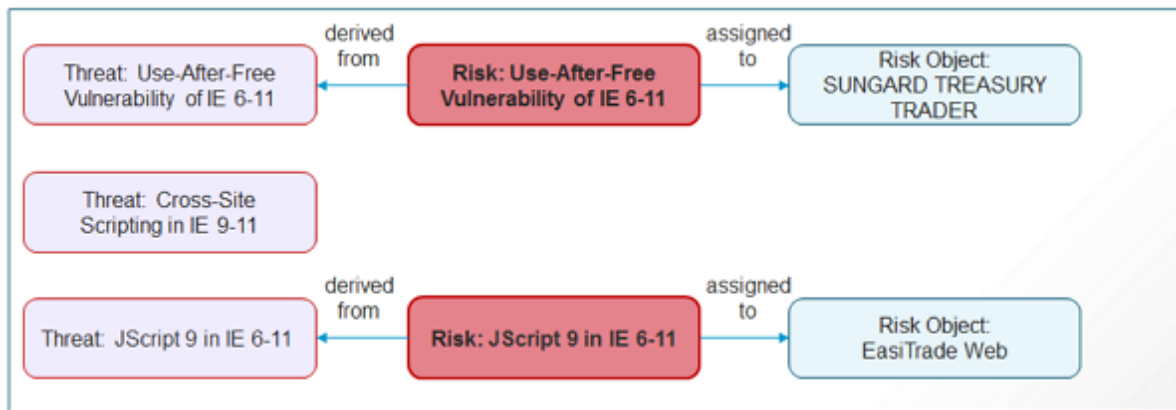
The *Associated Risks Page View* displays all risk objects that have been derived from a selected threat. The report includes information about the risk objects and their defined risks including the potential cost of damage to the application and the probability of damage to the application if the risk were to occur as well as if the risk were to be mitigated.

Evaluating Objects for Risk Relevance

Before the applications are assessed for risk, they should be prioritized in order to determine which applications are the most important to protect. To streamline the process of capturing the risks and their mitigations for the enterprise's application architecture, the base risk exposure of the applications in the enterprise should be evaluated. The base risk exposure is an evaluation of applications according to their potential risks. Each application that should be evaluated must be assigned to a risk management group whereby it will be evaluated by means of a risk relevance questionnaire.
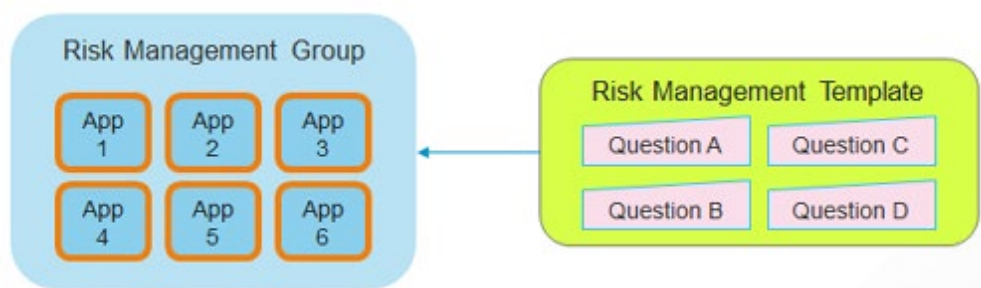
The questions to determine risk relevance are typically created by a user in your enterprise responsible for the risk assessment. The questions are configured in a risk management template that will be specified for the risk management group bundling the applications that are to be evaluated. Each application assigned to a risk management group is considered a risk object. It is the risk object that is evaluated and assessed in the context of the Risk Management capabilities. This ensures that this information is only visible to users in the user community that have access to the risk object.
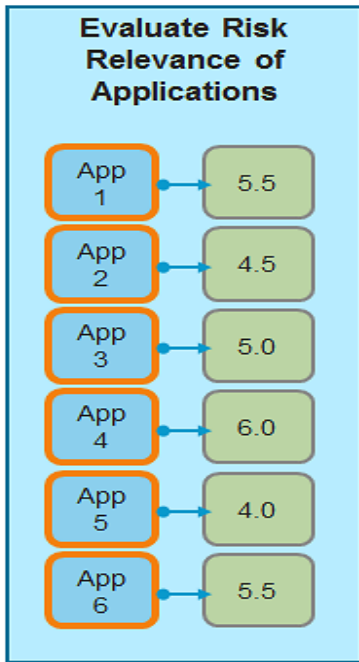
FIGURE: Applications with their risk relevance scores

For each application targeted by the risk evaluation, the configured questions must be answered in order to evaluate the level of risk to the application. A process owner would ideally evaluate the applications by answering a configured set of questions for each application in order to produce a score that determines the relevance of risk to each application. The answers provided for all questions about the application will be computed in order to generate a risk relevance score. This risk relevance score specifies the level of risk to the application.
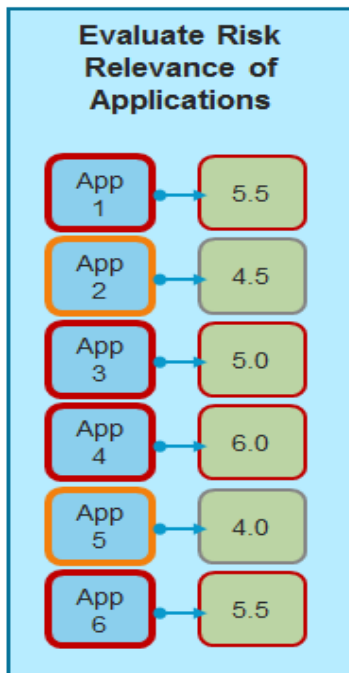
FIGURE: The threshold for risk relevance is set to 5

Once all applications have been evaluated, a threshold value can be defined.
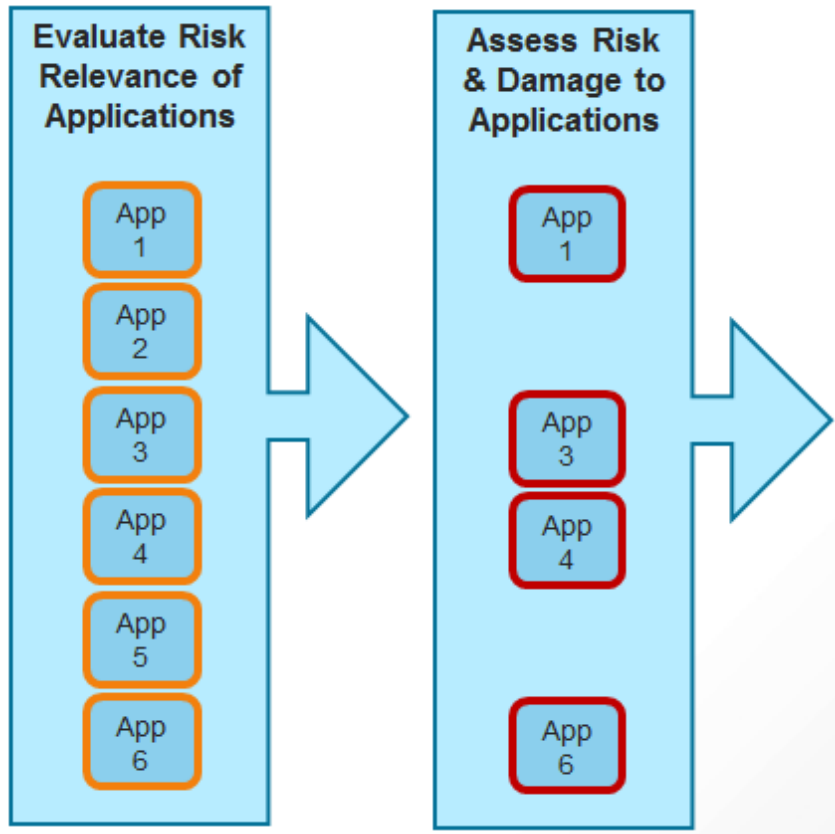
FIGURE: Applications above the threshold will be assessed for risk

All risk relevance scores that are equal to or above the specified threshold should be sent to the risk assessment phase in which the risks to the application are defined in more detail.

The following information is available:

- Creating Risk Management Groups

- Evaluating the Relevance of Objects for Risk Assessment

Creating Risk Management Groups

A risk management group is the container to logically structure the applications that will be evaluated and assessed. Each risk management group may have a different risk management template in order to allow various perspectives from which to structure and analyze risk objects. The risk management template assigned to the risk management group will determine the following:

- The object classes that may be targeted for the risk project

- The questions to be answered in order to assess the base risk exposure of the applications assigned to the risk management group

- The risk damage and risk probability indicator types that allow for the potential cost resulting from the risk and risk mitigation to be documented

- The risk portfolio that is available to analyze the risks to the applications in the risk management group

- The risk templates available to help define the risks to the applications in the risk management group

An application may be associated with multiple risk management groups, allowing the same risk object to be considered in different contexts.

A risk management group is created in the *Risk Management Functionality*. If necessary, you can create subordinate risk management groups. For each risk management group, a name, description, and risk management template must be defined.

All applications that should be evaluated for base risk exposure should be assigned to the risk management group in the *Assigned Objects Page View* of that risk management group.

Evaluating the Relevance of Objects for Risk Assessment

The *Risk Documentation Functionality* displays all risk object that a user is responsible for as the authorized user or by means of the user groups that he/she is a member of. This functionality provides access to the *Risk Relevance Questionnaire Page View* as well as the *Risk Assessment Page View*.

The questions in the *Risk Relevance Questionnaire Page View* must be answered for each application in the risk management group to determine a risk relevance score for its base risk exposure. For each question that you answer, a value will be mapped to an indicator type that represents an issue of relevance for the risk evaluation.

For a GDPR Risk Assessment, for example, the following questions (indicator types) and answers (value range) may be relevant to identify whether an application should be included in the risk assessment

Question	Answer
Data Anonymized?	- 1 - Yes - 2 - No
Data Encrypted?	- 0 - Fully Encrypted - 1 - Partially Encrypted - 2 - Not Encrypted
Retention Period of Processed Data	- 1 - < 3 years - 2 - Between 3 and 30 years - 3 - > 30 years

The indicator types **Data Proliferation**, **Data Sensitivity**, and **Risk of Leakage** have been configure as issues of relevance for the GDPR Risk Assessment. If a question regarding the impact of **Data Anonymized?** for an application is answered with the option **2 - No**, then the value may equal 0 (a very low score) for the indicator type **Data Proliferation** but may equal 4 (a very high score) for the indicator type **Risk of Leakage**.

The answers for all questions will be mapped to all indicator types relevant for the risk evaluation. All of the these values will be added together in order to produce a risk relevance score for the application that will help to determine its base risk exposure.

> The questions and answers, the indicator types representing the issues of relevance for the risk evaluation, and the mapping of answers to the indicator types are configured in the *Configuring Risk Management Templates for the Risk Management Functionality*.

The risk relevance scores will be displayed for all applications in the risk management group in the *Assigned Objects Page View*. The higher the application's risk relevance score, the higher is the base risk exposure of the application. In order to determine which of the applications should be included in the risk assessment, a threshold value can be defined in the **Risk Relevance Score** field. All objects with a risk relevance score that is equal to or higher than the value entered will be highlighted. Ideally, these are the objects that have the highest priority to be assessed for risk. Regardless of the threshold values defined in the **Risk Relevance Score**, any risk object may be assessed for risk in the *Risk Assessment Page View* of the risk object.

Carrying Out the Risk Assessment of Applications

The applications in the risk management group that have a high risk relevance score for base risk exposure have the highest priority to be assessed for risk. Regardless of the threshold values defined in the **Risk Relevance Score**, any risk object may be assessed for risk in the *Risk Assessment Page View* of the risk object. However, ideally this stage of the risk assessment targets only the objects that have been evaluated for risk relevance and determined to warrant risk assessment.
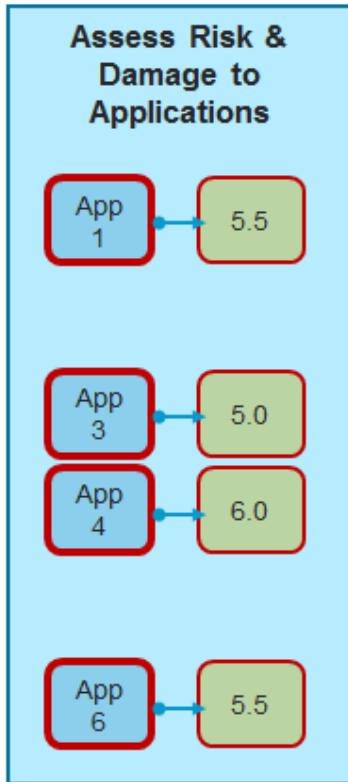
FIGURE: Applications to assess for risk

For each application in the risk assessment, one or more risks can be defined. The risks may be manually defined, based on the catalog of threats in the inventory, or copied from a preconfigured risk template.
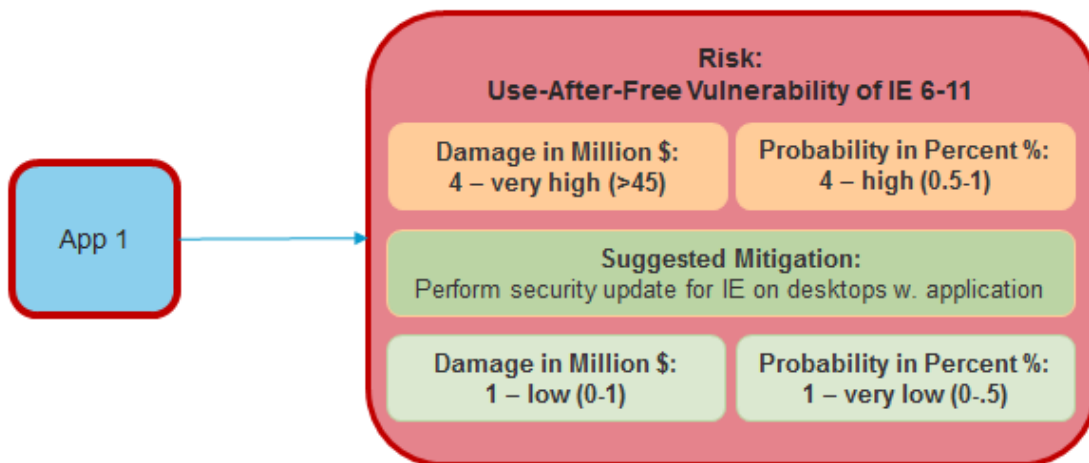
FIGURE: Risk definition including potential costs and costs after mitigation

The specification of the risk includes the potential cost of damage to the application and the probability of damage to the application as well as suggestions to mitigate the risk. The potential cost of damage to the application and the probability of damage to the application if the suggested mitigation is implemented can also be documented. The suggested mitigation is informational only. Mitigations that can be planned and made operational are captured in the next stage of risk management.

Assessing Applications for Risk

For each object in the risk management group that has been determine to have a high risk relevance score, define one or more potential risks to the object in the *Risk Assessment Page View*. Risks can either be defined from scratch or created based on a risk that has already been defined for another application in the risk management group. Risks that are copied from either another risk object can be modified, as needed.

Risks can also be defined for the application by selecting a risk template that has been associated with the risk management template assigned to the risk management group. Risk templates bundle a standard set of risks and, if relevant, the suggested mitigations to the risk object. Risks that have been added to the application via a risk template that are not relevant can be deleted from the application.

Once a risk has been added to the selected risk object, you can describe the risk as well as define a value of the potential damage caused by the risk as well as the probability of the risk occurring. You can also propose actions that could potentially mitigate the risk and provide a value of the potential damage and probability of the risk if the suggested actions were to be implemented.

> For more information about creating a risk mitigation for the risk that can be tracked and implemented, see the section Capturing and Managing Risk Mitigations.

Analyzing the Risk Assessment

The *Risk Objects Portfolio Page View* available for a risk management group helps to understand which applications are most at risk in the group. The report displays a portfolio analyzing all risk objects assigned to the risk management group. You can display the objects based on the values defined for risk damage and risk probably if the risk is not mitigated as well as the estimated risk damage and risk probability if the suggested mitigation action were to be implemented.

The *Risks Portfolio Page View* available for a risk object helps to understand which risks have been determined to incur the most damage and are most probable. The report displays a portfolio showing the values specified for the risk damage and risk probability for each risk defined for the selected risk object.

Capturing and Managing Risk Mitigations

For each risk defined for a risk object, a risk mitigation can be define in order to avoid, reduce or contain risks to the IT landscape. The risk mitigation articulates a step to avoid, reduce or contain the risk. For each risk mitigation, the architecture elements that might be impacted by the risk mitigation can be documented. Furthermore, a demand can be created to express the need to address the risk mitigation in the IT architecture. Once the demand to address the risk mitigation has been articulated, a project can be created to implement the risk mitigation.
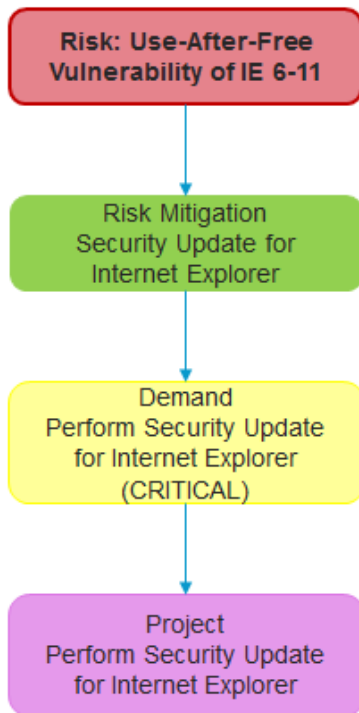
Risk mitigations can be captured for a risk associated with a risk object in the *Risk Mitigations Page View* page view. Risk mitigations can be captured as new objects or created on the basis of risk mitigation templates. Risk mitigations include a description of the mitigation, a target date when the risk mitigation should be implemented as well as the prioritization of the risk mitigation.

You can define the architecture objects in the IT landscape that are impacted by the risk mitigation. The architecture elements that may be impacted by the risk mitigation can be documented in the *Affected Architecture Page View* in the object profile of the risk mitigation. If the risk mitigation is derived from a risk mitigation template, it will automatically inherit the architecture context from the risk mitigation template. An affected architecture element may be based on any of the following object classes: Application, Business Data, Business Function, Business Object, Business Process, Component, Customer Segment, Device, Domain, ICT Object, Information Flow, Market Product, Master Platform, Organization, Peripheral, Sales Channel, Service Product, Solution Building Block, Standard Platform, Technology, and Vendor Product.

Furthermore, one or more demands can be created for the risk mitigation in the *Demands Page View* in the object profile of the risk mitigation. The risk mitigation's affected architecture will be inherited by the demand. The demands can then be associated with projects that realize and implement the risk mitigation.

To capture demands, you must have access to the Demand Management capability and to capture projects you must have access to the Project Portfolio Governance capability, both of which are part of the IT Planning Advanced sales package.

Select the risk in the table and navigate to its object profile. In the *Risk Mitigations Page View*, you can create the risk mitigation. You can later define the architecture objects in the IT landscape that are impacted by the risk mitigation and specify a demand based on the risk mitigation.

Managing and Storing the Data About the Risk Assessment

A record of the risk evaluation and risk assessment conducted for a risk management group can be saved and archived. At any time during the evaluation or assessment phase, a snapshot can be created of all applications assigned to a selected risk management group in the *Assigned Objects Page View* of a risk management group. The snapshots will be saved to the *Risk Management Snapshots Page View* of the selected risk management group. An unlimited number of snapshots may be created for a selected risk management group. Unnecessary snapshots can be deleted.

The snapshot records the data collected in the risk evaluation and risk assessment of all risk objects assigned to the selected risk management group. The name of the snapshot will be automatically generated and will include the name of the risk management group and the timestamp denoting the date and time of the snapshot (for example: Market Data_04062009_112030).

- The first section of the snapshot displays the name of the risk management group and the data from the *Assigned Objects Page View*.

- The subsequent sections of the snapshot display the risk relevance evaluation for each application in the risk management group. Here you will see the data from the *Risk Relevance Questionnaire Page View* and *Risk Assessment Page View* for each risk object.

- The Microsoft Excel file may be saved to your network drive via the **Save** functionality in Excel.

Chapter 3:   Information Risk Management

Business data is the mainstay of every large company today and must be protected against evolving threats and risks to the IT. Additionally, emerging legal entities and regulations such as the General Data Protection Regulation (GDPR) require that companies know the data they house and process and that they maintain reliable records of their processing activities, prove compliance for governing bodies, and guarantee that compliance is sustainable.

The Information Risk Management capability helps the enterprise to understand the risks associated with the data transferred via information flows, understand whether there is a critical need for data protection, manage the data in a manner that is compliant with regulation. The **Risk Management** functionalities described in the section Application Risk Management are equally relevant for the evaluation and assessment of risks to information flows between applications as well as the business data that is transferred. As described in the example for the assessment of risk to applications, risk management templates may be configured to target the class Information Flow or Business Data in order to instigation a risk evaluation and risk assessment of the information architecture.

In addition to the implementation of a risk assessment in order to meet security requirements regarding risk to the IT, data retention policies may be configured to document the storage and management of business data in order to ensure compliance with policies regarding data persistence and legal archival requirements. Data retention policies provide a means to document standard information about how business data should be retained and stored. The data retention policy is assigned to a business data as part of its business data usage definition.

Before you can begin to evaluate the risk to the information architecture, information on the organization's information landscape must already be captured and maintained. The activities around information gathering are done at the level of business data and are typically coordinated by an application owner or other responsible staff. Ideally, all relevant applications, the business data that is transferred by those applications, and the business data usage (CRUD) has already been captured in the inventory. For detailed information about capturing business data, see the chapter *Information Architecture Definition* in the reference manual *Enterprise Architecture Management*. For information about specifying and analyzing business data usage, see the chapter *Information Portfolio Governance* reference manual *Portfolio Management Basic*.

To implement data retention policies as part of Information Risk Management:

- Data retention policies must be configured in the *Data Retention Policies Page View*. For each data retention policy that is created, the following must be specified:

  - A description of the data retention policy.

  - A description of when the data retention policy shall begin. For example, 3 Months After Demise, One Year After Last Valid Transaction.

  - The amount of time that business data is to be stored by the enterprise. For example, 1 month, 6 months, 1 year, 3 years, 10 years, etc.

  - The rules regarding the archiving of the business data. For example, Instant Archiving Required, Deferred Archiving Allowed, etc.

  - The permissible means to store the business data. For example, Disk, Tape, Cold Stand-By Solution, Hot Stand-By Solution, etc.

  - The permissible means to access the business data. For example, Criminal Investigation, Police, Legal, Internal Auditing, External Auditing, Board, etc.

- The minimum level of encryption for the business data. For example, Advanced Encryption Standards (AES), etc.

  Data retention policies are configured by your enterprise in the **Reference Data** functionality in the **Configuration** module. For more information, see the section *Configuring Data Retention Policies* in the reference manual *Configuring Evaluation and Reference Data in Alfabet*.

- The data retention policy must be assigned to a business data as part of its business data usage definition. The data retention policy that is relevant for the business data is selected in the **Business Data Usage** editor in the *Business Data Page View* of the providing application or component.

Chapter 4: Project Risk Management

The success of operational project management is integral to the ability of an enterprise to provide its services in a cost-effective and reliable manner. Assessment of project risks during the execution of the project is inherent to managing the project portfolio. The Project Risk Management capability focuses on identifying and assessing the risks to the project, managing those risks to minimize the impact on the project, and ensuring efficient project delivery and thus business continuity.

The Project Risk Management capability helps the enterprise to understand the risks associated with projects. The **Risk Management** functionalities described in the section Application Risk Management are equally relevant for the evaluation and assessment of risks to projects. As described in the example for the assessment of risk to applications, risk management templates may be configured to target the class Project as well as any project stereotype in order to instigation a risk evaluation and risk assessment of the project portfolio architecture.

In addition to the implementation of a risk assessment in order to ensure the successful outcome of your company's operational project planning, Alfabet provides project tracking capabilities to monitor and measure the progress of the IT projects in the enterprise. Projects can be monitored regarding the achievement of target values via a project evaluation as well as the tracking of the changes made to a milestone's target date.

A project evaluation type is an evaluation type that allows projects to be monitored regarding the achievement of target values. A new project evaluation can be created in regular intervals in order to monitor the project according to the indicator types configured for the project evaluation type. The current and target values can be defined for each indicator type that represents a criteria of the evaluation as well as the indicator type that represents the current achievement of the indicator type in relation to the target value indicator type. To implement project evaluations as part of Project Risk Management:

- Project evaluation types must be configured in the **Evaluations & Portfolios** functionality as well as the **Class Configuration** functionality in the **Configuration** module. For more information, see the section *Configuring Reference and Evaluation Data Required for Project Management* in the reference manual *Configuring Evaluation and Reference Data in Alfabet*.

- Indicators are defined for a project and its sub-projects in the *Project Evaluation Page View* of the respective project.

- The project evaluation types will then be available in the *Evaluation History*.

- The target date of project milestones can be tracked in the *Project Tracking Overview Report Page View*.

Before you can begin to evaluate the risk to the project portfolio, projects must be captured and tracked in Alfabet by means of the Project Portfolio Governance capability in the IT Planning Advanced sales package. Milestones are captured by means of the IT Planning Complete sales package. For detailed information about creating projects and tracking their milestones in Alfabet, see the reference manual *IT Planning Advanced*.

Chapter 5: Compliance Management

Staying compliant is critical for enterprises dealing with IT environments of financial institutions and government bodies, as even a slight security breach can create a seriously adverse impact. Companies must assess and validate compliance for various types of legislation and standards including SOX, COBIT, or GDPR, for example. The Compliance Management capability in Alfabet provides coherent support for the definition of compliance inquiries launched for a regulatory evaluation of a specific set of objects in the IT architecture. The capability allows your enterprise to specify the issues and objects targeted by a compliance project as well as manage the compliance project to ensure that it is completed. Finally, internal and external auditors can audit adherence to the control structure and the correctness of the evaluated objects.

The Compliance Management capability in Alfabet provides support for the definition of compliance inquiries, management of compliance projects, as well as the evaluation of target objects in the context of a compliance project as well as the auditing of compliance projects. The following functionalities constitute the Compliance Management capability:

- The *Compliance Configuration Functionality* allows the blueprint of the compliance inquiry to be defined by creating compliance control sets and compliance domains. The compliance control set allows you to define the target objects and the users responsible for providing information about the target objects as well as the set of standardized questions that constitute the inquiry. Every compliance project will be created based on a compliance control set and the geographical or topical compliance domain that is the target of the evaluation.

- The *Compliance Projects Functionality* allows compliance projects to be created, activated, and managed.

- The *Compliance Evaluations Functionality* allows users to answer questions about the target objects that they are responsible for in the compliance project.

The compliance projects in your enterprise can be initiated periodically as needed. Once a compliance project has been activated, relevant users that have been identified to answer questions about specific objects will receive an email notification and assignment about their compliance-relevant tasks.

The following information is available:

- Methodology: Understanding Compliance Management

- Prerequisites for Compliance Management

- Specifying Compliance Control Sets and Compliance Domains

- Initiating and Managing Compliance Project

- Assessing the Objects Targeted by the Compliance Project

Methodology: Understanding Compliance Management

A compliance project represents the inquiry to be launched in the enterprise in order to assess the regulatory compliance of a set of objects. For example, a compliance project could target the evaluation of SOX compliance for a specific set of applications in the enterprise.

The compliance evaluation is highly configurable based on the needs of your enterprise. Each compliance project is based on a configured compliance domain and compliance control set. The compliance domain specifies the valid area for which the compliance project should be executed. This could be a specific topic or geographic area, for example.

The compliance control set is like a blueprint that can be used for multiple compliance projects.
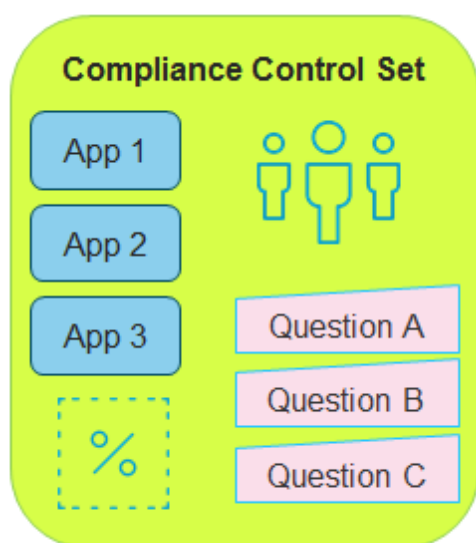
The compliance control set determines the following:

- The questions posed about the objects in the IT architecture. The questions are captured by means of compliance controls. The compliance controls are structured hierarchically whereby each top-level compliance control represents a branch in the network of compliance questions. The compliance control at the leaf-level of the hierarchy is the compliance control in which the question is defined about the target object.

- The objects that are targeted by the compliance evaluation. The objects targeted by the compliance evaluation are determined by the compliance policies that are created for the compliance control set. The compliance policy includes the queries that find the objects that are targeted by the compliance evaluation.

- The users that are responsible for answering questions about the objects targeted by the compliance evaluation. The responsible users are also determined by the compliance policies that are created for the compliance control set. The responsible users may be the authorized user or users with a specified role for the target object. Users that have no direct relationship to the target object must be found by means of queries.

- The indicator type to use as the metric to answer all questions asked in the compliance evaluation. One indicator type must be assigned to the compliance control set. It is used as the metric for all questions in a compliance project. For example, an indicator type could allow the following values to be selected as answers to the questions captured in compliance controls:0 - no action taken to date,

1 - compliance plan defined, 2 - plan partially implemented, 3 - plan fully implemented. 4 - not relevant.
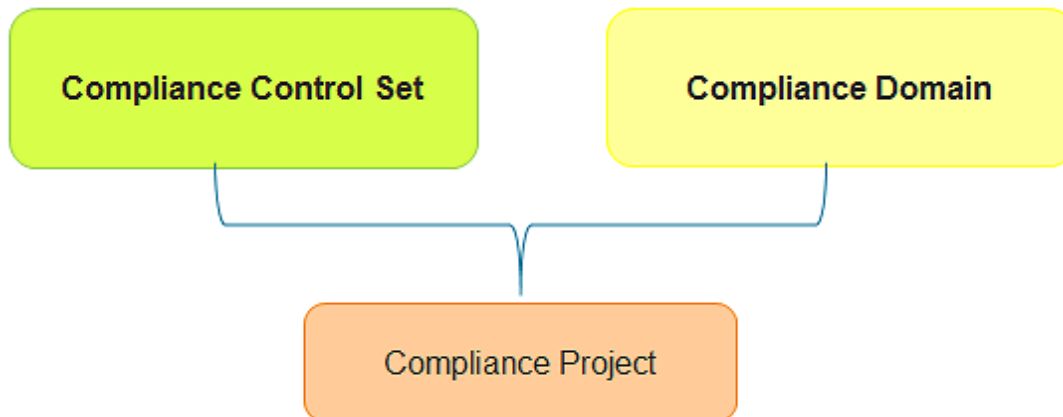
The compliance project therefore is an instantiation of the compliance control set for a specific time and area of validity that is determined by the compliance domain. For example, a compliance project based on a compliance control set representing SOX might be the SOX assessment in Q1/2020 for a regional subsidiary in the enterprise. A compliance project can only be based on a compliance control set if the release status of the compliance control set has been set to **Approved**. Only one compliance project may be active for a selected compliance domain and defined date.

The release statuses implemented in Compliance Management will depend on your solution configuration. Each compliance control set and compliance project will have an approved status and a retired status although they may have different names. The following represents a typical lifecycle of a compliance evaluation:
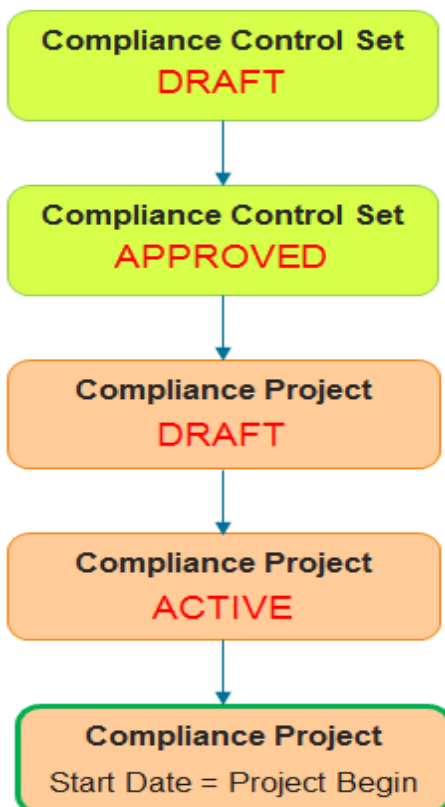
- **Release Status** attribute of compliance control set is set to **Draft**: The compliance control set can be defined as needed. Compliance policies can be added, deleted, and edited. Compliance controls can be added and deleted from the compliance control hierarchy.

- **Release Status** attribute of compliance control set is set to **Approved**: The compliance controls can no longer be added, deleted, or edited. A compliance project can be created based on the compliance control set.

- **Release Status** attribute of compliance project is set to **Draft**: The compliance project is initiated for a selected compliance domain and for a specified period of time. The compliance policies may be added, deleted, or edited.

- **Release Status** attribute of compliance project is set to **Active**. Please note the following about the compliance project:

  - If the **Release Status** attribute is set to the approved release status (**Active**), the compliance project will be activated. The **Activate Compliance Project** option in the **Compliance Projects** functionality will only be available for compliance projects with the approved release status (**Active**).

  - The compliance policies may be edited. No new compliance policies may be added to the compliance project.

  - The compliance project becomes a running project when it's start date is reached. Email notifications will be automatically sent to responsible users and assignments will be generated for each compliance control that they are responsible for.

  - Please note the following changes that can be made to a compliance project that has been approved:

    - If a compliance project has been approved, the compliance policies may be edited. No new compliance policies may be added to the compliance project.

    - If additional objects that were not found by the object queries need to be added to the compliance project, a functionality is available that allows the compliance project to be amended.

  - Only one compliance project may be active for a compliance domain at one time. Additional compliance projects may be defined for the same compliance domain, but their **Release Status** attribute must be set to **Draft** until the predecessor compliance project is completed and acquires a **Retired** release status.

- **Release Status** attribute of compliance project is set to **Retired**: The compliance project has been completed.

- **Release Status** attribute of compliance control set is set to **Retired**: Any running compliance projects will be irrevocably deleted and no new compliance projects may be created for the compliance control set.

Prerequisites for Compliance Management

Various configurations must be completed first before a compliance control set can be created and specified.

- The following must be defined by a solution designer in the configuration tool Alfabet Expand.

- The object classes that are the target of the compliance evaluation. Only object classes that have been configured in the XML object **ComplianceManager** may be targeted in a compliance project. The permissible object classes can then be selected in the **Compliance Policy** editor when the compliance evaluation is being configured. The following object classes may be the target of compliance evaluation:

  - `Application`
  - `ApplicationGroup`
  - `BusinessData`
  - `BusinessFunction`
  - `BusinessObject`
  - `BusinessProcess`
  - `Component`
  - `ComponentGroup`
  - `Demand`
  - `DemandGroup`
  - `Deployment`
  - `Device`
  - `DeviceGroup`
  - `Domain`
  - `ICTObject`

  - `ICTObjectGroup`
  - `Location`
  - `MasterPlatform`
  - `Peripheral`
  - `PeripheralGroup`
  - `Project:<Stereotype>`
  - `MarketProduct`
  - `MarketProductGroup`
  - `StandardPlatform`
  - `Technology`
  - `TechnologyGroup`
  - `Person`
  - `Vendor`
  - `VendorProduct`

- The queries used to find the targeted objects of a compliance evaluation. The queries must be specified in configured reports for which the **Category** attribute is set to `Compliance`. The relevant queries can then be selected in the **Object Queries** tab in the **Compliance Policy** editor when the compliance evaluation is being configured.

- The user responsible to answer a question for the target object can either be the authorized user of the target object or a user with a specified role for the target object. If a different user is required to answer the questions for the target object, then queries must be specified to find the users who are responsible for answering the questions. The queries must be specified in configured reports for which the **Category** attribute is set to `Compliance`. The relevant queries can then be selected in the **Permission Rules** tab in the **Compliance Policy** editor when the compliance evaluation is being configured.

- If the compliance controls should be prioritized in terms of the order in which they are executed, then queries must be configured that return the relevant compliance controls that should be answered for the compliance project. The queries must be specified in configured reports for which the **Category** attribute is set to `CompliancePrioritization`. The relevant queries to execute for the compliance project can be selected in the **Compliance Control Prioritization Policy** field in the **Compliance Project** editor.

- The color-coding used in the *Manage Objects Page View* to understand the completion state of an object's evaluation. This is also configured in the XML object **ComplianceManager**.

- A release status definition must be created for the object class Compliance Control Set (`ComplianceControlSet`) and Compliance Project (`ComplianceControlSetInstance`) in the XML object **ReleaseStatusDefs**. The release status definition also specifies the permissibility of which release status may transition to another release status. The release statuses implemented in Compliance Management will depend on your solution configuration. Each compliance control set and compliance project will have an approved status and a retired status although they may have different names. For more information about configuring release statuses for the Compliance Management capability, see the section *Configuring Release Status Definitions for Compliance Projects* in the reference manual *Configuring Alfabet with Alfabet Expand*.

- For more information about the configuration of the XML object **ComplianceManager** and the release statuses and queries required for the Compliance Management capability, see the section *Configuring the Compliance Management Capability* in the reference manual *Configuring Alfabet with Alfabet Expand*.

- A user with access to the **Evaluations & Portfolios** functionality must configure an evaluation type containing the indicator type to use as the metric to evaluate the targeted objects in the compliance evaluation. Please note that one indicator type is used as the metric for all questions in a compliance project. The indicator type should include the range of values that can be selected as an answer to the questions. For example, an indicator type have a range defined such as 0 - no action taken to date, 1 - compliance plan defined, 2 - plan partially implemented, 3 - plan fully implemented. 4 - not relevant. Please be aware that all questions posed in the compliance controls must be answerable based on the options associated with the indicator type defined for the compliance control set. The configuration of evaluation types and indicator types is described in the section *Configuring Evaluations, Prioritization Schemes, and Portfolios* in the reference manual *Configuring Evaluation and Reference Data in Alfabet*.

Specifying Compliance Control Sets and Compliance Domains

Compliance control sets are created and specified in the *Compliance Configuration Functionality*: You can specify multiple compliance control sets. The compliance controls defined for one compliance control set can be reused in another compliance control set.

- **Create one or more compliance control sets for the enterprise**. For each compliance control set, define the indicator type that determines the metrics that will be used to evaluate the architecture elements relevant to the compliance project. Please be aware that only one indicator type can be implemented for the compliance control set. Therefore, all questions posed in the compliance controls must be answerable based on the options associated with the indicator type defined for the compliance control set. The compliance control set is created in the *Compliance Control Sets Page View* available in the *Compliance Configuration Functionality*.

- **Create all compliance policies relevant for the compliance control set**. You must specify the configured reports containing the queries that determine the rules to find the objects that will be the target of the project as well as the users that will be responsible for answering the questions about those objects. These compliance policies will be available for the compliance controls and must be explicitly assigned to the compliance controls that they are relevant for in the *Compliance Policies Page View* available for each compliance control.

  - For each compliance policy, you can specify one or more object queries to find the objects targeted by the compliance evaluation. Please note that it is possible to specify a queue for

the compliance policies in the context of the *Compliance Policies Page View* available for each compliance control.

> A compliance control targeting application security checks that sensitive applications are operated in a secured physical environment. The compliance control has two compliance policies assigned to it. One compliance policy **Applications Supporting Revenue-Generating Processes** finds applications supporting business processes that are relevant for sales. The other compliance policy **Critical Applications Requiring Access-Control and Video-Surveyed Facility** finds applications that are general candidates for IT security. The applications supporting business processes may or may not be critical applications requiring access control.
>
> In order to find out which applications supporting revenue-generating business processes also fulfill the criteria for critical applications requiring access control, the queries must be queued. In this case, the compliance policy **Applications Supporting Revenue-Generating Processes** should be executed first and the compliance policy **Critical Applications Requiring Access-Control and Video-Surveyed Facility** should be executed next as a second set of criteria. To configure this query scenario, the **Base Use** attribute would be set for the compliance policy **Applications Supporting Revenue-Generating Processes** and the **Update** attribute would be set for the compliance policy **Critical Applications Requiring Access-Control and Video-Surveyed Facility**.

- For each compliance policy, you can specify either the authorized user and/or users with a specified role to answer the compliance questions. Or, if other users are required to answer the compliance questions, you can specify one or more queries to find the relevant users.

- Compliance policies are assigned to the compliance control set in the *Compliance Policies Page View* available in the object profile of the compliance control set.

- **Structure a hierarchy of compliance controls for the compliance control set**. The most descendant control in each leaf hierarchy represents a question to be asked in an inquiry.

  - The compliance controls are structured hierarchically. You may create an unlimited number of top-level compliance controls for the selected compliance control set. Each top-level compliance control represents a branch in the network of compliance questions. Compliance controls at the top-level of the hierarchy are defined in the *Top-Level Compliance Controls Page View* of the compliance control set

  - Each subordinate compliance control is defined in the *Subordinate Compliance Controls Page View* of the parent compliance control. The most subordinate compliance control in the hierarchy leaf is the compliance control in which the question is defined. The question that is asked in the evaluation must be defined in the **Description** attribute of the leaf-level compliance control in the hierarchy. Please note that the lower the compliance control is in the compliance control hierarchy, the more granular should be the description. If the compliance control is at the leaf-level of the compliance control hierarchy, then the **Description** attribute should contain the question being posed for the target object. Please be aware that the question posed must be answerable based on the options associated with the indicator type defined for the compliance control set.

- **Assign the relevant compliance policies defined from the compliance control set to the relevant compliance control**. All compliance policies created for the compliance control set will be automatically displayed in the *Compliance Policies Page View* available for each compliance control but they must be explicitly assigned as needed to the relevant compliance control. The compliance policies are used to find the target objects and users that are relevant for the compliance control. Please note the following:

- If the compliance policy is relevant for the entire hierarchy of compliance controls in a branch, then the compliance policy should be assigned to the top-level compliance control. If compliance policies have been explicitly assigned to an ascendant compliance control, the subordinate compliance controls will inherit the compliance policy definition unless the compliance policy definition is changed for the compliance control. In this way you can refine the assignment of compliance policies by adding or removing compliance policies.

- You can specify a queue for the compliance policies so that objects found by a first compliance query are reassessed by a second compliance query. In this way, you can specify that a compliance policy 1 is used to implement the first set of criteria to find target objects and then a second compliance policy is implemented to find objects based on a second criteria.

   > A compliance control targeting application security checks that sensitive applications are operated in a secured physical environment. The compliance control has two compliance policies assigned to it. One compliance policy **Applications Supporting Revenue-Generating Processes** finds applications supporting business processes that are relevant for sales. The other compliance policy **Critical Applications Requiring Access-Control and Video-Surveyed Facility** finds applications that are general candidates for IT security. The applications supporting business processes may or may not be critical applications requiring access control.
   >
   > In order to find out which applications supporting revenue-generating business processes also fulfill the criteria for critical applications requiring access control, the queries must be queued. In this case, the compliance policy **Applications Supporting Revenue-Generating Processes** should be executed first and the compliance policy **Critical Applications Requiring Access-Control and Video-Surveyed Facility** should be executed next as a second set of criteria. To configure this query scenario, the **Base Use** attribute would be set for the compliance policy **Applications Supporting Revenue-Generating Processes** and the **Update** attribute would be set for the compliance policy **Critical Applications Requiring Access-Control and Video-Surveyed Facility**.

- If changes have been made to the compliance policies assigned to an ascendant compliance control in the compliance control hierarchy, you can update the selected compliance control so that it inherits the changes made to compliance policies. This is done via the **Inherit Policy Adjustment** button in the *Compliance Policies Page View*.

- **When the compliance control set is complete, change the release status to Approved.** Once a compliance control set has been approved, the compliance control set including the compliance control hierarchy cannot be changed. Please note however that compliance policies can be added to and edited for a compliance project that has the **Release Status** attribute set to **Draft** or **Active**. In other words, after a compliance project has been activated, the compliance policies can be amended in the context of the running compliance project in the *Compliance Policies* for the relevant compliance project.

- **Define compliance domains**. Define one or more compliance domains that represent the topical or geographic areas for which compliance projects are to be executed. A compliance project can be activated for a specified compliance domain or it can be activated independent of a compliance domain definition. The compliance domain is created in the *Compliance Domains Page View* available in the *Compliance Configuration Functionality*.

Initiating and Managing Compliance Project

Compliance projects can be created once the compliance control set has been approved. You can create, modify, activate, and manage a compliance project in the *Compliance Projects Functionality*.

- **Create the compliance project.** To do this, you must select the compliance control set that the project is based on as well as the compliance domain that the project will target. When the **Release Status** attribute of compliance project is set to **Draft**, the compliance project is initiated for a selected compliance domain and for a specified period of time. Compliance policies may be added, deleted, or edited. The compliance project is created in the *Compliance Projects Functionality*.

  - When the **Release Status** attribute of compliance project is set to **Active**, the compliance project will be activated. The **Activate Compliance Project** option in the **Compliance Projects** functionality will only be available for compliance projects with the approved release status (**Active**). Please note the following:

    - The compliance policies may be edited. No new compliance policies may be added to the compliance project.

    - The compliance project becomes a running project when it's start date is reached. Email notifications will be automatically sent to responsible users and assignments will be generated for each compliance control that they are responsible for.

    - Please note the following changes that can be made to a compliance project that has been approved:

      - If a compliance project has been approved, the compliance policies may be edited. No new compliance policies may be added to the compliance project.

      - If additional objects that were not found by the object queries need to be added to the compliance project, a functionality is available that allows the compliance project to be amended.

    - Only one compliance project may be active for a compliance domain at one time. Successor compliance projects may be defined for the same compliance domain, but their **Release Status** attribute must be set to **Draft** until the predecessor compliance project is completed and acquires a **Retired** release status.

  - If compliance controls (the questions about target objects) are to be prioritized in terms of the order in which they are executed in a compliance project, you can select configured reports that have been configured to find the compliance controls that are relevant for the compliance project. For example, a query could specify that only compliance controls on with a **Level ID** attribute of 1, 2, and 3 are relevant to a compliance project. Once the first compliance project is completed, you could then initiate the compliance project again and specify that compliance controls with a **Level ID** attribute of 4, 5, and 6 are relevant to a compliance project. The queries will return the relevant compliance controls that should be included in the compliance project. The relevant queries to execute for the compliance project can be selected in the **Compliance Control Prioritization Policy** field in the **Compliance Project** editor.

- **Modify the compliance policies**. While the compliance project has a **Draft** release status, you can add new compliance policies or edit the existing ones. Once a new compliance policy has been created, it must be manually added to the existing compliance project controls. To achieve this, go to the *Top-Level Compliance Controls Page Vie* available for the compliance project. Select the compliance project control that the new compliance policy shall be applied to, click the **Navigate** button and open the *Compliance Policies Page View*. Click the **Compliance Policy Adjustment**

button and in the editor that opens, set a checkmark in the **Base-Use** column for the compliance policy that shall be applied to the compliance project control.

- **Activate the compliance project**. Once the compliance project is activated, automatic email notifications and assignments will be sent to all users that have been identified as responsible for assessing a target object. The project will become a running project when it reaches its start date. The compliance project is activated in the *Compliance Projects Functionality*.

- **Review the existing target objects in the compliance project**. The existing target objects are displayed in the *Manage Objects Page View* for the compliance project. You can also add additional target objects to the compliance project that were not find by the compliance policies.

- **Review the completeness of the assessment of the compliance project**. All relevant users can be sent email notifications about pending compliance project controls that they are responsible for evaluating for a specific object. The compliance project can be tracked in the following views and emails can be sent to remind users to process their target objects:

  - The *Evaluation Summary Page View* allows you to view the objects that must be evaluated by the compliance project, assess how complete the evaluation is, and notify the responsible user(s) about their evaluation.

  - The **Quality Assessment** page view displays a pie chart showing the breakdown of the values defined in the evaluation of the target object in the compliance project.

  - The *Completion State Page View* displays a pie chart showing the percentage of the questions that have been completed for a given object class in the selected compliance project versus the percentage of questions that are still pending.

- **Create a successor compliance project**. The successor compliance project will inherit all compliance controls and compliance policies defined for the compliance project that it is based on. The start date for the new compliance project will be automatically set to the day after the end date of the selected compliance project. After the new compliance project is created, you can modify the attributes including the start date, as needed. The successor compliance project is created in the *Compliance Projects Functionality*.

Assessing the Objects Targeted by the Compliance Project

Users responsible for a compliance project control will receive an assignment about it in the *My Assignments Functionality*. They can double-click the assignment to navigation to the views where the questions posed about the target object can be processed.

The target objects are evaluations by the responsible users in the *Compliance Evaluations Functionality*. To access the target objects that a user is responsible for in the compliance project, double-click the relevant compliance project in the **Compliance Evaluations** explorer: There are two different methods for a user to answer questions regarding objects. Wizards guide the user through the process of answering the relevant questions:

- The *Evaluation by Objects Page View* allows users to answer the same question for all target objects relevant to the compliance project on a question-by-question basis. In other words, this method of completing the assessment allows you to answer one question pertaining to all target objects.

- The *Evaluation by Compliance Controls Page View* allows users to answer all questions for objects in the selected compliance project on an object-by-object basis. In other words, this method of

completing the assessment allows you to answer all questions pertaining to an individual object, and then move on to the next object.