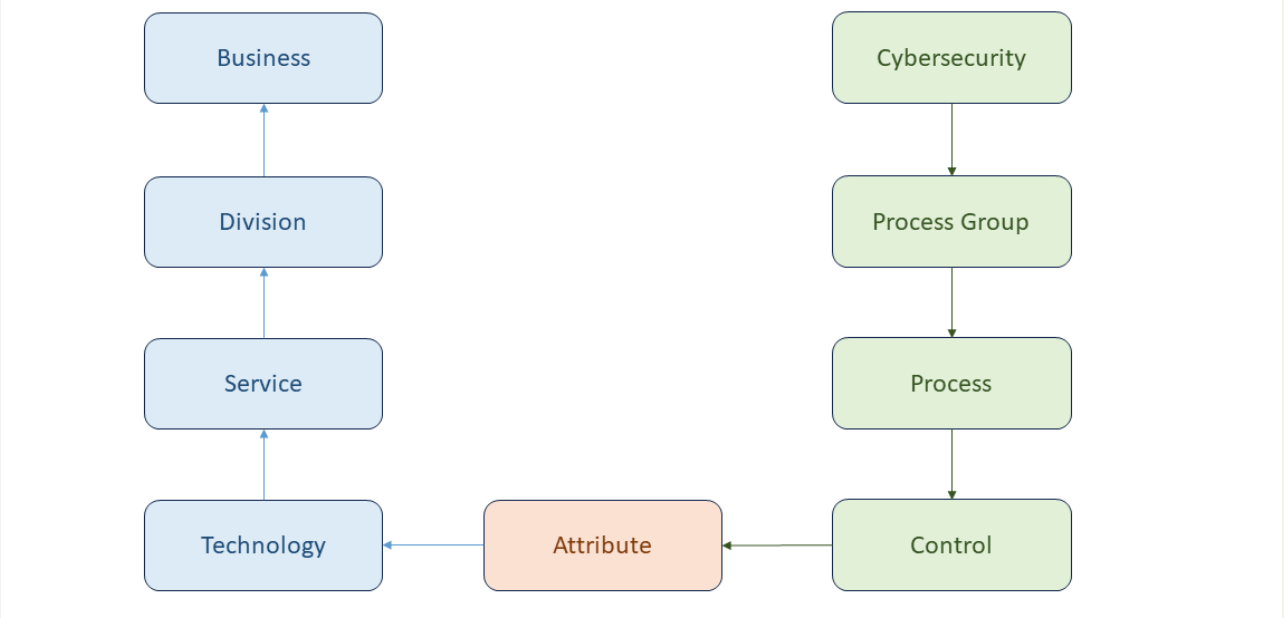
User Guide: COBRA

Introduction

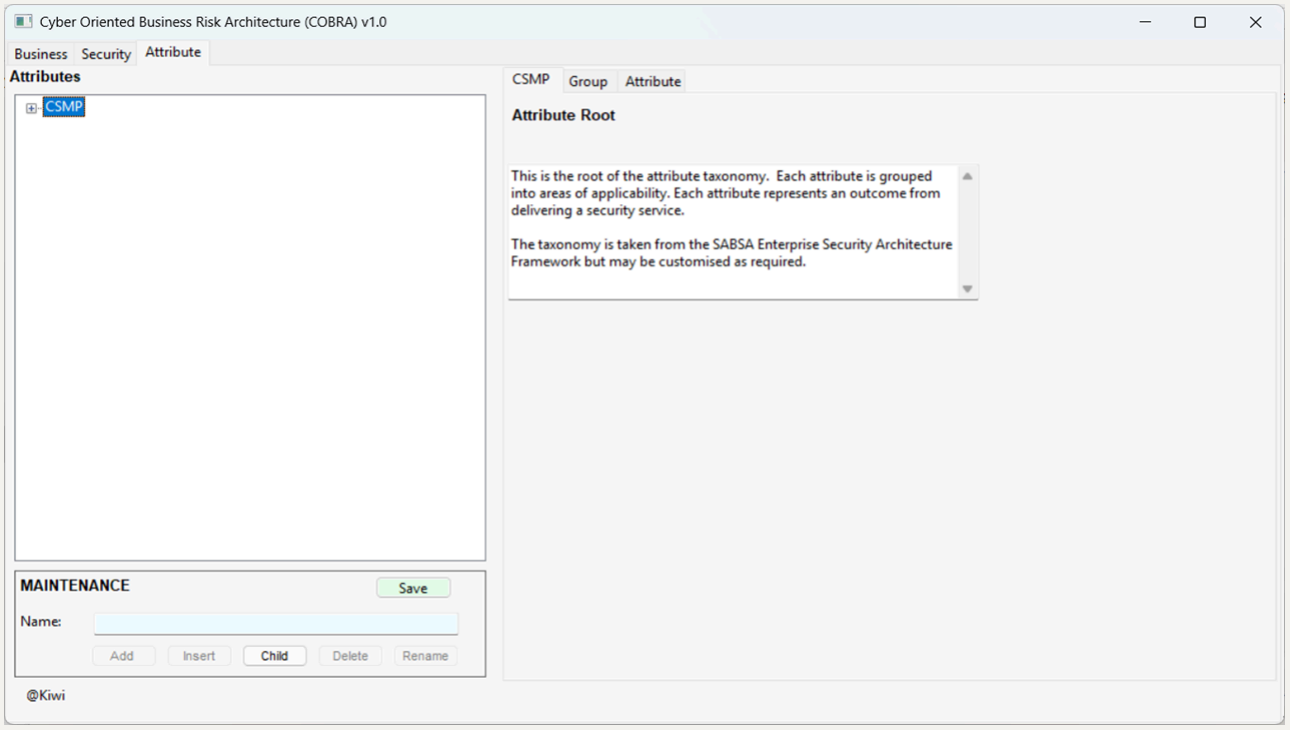
The *cobra* package has been developed to support the assessment of how effectively cybersecurity management supports the business. The package is driven by a first-order model of the business represented as business divisions, and within the divisions the services which directly or indirectly deliver value to the business. The cybersecurity activity is modelled as a set of strategic, tactical, and operational processes which result in cybersecurity controls in support of the technology used in the business services. The two sides of the model are shown below, linked by a concept known as *attributes*.



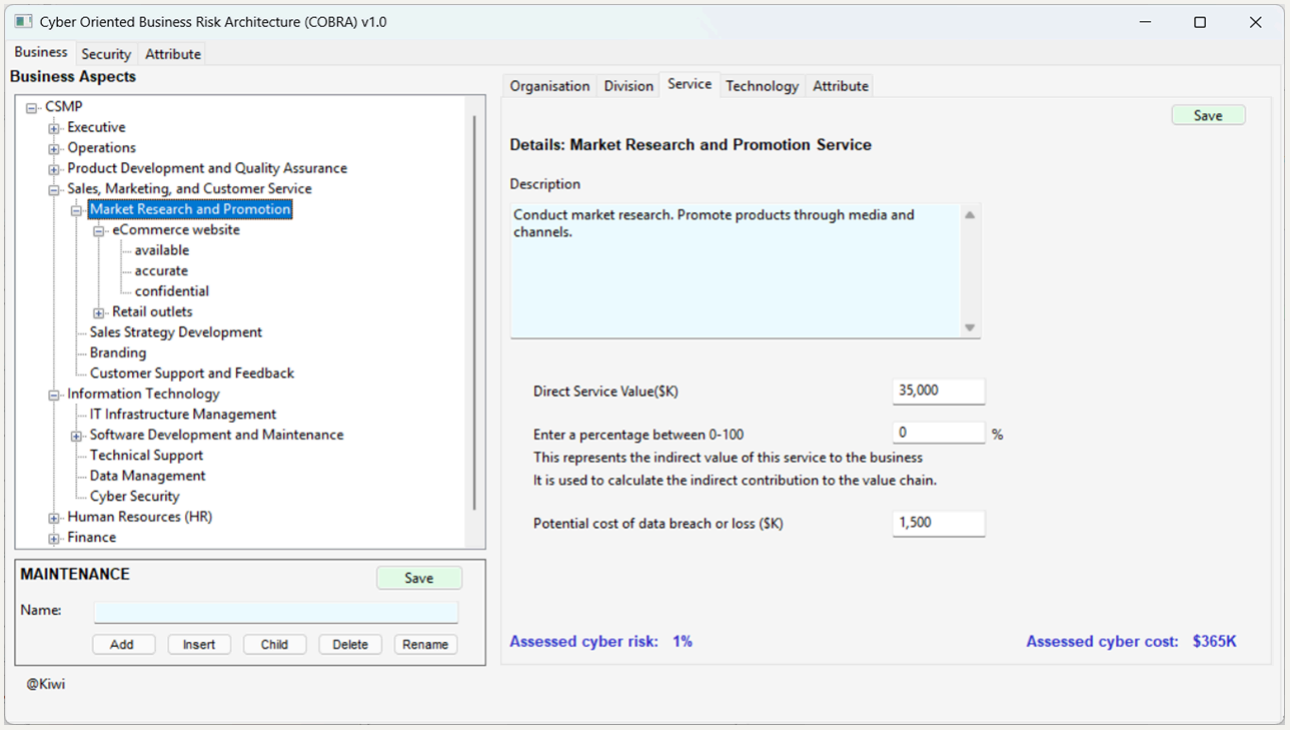
Attributes are a concept introduced in the SABSA Enterprise Security Architecture framework, and represent the atomic elements of security that are required to ensure business outcomes are delivered. They provide a common language in which the business can request security and the cybersecurity team can deliver it. In the *cobra* model, the delivery of cybersecurity into the technology, and the effectiveness of that technology in supporting business services, is represented through the use of SABSA attributes.

User Interface

The *cobra* package is a GUI application which runs as a Python script. This is supported by an internally managed sqlite3 database. The main GUI screen is as shown below.



The interface is in two parts: at the left a tree structured view of the business, security, and attribute elements; and a details panel on the right. The panels at the right are activated when an element of the tree is selected, as below.



Each of the left-hand details panels has a *Save* button which is used to save any changes made in the panel.

Similarly, the tree structures all have a Save button at the bottom which is used to save the active tree after any changes have been made.

Initial Setup

If the cobra script is run with no database in the script folder then a new database will be created. This will have an initial business entry called Executive, the three process groups of strategic, tactical and operational but no security processes, and the standard SABSA attribute taxonomy groups but no attributes. If the script is run with a populated database in the same folder, then the database information will be loaded. A pre-populated database is provided with a basic demonstration set of elements.

When setting up the cobra data, you should enter the business data under CSMP as Divisions, then within each Division enter the Services that it provides. Then under each Service, enter the Technologies that are used to deliver those services. Finally, under each Technology, enter the security attributes that are relevant to the service. Under the Security tab, you will find the three groups of security processes (Strategic, Tactical, Operational). Under each, you should add the relevant security process. Then within each security process, you should enter the controls delivered through that security service. Finally, under each control, you should add the relevant attributes for that control. Finally, under the attributes tab, you should enter your attribute taxonomy. This can be a simple list of attributes, or a hierarchical grouping. Once you've set it up, don't forget to save it.

Business Viewpoint

The Business Tree Controls

The left hand *Business* tab provides the business viewpoint. After clicking it and expanding the top level CSMP item, the business is described as a series of business divisions. If this is a new database then there will be no existing business structure. You will need to create the business divisions you require by entering the division name in the textbox below the left hand panel and selecting *Child*. This creates a division which is a child of the root item. To create an entry at the same level as the selected item, then enter the name in the textbox and press *Add*. pressed to add an entry at the same level

below the currently selected item. By clicking *Insert*, the entry is added above the currently selected item.

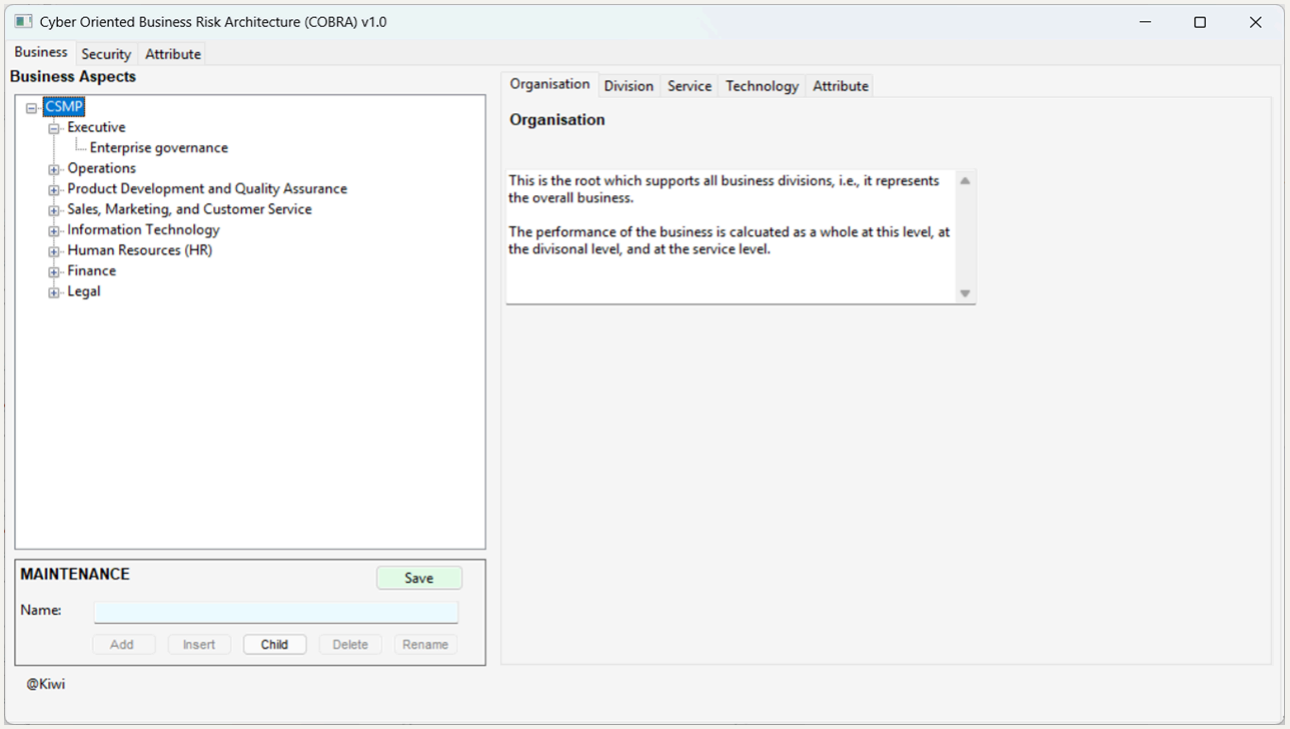
The *Delete* button will delete the currently selected entry, after confirming that you do indeed want to delete it. IO you want to change the name of an item in the tree, then double click it to have the item's name placed into the textbox, change it, and click *Rename*.

Don't forget, these changes won't be saved automatically. If you make changes and then quit, they will be lost. In order to save them, press the *Save* button which is located below the left hand panel.

Note that while the right hand panel tabs can be activated manually, only the page as selected in the tree will eb active; all others will be disabled.

The Business Root

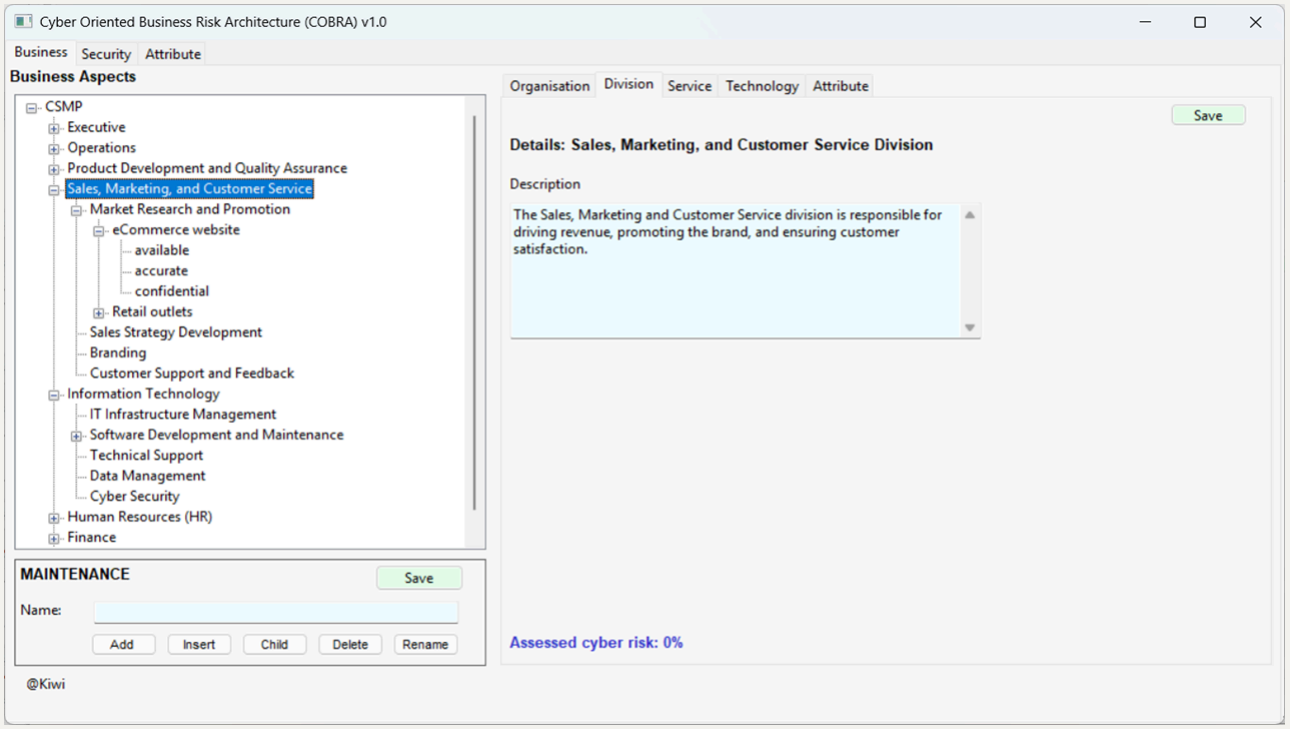
The Business Root has a standard description which cannot be changed and so there as no *Save* button on this panel.



Note that only the *Child* button below the left hand panel is active, as this is the only valid action at this level. By entering a name in the textbox and pressing *Child* a new Division will be added to the business.

The Business Division

Let's look at a business Division.



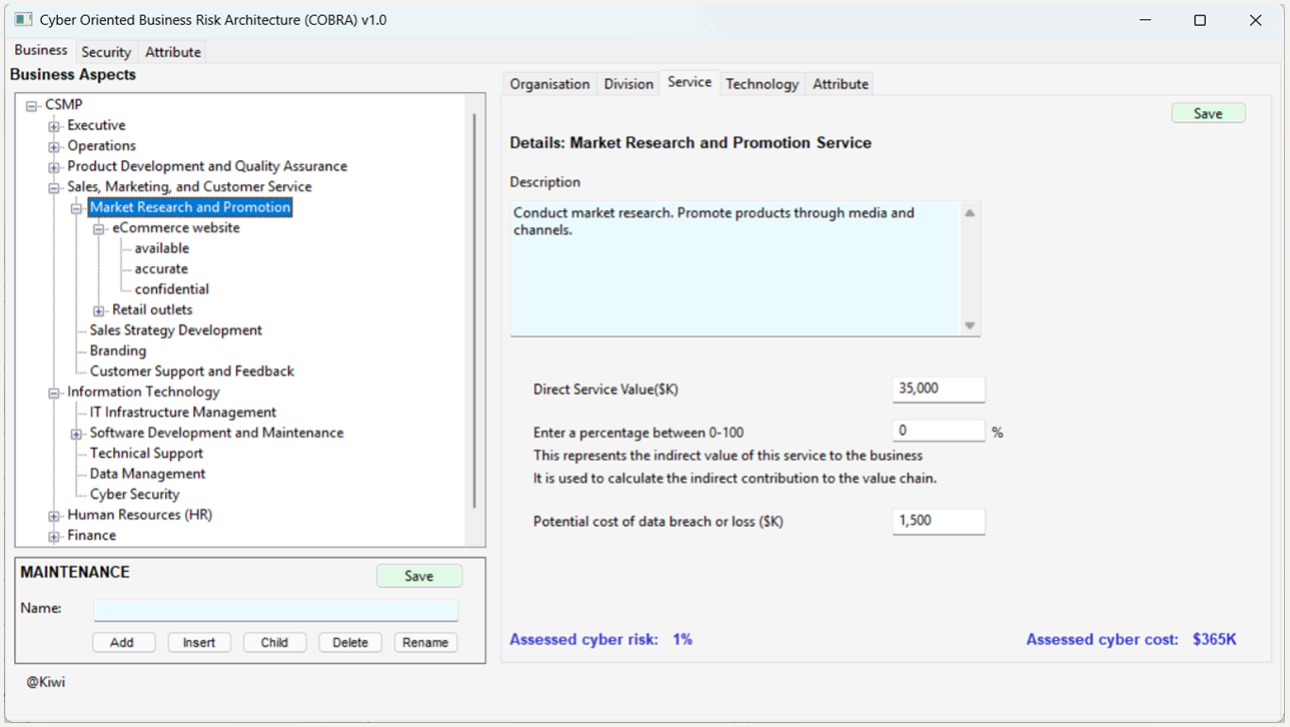
By expanding the top level *CSMP* root, the Divisions will be shown. Above we see an entry for **Sales and Marketing** which has a description and, at the bottom, shows the current level of cyber risk for the Division as a whole. This figure is based upon the cyber security risk assessment, which we'll cover later in this document.

The *Description* can be changed to reflect the Division activities, and saved by clicking *Save*.

A new division can be added by entering its name in the textbox below the left hand panel, and the pressing *Add* to add it after the current selection, or *Insert* to add it before the current selection. The new entry will have a blank description, this can be added and saved as required.

The Divisional Services

A business division consists of a set of services which either directly (through revenue) or indirectly (through support to revenue generating divisions) support the goals and objectives of the division. By expanding a division entry in the left hand panel, all the services provided by that division are shown. Let's take a look at a service.



The *service* is the key business element in the model, as this is where we represent the value of the business. There are three fields that we use to do this.

- **Direct Service Value**. The direct service value is the revenue that is gained for the business by running this service. In the example above, the *Product Promotion* service is shown as delivering $7.5M in sales. The service can be as granular as we like, but as a rule of thumb the services that use the same technology can be aggregated into a single service line as that is the level of granularity of the risk calculations.
- **% enabling the business**. There are many services which do not result in direct value. These include internal services such as *Finance* and *Logistics*, as well as services such as *compliance* activities. In either case, there is a cost of not doing them which we represent as an overall % reduction in the performance of the business.
- **Potential cost of data breach or loss**. The cost of a failure of the underlying technology for a service is represented as a reduction in the revenue earned by the service. However, in addition to that, there is the potential for breach of data and the attendant costs of remediation, which will be related to the kind and amount of data stored, or the loss of data through destruction of ransomware. While not affecting the service itself, these events will have associated direct costs. The costs of such events are represented separately as the potential cost of a data breach.

The **Market Research and Promotion** service above has the details of its contribution to the division's activities in the right hand panel. In order to add a service to a division, we enter the service name in the textbox below the left hand panel. If we have the division select, we press *Child* to add it to the next level down. If we have a service selected, then we add a new one by clicking either *Insert* or *Add*.

The right hand panel contains a service description. This is blank for a new service and can be added as required.

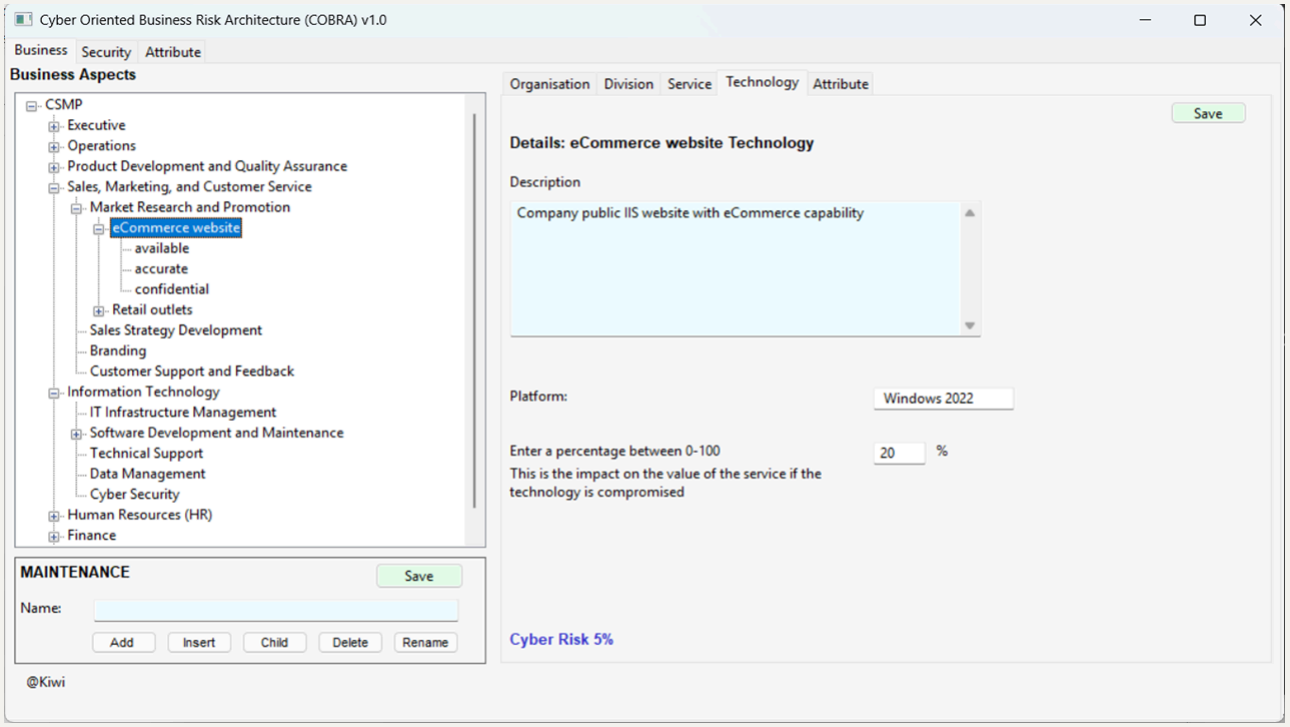
At the bottom we find the assessed cyber risk to the service, based on the cyber risk to the technologies used in that service. In this case, we see that the service could in the event of a cyber attack suffer up to a 3% impact. The cost of this is assessed as the risk percentage applied to the service revenue and the data breach/loss value. This is shown as the *Assessed cyber cost*.

The cyber risk is also applied to as a reduction in the overall business value calculated as the % enabling the business multiplied by the risk factor. This impact is not shown on this panel, but is aggregated with other enabling service risks to the business as a whole.

As usual, any changes made to the right hand panel require the *Save* button in the panel to be pressed to store them. Similarly, and changes made in the left hand panel requires the *Save* button to be pressed to save those changes.

The Service Technologies

Each service can be expanded to show the technology used to support that service. The cybersecurity program provides controls which protect the technologies used to run services. These may be revenue generating services, or they may be internal support services.



In the example above, we have an eCommerce website which is used to deliver direct product information to customers and also to support channel sales. The right hand panel has a description of the technology and an informative reference to the platform being used (this does not feature into the risk calculations at this stage, but is for information only).

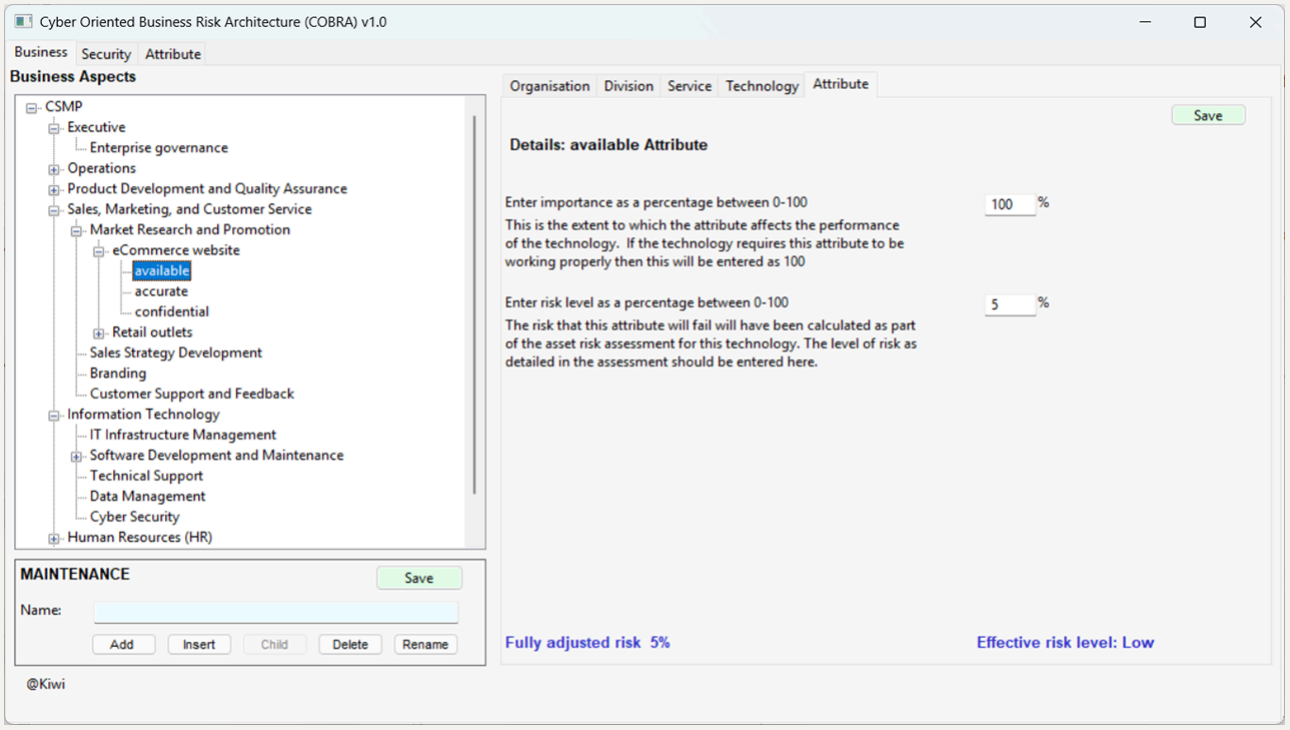
We represent the importance of the technology to the service as a percentage, indicating the loss of service value that would occur should the supporting technology be disrupted. In this example, we're indicating that there would be a 20% loss of revenue from the service, as well as a 20% chance of the data being breached or lost, in the worst case cyber attack.

The risk of a cyber attack being successful is shown in blue at the lower right. This is calculated from the underlying attributes of the technology.

As with the other elements, technologies can be added, change and removed by using the controls below the left hand pane.

The Technology Attributes

In the SABSA framework for enterprise security architecture, risk to technology is represented as a set of attributes. Attributes can be associated with a technology by adding them as children of the technology, as shown below.

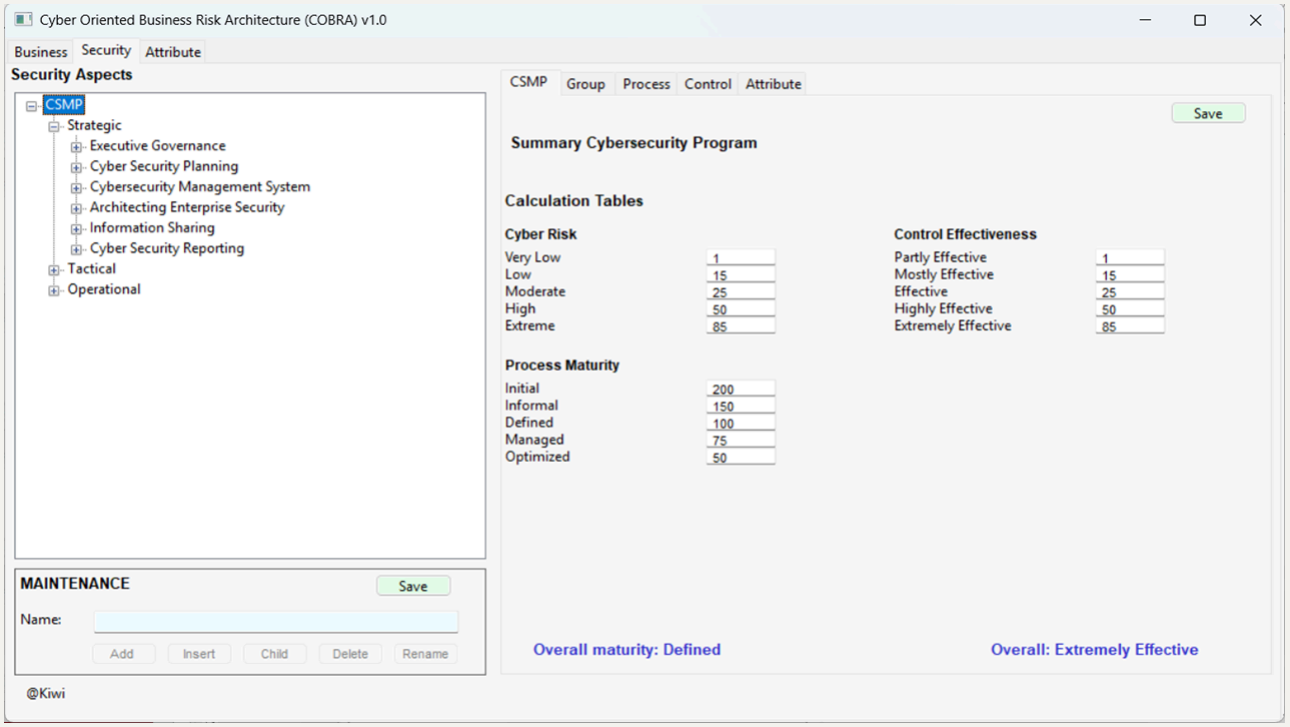


In this example, there are three attributes associated with the eCommerce website, and we've selected the first one, *available*. Individual attributes may be relatively more of less important in the technology, and this is represented as a percentage which reflects the maximum impact on the technology should that attribute be degraded or fail. This screen is not the main *attribute* screen, but just the link connecting the main attribute information with the technology.

Cybersecurity Viewpoint

The Cybersecurity Tree Controls

The *cobra* application provides a separate cybersecurity viewpoint. This is where the cybersecurity program is run to deliver security in the form of attributes. This part of the model starts with the cybersecurity program as a whole as shown on the main *CSMP* tree root.



This screen provides the context for the risk calculations, i.e. the thresholds at which risk, maturity, and effectiveness levels change. These should be adjusted as appropriate to the business being modelled.

At the bottom of the screen we find the summarized maturity of the cybersecurity program based on the maturity ratings entered on all processes, together with its overall level of risk that controls will fail based on attribute risk levels.

The overall maturity is calculated as:

```
(process weight * operational maturity) per process, divided by the
sum of the weights.
```

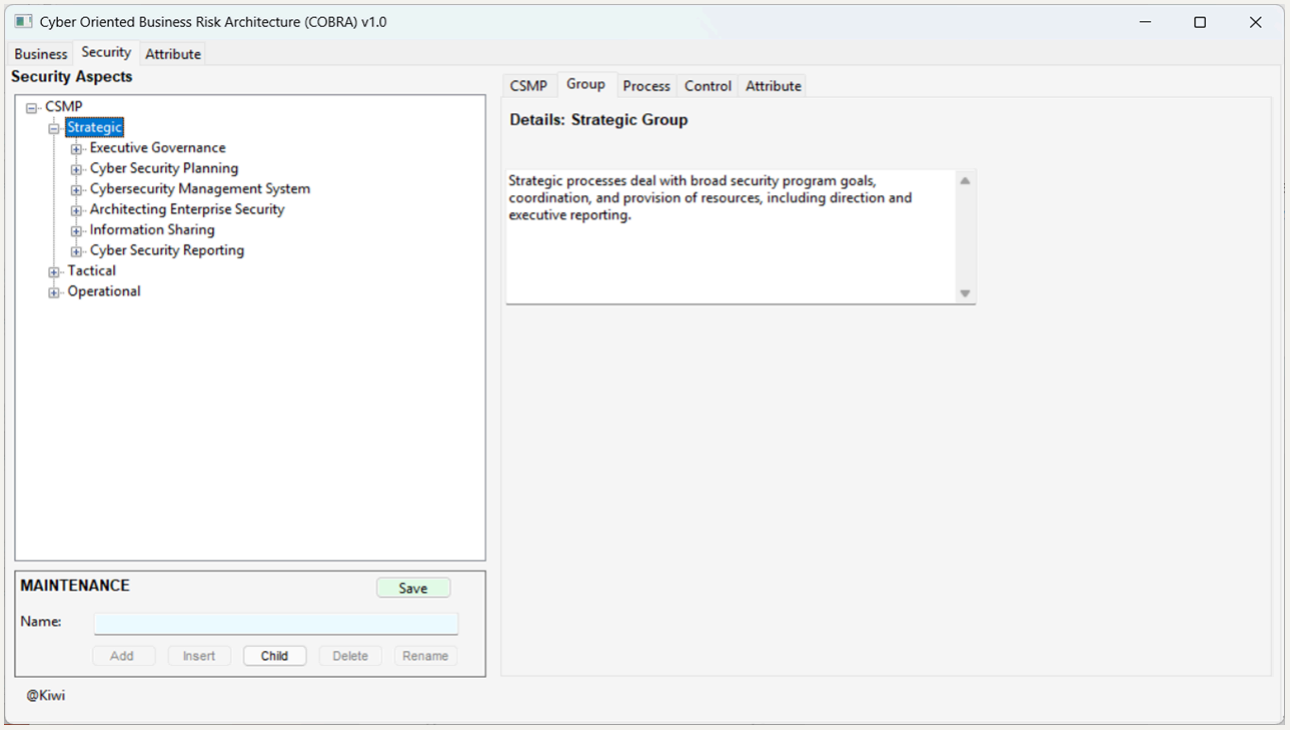
The overall effectiveness is calculated as

```
average effectiveness across all controls,
where effectiveness is weight *(100% - risk%) per control
```

The Cybersecurity Group

The processes are grouped into the three tiers of *Strategic*, *Tactical* and *Operational* controls. However, there is no difference in the way controls are handled between groups. This is just to allow for easier navigation. There are three groups predefined in the database: Strategic, Tactical, and Operational to align with the ISM3 approach to process

measurement.

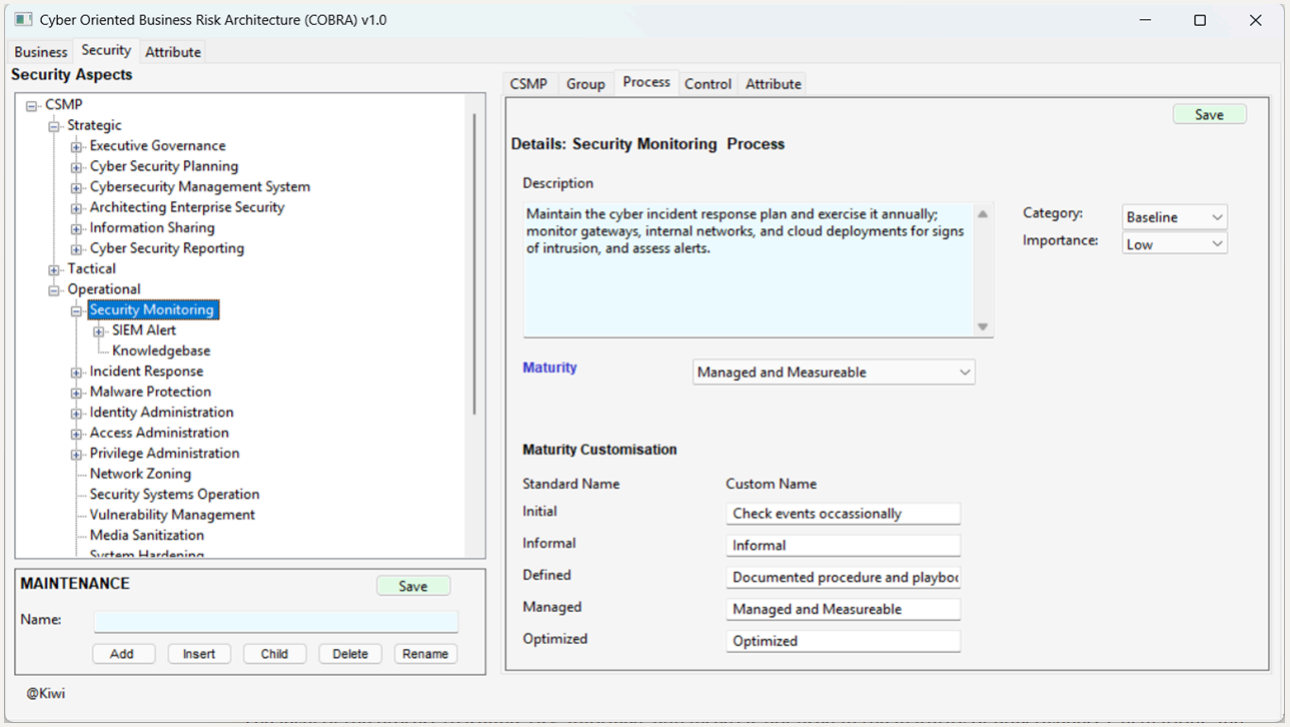


The description is hard coded and so there is no requirement to save the group details.

The Process Details

The cybersecurity process is where maturity of the cybersecurity program is established. Each process has two maturity values: (a) the capability maturity of the process, which ranges from non-existent to fully deployed (together with all supporting technology); and (b) for those processing in some form of deployment, the operational maturity of the process.

The description associated with the operational and capability maturity is customizable per process.

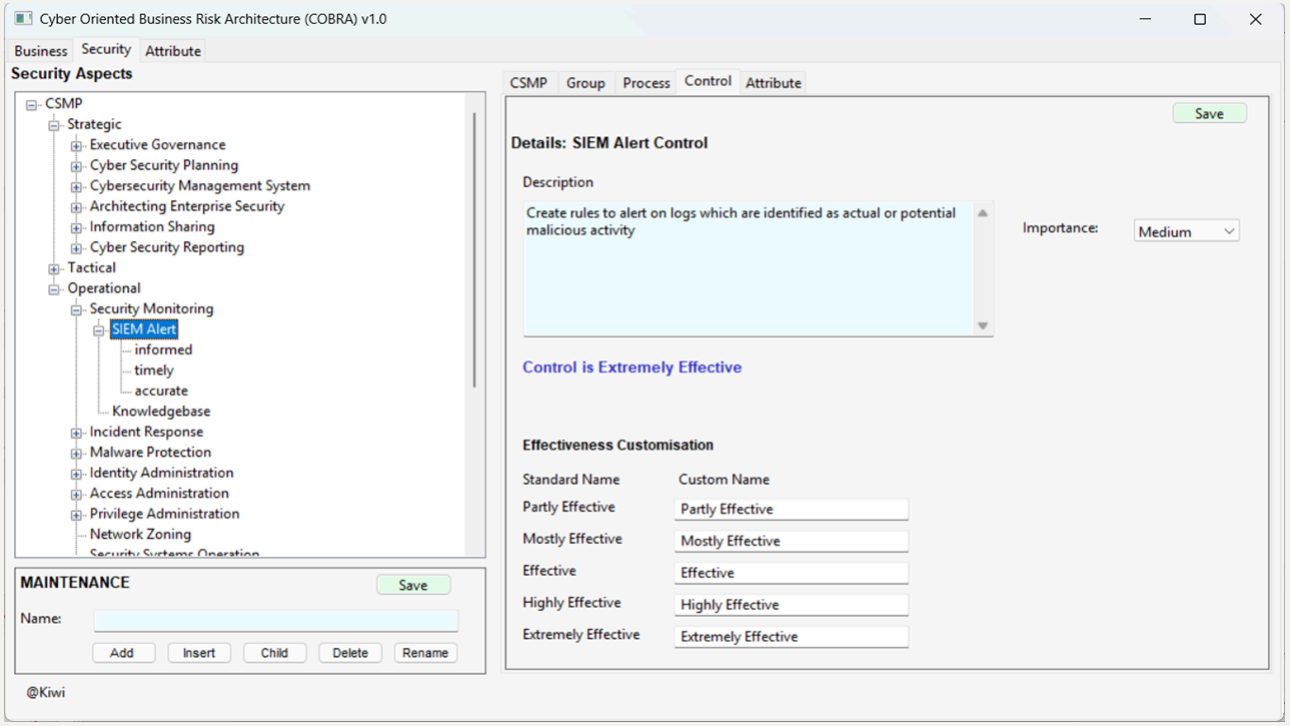


The level of the process (baseline, risk-informed, enhanced) is not used in the maturity or effectiveness calculations and is purely for information. The weight is used to determine extent to which the process contributes to the overall maturity of the cybersecurity program.

Calculating the maturity values of the process is carried out outside of this tool, and the results are then entered using the two drop down controls.

The Control Details

The cybersecurity program is in essence the cybersecurity processes. The objective of the cybersecurity processes is to deliver a defensive control for the business to use in the technologies which support their activities. Not all cybersecurity processes deliver operational controls for the business to use, for example the development of an enterprise security architecture does not contribute a control directly, but it has an impact on the effectiveness of the cybersecurity program as a whole and so can degrade or enhance those cybersecurity processes which do deliver controls.



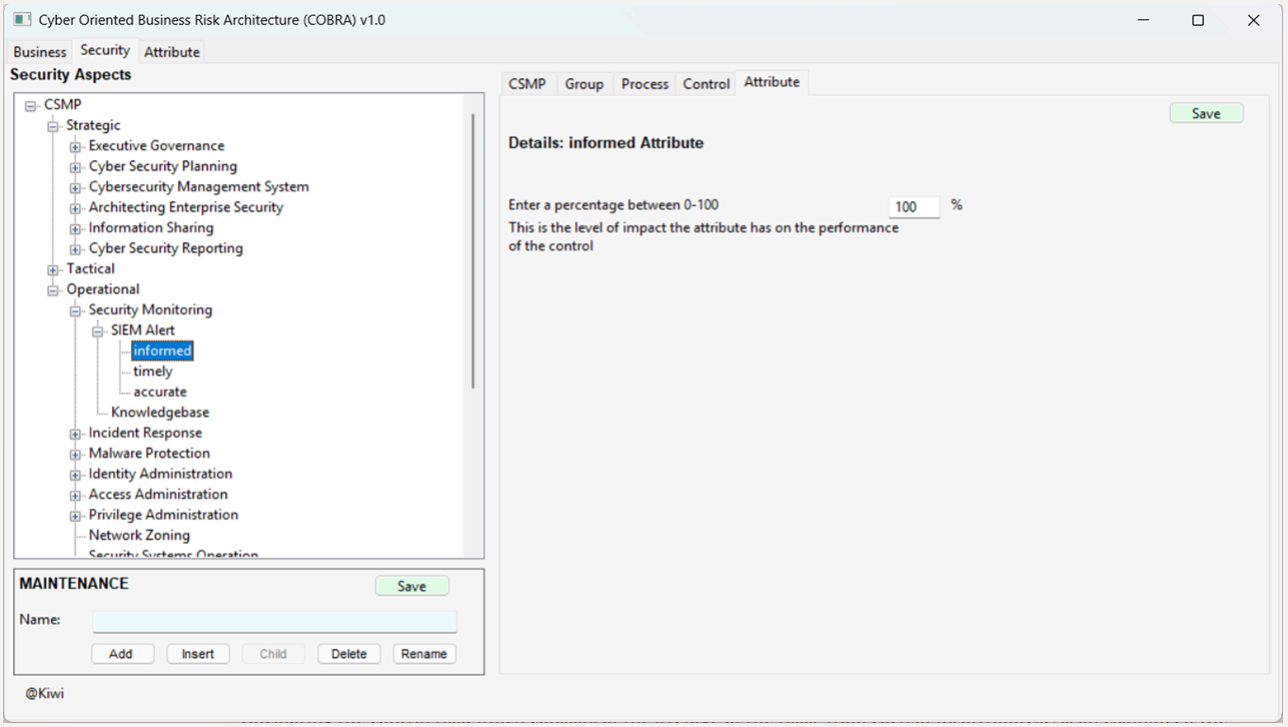
The control weight is used to factor the control effectiveness relative to other controls.

The control effectiveness is calculated by aggregating the underlying attribute risk.

The Control Attributes

Controls deliver security capability in the form of SABSA *attributes*. These are the security primitives which are applied to technology, such as *availability*, *integrity* and so on. SABSA provides a standard repository of attributes which we can use, or we can define our own. The SABSA attributes are described as attribute groups, with groups being focused on a particular type of use. The groups are for convenience as attributes the group makes no difference in the way in which attributes are used.

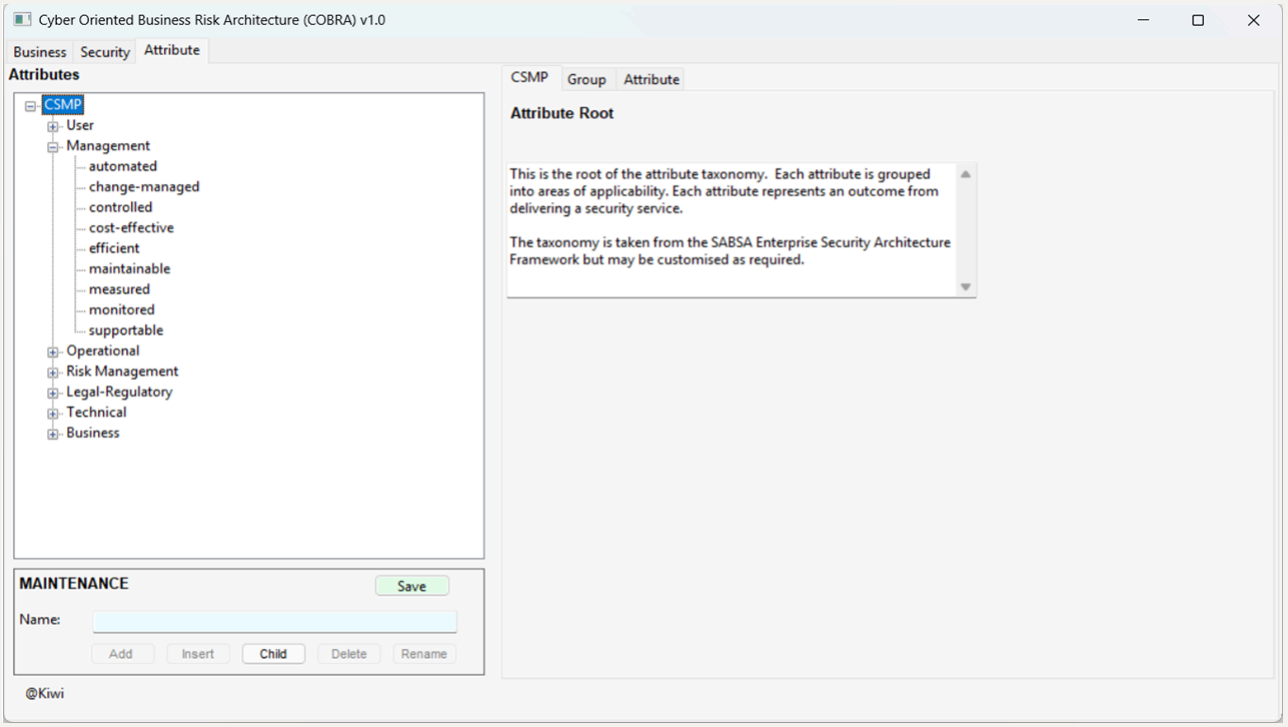
The control attributes are not the main attribute record - they are, like business attributes, a link between the main attribute record and the control record.



The link indicates the impact that the attribute will have on the performance of the control. This is then used when calculating the control risk, which consists of the average of the risks from each of its attributes. As an example, if the attribute has been assessed as having a 10% risk, and the impact on the control is 20%, then the resulting risk contribution at the control level from this attribute would be 2%.

The Attribute

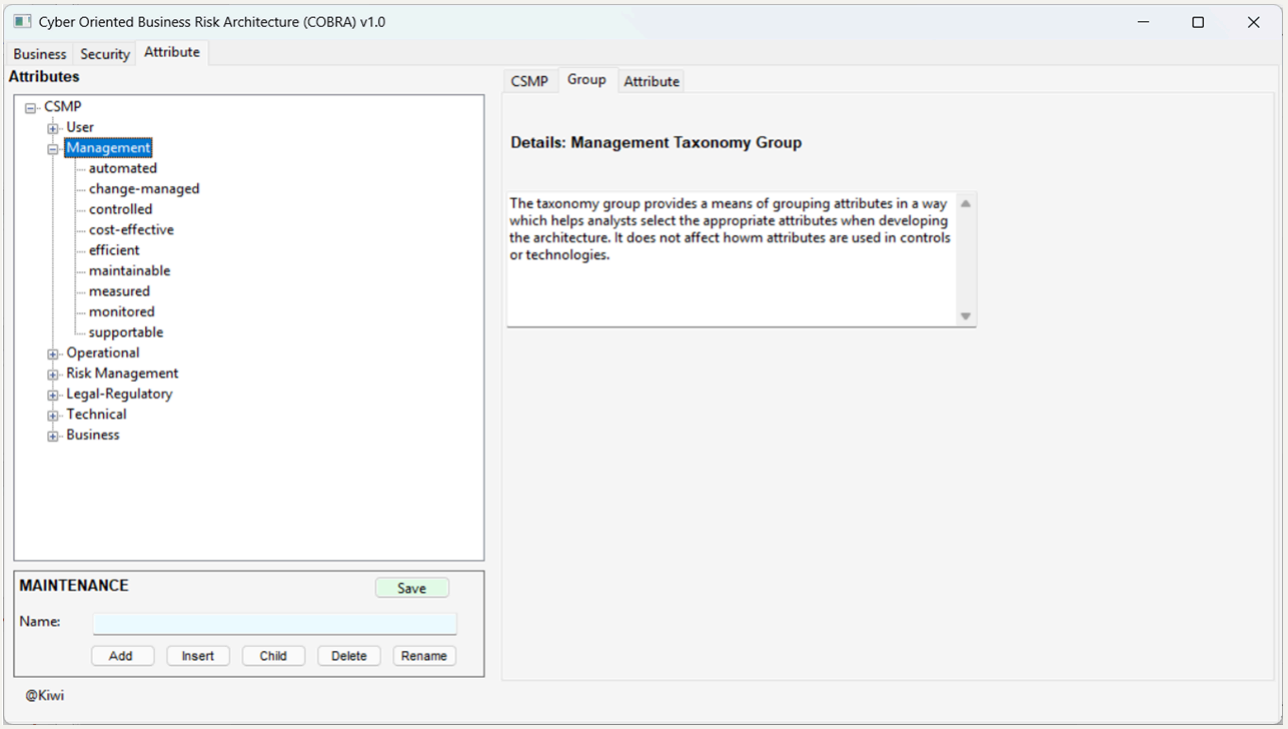
The Attribute tab provides a view of the main attribute record shown in groups. Attributes are in two tires - taxonomy group and attribute. When setting up a new database, the standard SABSA taxonomy with the groups *User*, *Management*, *Operational*, etc as shown below will be created. However, you can change these should you wish to use a different taxonomy.



The controls for adding data to the *Attribute* tree are the same as for the *Business* and *Security* trees.

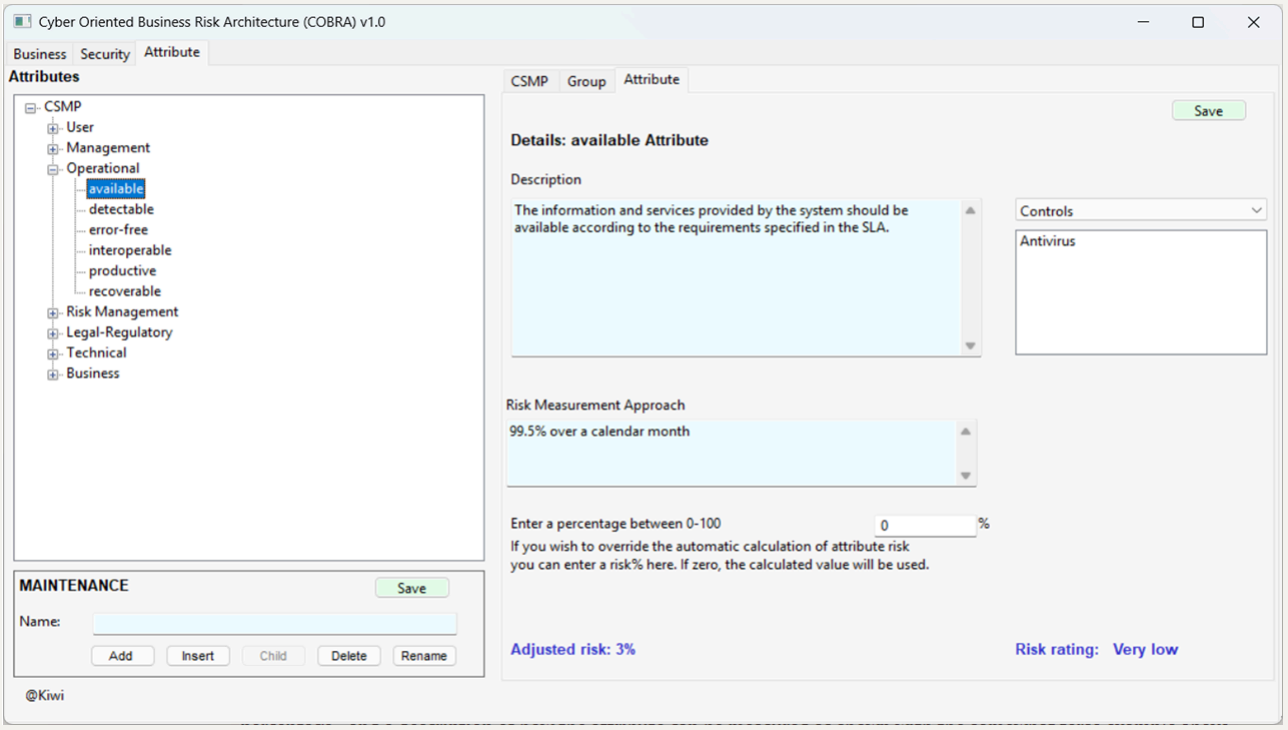
Attribute Group

The attribute group is just a convenient means of group a relatively large number of attributes and has no data associated with it.



The Attribute

The attribute record is the key to linking the security activities with the business activities.



The attribute has a descriptive field, with SABSA providing standard descriptions for the SABSA set of attributes but with a caveat to customize them to be in the language of the business. The description should be specific to the purpose of the attribute.

Each attribute has to be measurable in risk terms. The attribute record captures the type of metric - in this case a percentage - and a description of how the attribute can be measured as shown with the somewhat terse example above. These are descriptive fields only, as the measurement of attributes is done outside of this tool.

In practical terms, the measurement of attribute risk is done in association with the technology it supports, and an attribute will often support multiple technologies. The technology-oriented attribute risk is then used to calculate the overall attribute risk rating as an aggregate across all usage. This is the adjusted risk which takes into account teh maturity of the cybersecurity program processes. The adjusted risk is also shown as a risk level in the blue risk rating.

Attribute risk is used o calculate its parent control risk. A manual risk override value can be entered if there is reason for the risk used in control *Control,* risk calculations to be different from the calculated risk. The override field can also be used for attributes which are included but not associated with technology.

Risk Calculations

On the *Security Root* screen there is a panel which can be used to do a recalculation of the maturity and effectiveness of the cybersecurity program, and of all the risk levels. The logic is as follows.

- Calculate the Cybersecurity program maturity by taking the average weighted maturity value across all cybersecurity processes. Then use the factor table to select a *risk adjustment* factor.
- Update the *Technology* risk by aggregating (not averaging) all the individual technology attribute risk values. These are calculated as the base risk level for the technology attribute, factored by the percent impact it has on the technology, and then adjusted by the risk adjustment factor calculated above.
- Update the *Service* risk by aggregating (not averaging) all *Technology* risks associated with the *Service*.
- Update the business *Division* risk by averaging all service risks associated with the *Division*.
- Update the main *Attribute* risk as the average of all technology-related risks for that attribute.
- Update the *Control* risk as the average of all *Attribute* risks (taking into account either the calculated risk or, if one is present, the override risk).
- Update the Cybersecurity program control effectiveness by averaging all control risks across all divisions.

At this stage the capability maturity, i.e. the level to which the security process and its associated controls have been deployed, has not been factored into calculations. The intention is to use some form of risk reduction related to the maturity of the deployment (and hence the effectiveness of the control).

Maturity

The maturity calculation starts with the set of cybersecurity processes. At this stage, no calculations take account of capability maturity. Maturity calculations are based on the operational maturity of the cybersecurity processes.

Each process has an operational maturity level entered by the assessor together with a weight entered by the assessor. The maturity level is descriptive but represented internally as an index 0-5 which we denote *om*. The weight represents the relative importance of this process against other processes in the cybersecurity programme. We

denote the weight of the process *wm*. The overall maturity of the cybersecurity program denoted *maturity* is then calculated as

$$maturity = (\sum om * wm) / \sum wm$$

We assert that at a lower level of maturity, the risk of the controls provided by the process failing is increased, while at a higher level of security they are reduced. The extent of increase or reduction in risk is denoted *dm*. We then calculate the overall risk increase/reduction factor, the delta risk, is then denoted as *dr* which we calculate as

$$dr = maturity * dm$$

We will subsequently use *dr* to adjust our attribute-driven risk that we'll calculate next.

Effectiveness

Each technology attribute has an attribute risk calculation entered (the *base* risk) which is calculated external to the program as for any SABSA attribute risk calculation. This is denoted *br* and is adjusted based on the maturity-derived delta risk *dr*.

The technology attribute also has an impact rating set by the assessor which indicates the maximum impact a failure of the attribute could have on the technology should it fail entirely, the risk relevance, which we denote as *rr*. The overall risk to the technology *tr* is calculated as the sum of all attribute risk.

$$tr = \sum br * dr * rr$$

We don't take an average of the attribute risk, as each attribute contributes in its own right to the overall technology risk. The maximum technology risk is 100%.

A service consists of business processes supported by technology and people. For each technology used in the service we record the impact a loss of the technology would have on the service, which we denote as the delta technology risk *dt*. The overall risk to the service from its underlying technology, which we denote as *sr*, is simply the sum of all technology risk *tr* factored by *dt*.

$$sr = \sum tr * dt$$

The final calculation of cyber risk occurs at the Division level, and is the average of all service effectiveness managed by the Division. We denote this as group risk, *gr* and the number of services in the group are denoted by *ns*.

$$gr = (\sum sr)/ns$$

Attribute Risk

Different technologies may have their security requirements represented by the same attribute. We denote the number of instances of the attribute as *na*. In order to assess the overall risk of an attribute, which is shown on the attribute record and denoted *ar*, is the average of the per-technology attribute risk.

$$ar = (\sum br * dr * rr)/na$$

The attribute record allows for an assessor to enter a risk level, the risk override, which takes precedence over the calculated risk. The final risk value is then used to select a risk rating from the risk and effectiveness table below.

Control effectiveness

By assessing the level of risk associated with each attribute at the point of risk realization, the technology level, and then deriving overall attribute risk from that, we can reflect back to the control through which we delivered the security attribute the effectiveness of that control which we denote as *ce*. In other words, the control is as effective as the effectiveness of the attributes it delivers.

We provide an impact rating *ir* to allow for each attribute to contribute to a varying extent to the effectiveness of the control as determined by the assessor.

$$ce = 100 - \sum ar * ir$$

The calculation is then used to select the appropriate level of effectiveness from the risk and effectiveness table below.

Cybersecurity Effectiveness

The overall effectiveness of the cybersecurity program which we denote as *effectiveness* is determined by taking the average of the weighted control effectiveness. We denote the control overall performance weighting for effectiveness purposes as *cw*.

$$effectiveness = (\sum ce * cw)/\sum cw$$

Potential Cost due to Cyber Risk

A service is the point at which revenue occurs, and so each service has an assessed service value *sv*. Should an event occur which results in a data breach for this service, the cost of data breach is denoted by *bv*. We can calculate the potential cost of cyber risk, *sc*, as follows

$$sc = sr * (sv + bv)$$

Tables

The tables used to support calculations can be adjusted using the top level Security screen.

MATURITY	RISK ADJUSTMENT
Non-Existent	200%
Initial	200%
Informal	150%
Defined	100%
Managed	75%
Optimized	50%

EFFECTIVENESS	RISK LEVEL	RISK %
Extremely Effective	Very Low	0-14%
Highly effective	Low	15-24%
Effective	Moderate	25-49%
Mostly Effective	High	50-84%
Partly effective	Very High	85-100%