# Using Assessment Type: Control Specification

The Control Specification assessment type allows you to quantify the effectiveness of your controls, so you can show that there are benefits to them or improvements to be made.

On this page

* [Task 1 (Optional): Complete the General Information section](#Xbde82ba75392f3eb3fce2a3e0258975d69fa8aa)
* [Task 2: Add initiation categories and controls](#Task2Addinitiationcategoriesandcontrols)
* [Task 3: Add consequences](#Task3Addconsequences)
* [Task 4: Review the quantified metrics](#Task4Reviewthequantifiedmetrics)

## Task 1 (Optional): Complete the General Information section

In the General Information section, do the following:

1. Provide a description of the risk event.
2. If you don't want the risk event to be included in aggregations, select Exclude from aggregations.

* **Note:** The Status field is based on two factors: whether required data (Risk, Risk Event Name, Consequence Instances, Driver Instances) is present in the Risk Event record in Archer and whether you have completed filling out this form. If either is incomplete, or if you selected "Exclude from aggregations", the status is Exclude, meaning that the risk event will not be aggregated.

## Task 2: Add initiation categories and controls

In the Initiation Categories (Drivers) section, do the following:

1. Click Add button.
2. Enter an initiation category and inherent rate.
   * An initiation category is a category of risk event occurrences based on the controls that, if successful, would have prevented occurrence of the risk event. For example, if your Risk Event is a DDoS attack, you might have "Spyware", "Malware", and "Botnet Attack" initiation categories.
   * The inherent rate is how many times a year, on average, you think this initiation category will occur, given no controls in place.

* Insight calculates the Proportion, Full, and Actual fields. The Proportion is a percentage based on the inherent rate of the initiation category divided by the sum of the inherent rates for all categories. The Full and Actual fields are set to the Inherent rate until you add controls.

1. Add preventive controls. These are the individual controls in this category that would prevent the risk event from occurring. For example, in a "Botnet Attack" initiation category, you might have "DR Plan", "Patching", and "DNS Firewall" controls.

* You can either create new preventive controls or lookup existing controls from Archer. New controls are created in Archer when you save the assessment form.
  + To create new preventive controls, do the following: Click Add New Preventive Control. Enter a name, procedure ID, type, and probability of success, and click Add. The procedure ID is required in Archer. You can enter any text, but you may want to follow a numbering convention if you have one. The probability of success is how likely the control is to prevent the risk event from occurring. Enter a decimal between 0 and 1, but not including 1.
  + To lookup existing preventive controls from Archer, do the following: Click Add Existing Preventive Control. Select the control, enter a probability of success, and click Add. Only control procedures with a Control Goal of "Preventive" are displayed. The probability of success is how likely the control is to prevent the risk event from occurring. Enter a decimal between 0 and 1, but not including 1.
* Insight calculates the Lifecycle, Compliance, and Actual fields. For new controls, the Lifecycle and Compliance fields are set to "Proposed" and "Open". For existing controls, both are pulled from Archer. The Actual Probability of Success is calculated based on the control compliance and lifecycle multiplier.
* The Value of Preventive Control fields are populated once you define consequences.

## Task 3: Add consequences

1. In the Consequences section, click Add button.
2. Enter a name, select a type, and click Add.
   * The following consequence types are economic: Financial
   * The following consequence types are non-economic: Environmental, Health & Safety, Reputation, Social, and Sustainability
3. Do one of the following:
   * For economic consequences, enter the inherent minimum, median, and downside impacts in dollars.
     + The minimum impact is an absolute least possible impact, often representing fixed unavoidable costs.
     + The median impact is the mid-point of the distribution in the sense that it is equally likely for the impact to be less than or greater than the median.
     + The downside impact is only exceeded 10% of the time. It is not a worst case.
   * Insight uses the values you provide to model a range of potential impacts that could happen when a risk event occurs. Use the menu to view one of the following figures:
     + **Loss Per Occurrence** shows the economic loss incurred by a single occurrence of the risk event. The figure shows the probability density function (pdf) of this uncertainty, which indicates the range over which the loss is more or less likely to fall.
     + **Actual Annual Loss** takes account of both the number of occurrences and the loss incurred on each occurrence, given current controls and mitigations in place.
     + **Inherent Annual Loss** takes account of both the number of occurrences and the loss incurred on each occurrence, without considering current controls and mitigations in place.
     + **Full Annual Loss** takes account of both the number of occurrences and the loss incurred on each occurrence, assuming current controls and mitigations in place are fully effective.
     + For all annual loss figures:
       - The annual loss is zero if there are no occurrences. The uncertainty range of non-zero losses is slightly broader than for a single loss because of the possibility of multiple occurrences.
       - The figure shows a cumulative distribution curve, which indicates the probability that the loss is the horizontal value or less. The curve starts at the probability of no occurrence (and thus no loss).
       - The figure also shows the density function for non-zero loss for one or more occurrences of the risk. This indicates the range over which a loss is more or less likely to fall, when there is a loss at all.
     + You can click any of the legend items to hide them from the figures.
   * Insight also calculates the expected annual loss, value at risk, and the conditional value at risk, which are displayed under the figures. The value at risk and conditional value at risk percentages are what you defined in [Set Up Insight UI Settings](insight_uc_setting_up.htm#Set2).
   * For non-economic consequences, enter the inherent minimum, most likely, and maximum impact levels as a utility scale. Click the ? icon to view descriptions of what type of impact qualifies for each level based on the selected impact type.
     + The minimum impact level is the smallest possible impact.
     + The most likely impact level is the most likely possible impact.
     + The maximum impact level is the largest possible impact.
   * Insight uses the values you provide to model a range of potential impacts that could happen when a risk event occurs. You can hover over any point in the probability distribution to see the probability for a specific impact level.
4. Add mitigating controls. These are the individual controls that can decrease the impact of the consequence when the risk occurs.

* You can either create new mitigating controls or lookup existing controls from Archer. New controls are created in Archer when you save the assessment form.
  + To create new mitigating controls, do the following:
    1. Click Add New Mitigating Control.
    2. Enter a name, procedure ID, type, and probability of success, and click Add.
       - The procedure ID is required in Archer. You can enter any text, but you may want to follow a numbering convention if you have one.
       - The probability of success is how likely the control is to prevent the risk event from occurring. Enter a decimal between 0 and 1, but not including 1.
  + To lookup existing mitigating controls from Archer, do the following:
    1. Click Add Existing Mitigating Control.
    2. Select the control, enter a probability of success and a reduction factor, and click Add.
       - Only control procedures with a Control Goal of "Mitigating" are displayed.
       - The probability of success is, if the risk event occurs, how likely it is that this mitigating control reduces the impact of the consequence. Enter a decimal between 0 and 1, but not including 1.
       - The reduction factor is the reduction in impact (either a percentage for financial consequences or number of utility levels for non-financial) due to the mitigating control.
  + Insight calculates the Lifecycle, Compliance, and Actual fields. For new mitigating controls, the Lifecycle and Compliance fields are set to "Proposed" and "Open". For existing controls, both are pulled from Archer. The Actual Probability of Success is calculated based on the control compliance and lifecycle multiplier. The Value of Mitigating Control fields are this control's contribution to reducing the impact of the related consequences.

1. Repeat steps 1 - 5 for each consequence.

## Task 4: Review the quantified metrics

As you enter risk and consequence information, the values in the Quantified Metrics panel automatically update. When you're using the Control Specification assessment type, you get actual, inherent, and full values.

| Value | Description |
| --- | --- |
| Rate | The expected number of times a risk event occurs annually. |
| *Economic section* | |
| Expected loss per occurrence | If the risk occurs once, the expected impact based on all financial consequences.  For example, say you have two financial consequences. Financial Consequence 1 has a expected loss of $700,000, Financial Consequence 2 has an expected loss of $300,000. Your economic impact per occurrence would be $1m. |
| Expected annual loss | Annual expected impact of financial consequences based on the number of expected occurrences of the risk event annually.  Continuing with the previous example, your economic impact per occurrence is $1m, but your number of occurrences is 2, so your annual economic impact would be $2m. |
| Value at risk at *n%* | The value at risk is effectively the best outcome of the worst n% of occurrences.  The percentage is what you defined in [Set Up Insight UI Settings](insight_uc_setting_up.htm#Set2) |
| Conditional value at risk at *n%* | The conditional value is the average of the worst n% of occurrences.  The percentage is what you defined in [Set Up Insight UI Settings.](insight_uc_setting_up.htm#Set2) |
| *Total section* | |
| Expected impact per occurrence | If the risk occurs, the expected impact based on all consequences (financial and non-financial).  The economic equivalent for each consequence is totaled and then converted to the [utility scale](insight_uc_setting_up.htm#Populate).  Continuing with the previous examples, say you also have 1 reputational consequence, and 1 environmental consequence. Reputational Consequence has an expected economic equivalent loss of $400,000 and Environmental Consequence has a economic equivalent loss of $200,000.  Also, say your [global variables](insight_uc_setting_up.htm#Task1) are the following:   * # of levels 6 * Level 1 = 1,000 * Level 6 = 100,000,000   This gives you a level ratio of 10. Each level is 10 times the previous one:   1. 1,000 2. 10,000 3. 100,000 4. 1,000,000 5. 10,000000 6. 100,000,000   Given this, to get your total impact per occurrence, all of the economic equivalents are added (700,000 + 300,000 + 400,000 + 200,000 = $1.6m) and converted to the utility scale.  The utility scale conversion is (1 + LN(value/Level1)/LN(LevelRatio), so in this example you would have 1 + LN(1.6M/1,000)/LN(10), which gives you a utility scale value of 4.2  **Note:** You will not see the economic equivalent of any single consequence in the assessment. |
| Expected annual impact | If the risk occurs, the expected impact based on all consequences (financial and non-financial) and the rate of occurrence.  The financial equivalent for each consequence is totaled and then converted to the [utility scale](insight_uc_setting_up.htm#Populate).  Finishing the example above, the annual total impact would be 4.5. The total impact per occurrence (in economic equivalents): $1.6m, multiplied by the number of occurrences: 2 = $3.2m, converted to the utility scale: 1 + LN(3.2M/1,000)/LN(10). |