EX.4 Risk treatment results

EX.4.1 A risk treatment plan (template)

EX.4.1.1 Template

Risk treatment plan R« [RTP1] event number »

[« [RTP2] event name »]

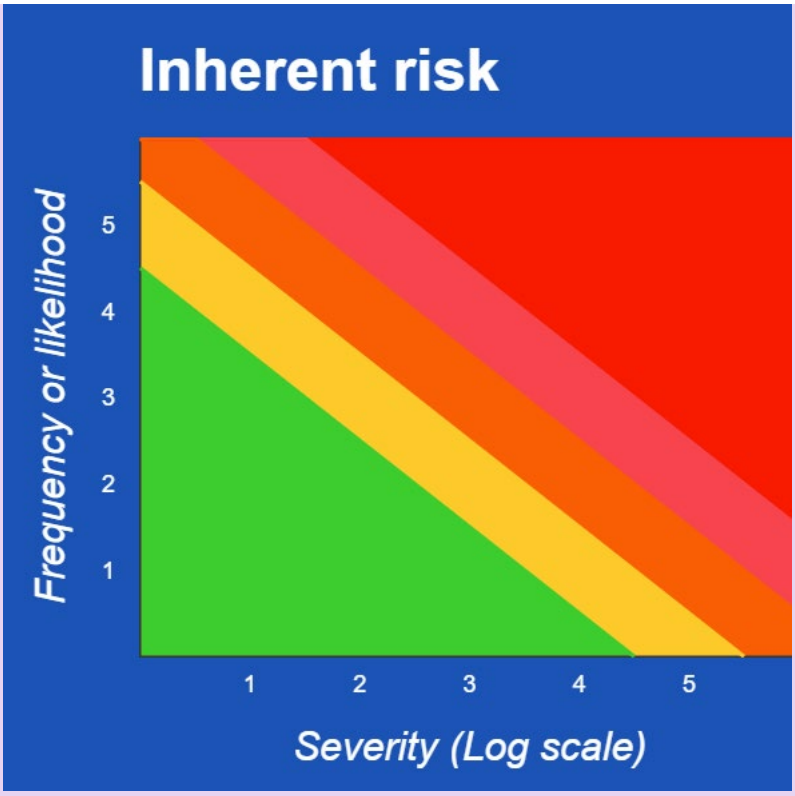
Event description

« [RTP3] Event description »

Risks before treatment

Likelihood	Consequence	Severity	Risk
« [RTP4] Copy data from risk assessment results to here »	C[1]	« [RTP4] Copy data from risk assessment results to here »	« [RTP4] Insert the sum of likelihood and severity here »
	I[1]	« Ditto »	« Ditto »
	A[1]	« Ditto »	« Ditto »

(1) Delete row if consequence does not apply to this event



« [RTP4] Copy the graph too »

Risk treatment plan

Preventing the event

« [RTP5] List or storyboard necessary preventive control statements from Appendix B for this event, customised as appropriate, see Chapter 3 »

Detecting the event

« [RTP6] List or storyboard necessary detective control statements from Appendix B for this event, customised as appropriate, see Chapter 3 »

Reacting to the consequences (2)

(2) *Just say "Reacting to the consequence" if this event has only one consequence*

Undesirable disclosure of information

« [RTP7a] List or storyboard necessary reactive control statements for confidentiality from Appendix B for this event, customised as appropriate, see Chapter 3 »

Loss of integrity

« [RTP7b] List or storyboard necessary reactive control statements for integrity from Appendix B for this event, customised as appropriate, see Chapter 3 »

Inability to carry some or all of one's business

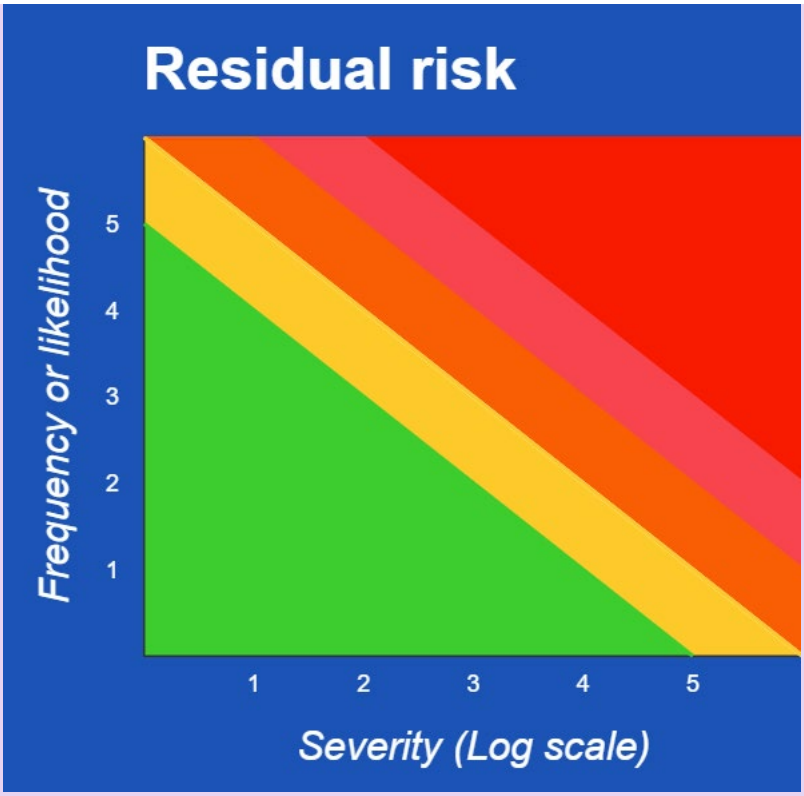
« [RTP7c] List or storyboard necessary reactive control statements for availability from Appendix B for this event, customised as appropriate, see Chapter 3 »

Risks after treatment

Likelihood	Consequence	Severity	Risk
« [RTP8a] Insert new likelihood value following application of effectiveness data from table below[3]»	C[4]	« [RTP8b] Insert calculated value[3] »	« [RTP8c] Insert calculated value[3] »
	I[4]	« Ditto »	« Ditto »
	A[4]	« Ditto »	« Ditto »

(3) See Chapter 3 for instructions on how to do this

(4) Delete row if consequence does not apply to this event



« [RTP9] Add explanatory text as necessary »

Approval

« [RTP10] Say when this plan was approved and provide a reference to evidence of that approval. »

Previous plans

« [RTP11] Either say that this is the first approved plan, or when and why it was revised, together with a reference to previous plans. »

Effectiveness of risk treatment

The following data have been used to estimate the residual risk:

Treatment pair	Control behaviour	Risk modification parameters	
Preventive and detective controls	« [RTP12a] N-factor/ strangulation/excess[6] »	FoL modification: « [RTP12b] Insert value[7] »	Limit: « [RTP12c] Insert value[8] »
Reactive controls for: Undesirable disclosure of information[5]	« Ditto »	Sev modification: « Ditto »	Limit: « Ditto »
Reactive controls for: Loss of integrity[5]	« Ditto »	Sev modification: « Ditto »	Limit: « Ditto »
Reactive controls for: Inability to carry out some or all of one's business[5]	« Ditto »	Sev modification: « Ditto »	Limit: « Ditto »

(5) *Delete row if consequence does not apply to this event*

(6) *Delete as appropriate*

(7) *Content of cell only applies if N-factor or strangulation*

(8) *Content of cell only applies if excess or strangulation*

« Add explanatory text as necessary »

EX.4.1.2 Example using listed necessary controls

Risk treatment plan R« [RTP1] number of plan »

[« [RTP2] event name »]

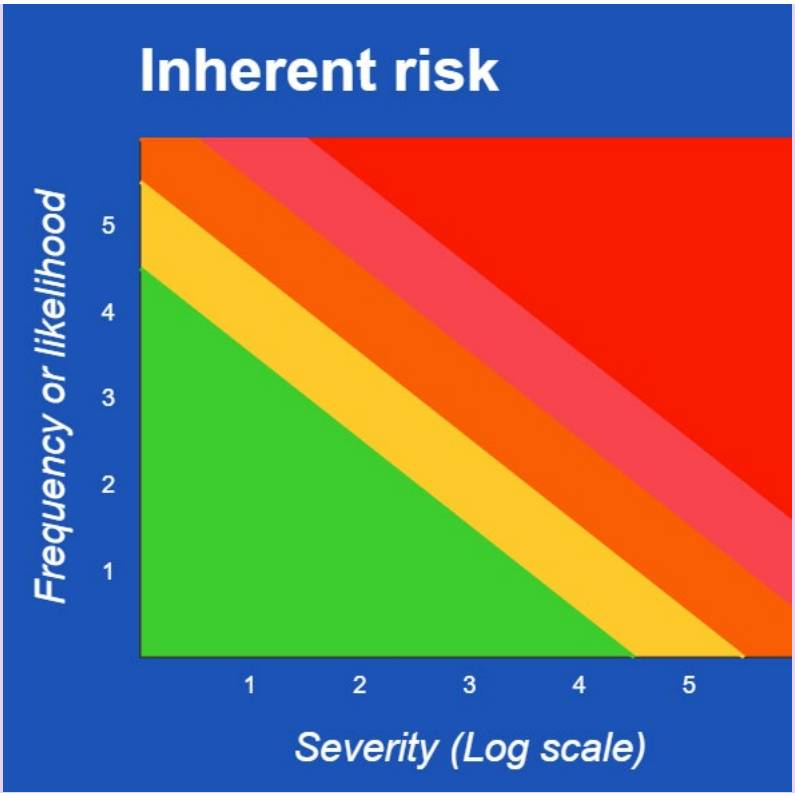
Event description

« [RTP3] Event description »

Risks before treatment

Likelihood	Consequence	Severity	Risk
« [RTP4] Copy data from risk assessment results to here »	C[1]	« [RTP4] Copy data from risk assessment results to here »	« [RTP4] Insert the sum of likelihood and severity here »
	I[1]	« Ditto »	« Ditto »
	A[1]	« Ditto »	« Ditto »

(1) Delete row if consequence does not apply to this event



Copy the graph too

Risk treatment plan

Preventing the event

« List or storyboard necessary preventive control statements from Appendix B for this event, customised as appropriate, see Chapter 3 »

Detecting the event

« List or storyboard necessary detective control statements from Appendix B for this event, customised as appropriate, see Chapter 3 »

Reacting to the consequences [2]

[2] Just say “Reacting to the consequence” if this event has only one consequence

Undesirable disclosure of information

« List or storyboard necessary reactive control statements for confidentiality from Appendix B for this event, customised as appropriate, see Chapter 3 »

Loss of integrity

« List or storyboard necessary reactive control statements for integrity from Appendix B for this event, customised as appropriate, see Chapter 3 »

Inability to carry some or all of one’s business

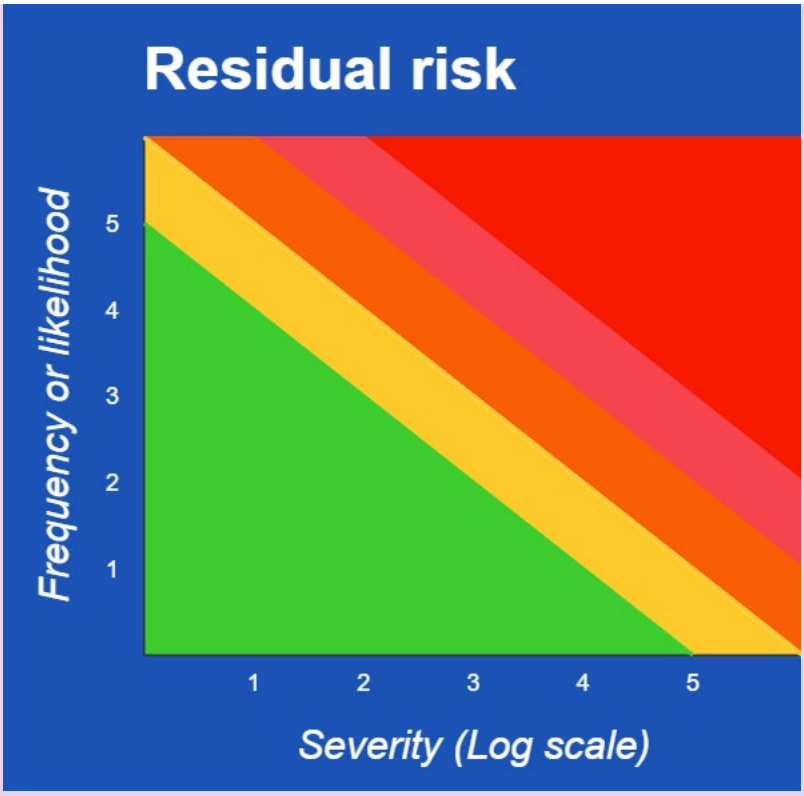
« List or storyboard necessary reactive control statements for availability from Appendix B for this event, customised as appropriate, see Chapter 3 »

Risks after treatment

Likelihood	Consequence	Severity	Risk
« Insert new likelihood value following application of effectiveness data from table below[3]»	C[4]	« Insert calculated value[3] »	« Insert calculated value[3] »
	I[4]	« Ditto »	« Ditto »
	A[4]	« Ditto »	« Ditto »

[3] *See Chapter 3 for instructions on how to do this*

[4] *Delete row if consequence does not apply to this event*



« Add explanatory text as necessary »

Approval

« Say when this plan was approved and provide a reference to evidence of that approval. »

Previous plans

« Either say that this is the first approved plan, or when and why it was revised, together with a reference to previous plans. »

Effectiveness of risk treatment

The following data have been used to estimate the residual risk:

Treatment pair	Control behaviour	Risk modification parameters	
Preventive and detective controls	« N-factor/ strangulation/excess[6] »	FoL modification: « Insert value[7] »	Limit: « Insert value[8] »
Reactive controls for: Undesirable disclosure of information[5]	« Ditto »	Sev modification: « Ditto »	Limit: « Ditto »
Reactive controls for: Loss of integrity[5]	« Ditto »	Sev modification: « Ditto »	Limit: « Ditto »
Reactive controls for: Inability to carry out some or all of one's business[5]	« Ditto »	Sev modification: « Ditto »	Limit: « Ditto »

[5] *Delete row if consequence does not apply to this event*

[6] *Delete as appropriate*

[7] *Content of cell only applies if N-factor or strangulation*

[8] *Content of cell only applies if excess or strangulation*

« Add explanatory text as necessary »

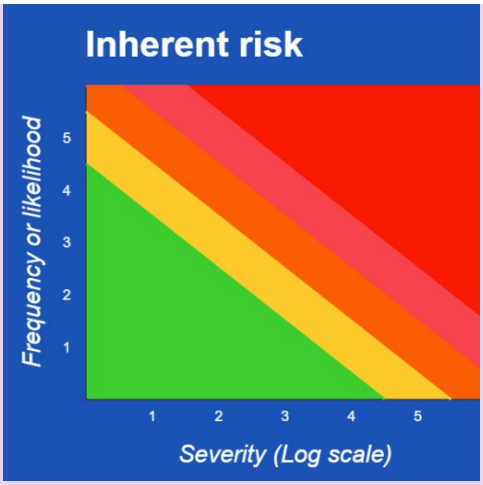
EX.4.1.3 Example stories

Example stories are given in Appendix B.

EX.4.1.4 Summary of results

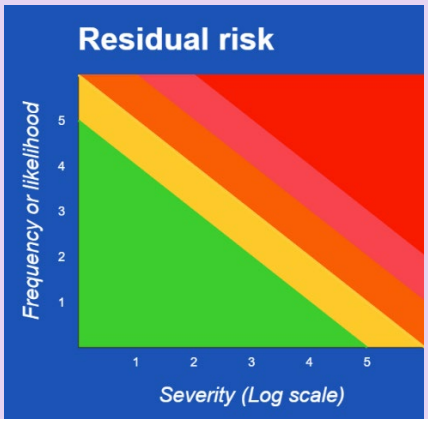
Organisations may wish to produce a summary of all risk treatment results to show how the overall inherent risk is modified.

Risks before treatment



There are 12 risk treatment plans:

- R1 – Fraud or error
- R2 – Poor stewardship of information
- R3 – Successful cyberattack
- R4 – Office/data centre break-in
- R5 – Theft/loss of mobile devices
- R6 – Software failure
- R7 – Hardware and environmental failure
- R8 – Internet/communications failure
- R9 – Acts of God, vandals and terrorists



EX.4.3 Statement of Applicability

EX.4.3.1 Traditional layout (extract)

In this example, a table is used for each of the 35 sub-headings in ISO/IEC 27001, Annex A. In the table shown below, each row exemplifies how to present:

a) a necessary control whose specification is identical to that given in ISO/IEC 27001, Annex A;
b) a necessary control whose specification is a variation of that given in ISO/IEC 27001, Annex A;
c) a custom control, i.e., a necessary control that is not in ISO/IEC 27001, Annex A;
d) an Annex A control that is obviated by a custom control; and
e) an Annex A control that is excluded for some other reason.

Id	Name	Specification	Necessary/excluded	Type	Reason for inclusion or exclusion	Status
A.n.m.1	« Control name[1] »	« Control specification[1] »	Necessary control		« References to RTPs which use this control[2]»	« Implemen
A.n.m.2	« Control name[1] »	« Modified control specification[3] »	Control variation		« References to RTPs which use this control[2]»	« Implementation status[2]»
« Custom identifier[2] »	« Custom name[2] »	« Control specification[2] »	Custom control		« References to RTPs which use this control[2]»	« Implement
A.n.m.3	« Control name[1] »	« Control specification[1] »	Obviated		« Reason for obviation and reference to the custom control that is performing the obviation»	Not applicable
A.n.m.4	« Control name[1] »	« Control specification[1] »	Excluded		« Reason for non-applicability»	Not applica

(1) *Copied without alteration from ISO/IEC 27001, Annex A*

(2) *See Chapter 4*

(3) *The Annex A control specification has been struck through to show that this is not an organisational requirement in this case. The organisational control requirement in in the attribute cell*

EX.4.3.2 Modern layout

In this example, five tables would be used one for each of the four control pillars: organisational, people, physical and technological, and a fifth for excluded Annex A controls. The example presents an extract from the technological table. Appendix C presents the questions together with their reference control identifiers. Control specifications are created by:

1. ignoring questions with 'No' answers
2. replacing questions with 'Similar' answers with your replacement question to which the answer is 'Yes'
3. combining the question text for questions with 'Yes' answers and replacement questions associated with the same reference control identifier
4. replacing the resultant text for each reference control identifier with its statement form (e.g., "Do you subscribe…?" becomes "We subscribe…".

Copy the Annex A references exactly as given in Appendix C. If the entry is blank, the control entry is a custom control. If the entry is of the form *A.x.y.z**, it is a variant of Annex A control *A.x.y.z*, otherwise it corresponds directly to Annex A control *A.x.y.z*.

4 Technological controls

Id	Name	Specification	Events	PDR [1, 4]	CIA [1, 4]	Status	Annex A
« Reference control identifier[1] »	« Control name[2] »	« Control specification[3] »	« References to RTPs which use this control[1]»			« Implementation status»	Annex A control map: « List of associated Annex A controls or blank[1]»

Excluded Annex A controls

Control	Rationale
A.n.m.4 « Control name[5] »	« Reason for exclusion»

(1) Copied from Appendix C, customised as used in an RTP, see Chapter 4.

(2) Invent a suitable name

(3) See text above for creating specifications from questions

(4) Optional, see Chapter 4

(5) Copied without alteration from ISO/IEC 27001, Annex A