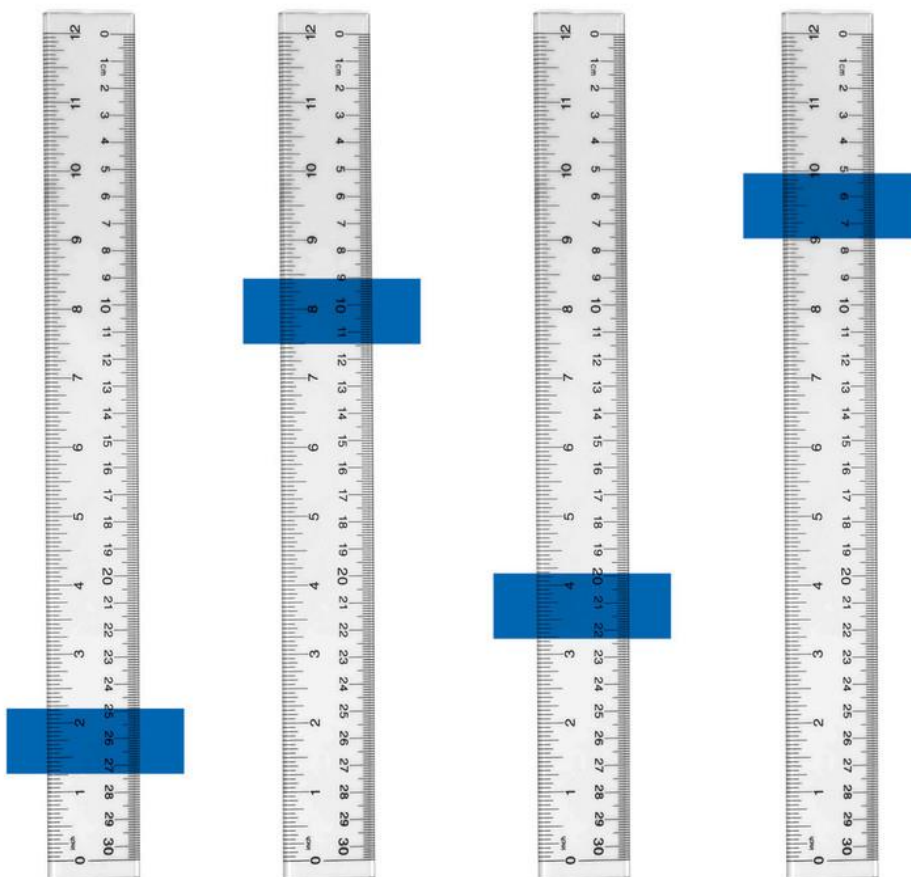


EXAMPLE

Global Compliance Solutions Risk & Compliance Health Check

REPORT

[DATE]



EXAMPLE

Contents:

Area	Page
Executive summary	3
Understanding the background	4
Risk calculations	5
Dashboard results	7
Gaps, risks and recommendations	9
Appendix	11

EXAMPLE

1. **Executive Summary**

FREE TEXT – specific to survey results, highlighting high risk areas.

EXAMPLE

2. **Understanding the background (THESE ARE WRITTEN FOR ALL AREAS AND WILL BE SPECIFIC FOR EACH AREA)**

“Modern slavery” is a term used to encompass slavery, servitude, forced and compulsory labour, bonded and child labour and human trafficking. Victims are coerced, deceived and forced against their free will into providing work or services. Modern slavery is a crime and a violation of fundamental human rights.

Human trafficking is where a person arranges or facilitates the travel of another person with a view to that person being exploited.

The Modern Slavery Act aims to prevent modern slavery, protect victims and sets out a range of serious criminal offences and penalties, including imprisonment. The Act requires organisations that are in scope to publish an annual statement explaining what they have done during the previous financial year to ensure that modern slavery is not occurring in their (i) own organisation and (ii) supply chains.

The Act is not prescriptive but provides a list of information that “may” be included in the statement:

- the organisation’s structure, its business and its supply chains;
- its policies in relation to slavery and human trafficking;
- its due diligence processes in relation to slavery and human trafficking in its business and supply chains;
- the parts of its business and supply chains where there is a risk of slavery and human trafficking taking place, and the steps it has taken to assess and manage that risk;
- its effectiveness in ensuring that slavery and human trafficking is not taking place in its business or supply chains, measured against such performance indicators as it considers appropriate; and
- the training about slavery and human trafficking available to its staff.

Where a company fails in its obligation to publish a statement under the Act, an injunction can be issued by the UK Secretary of State to enforce the duty to prepare a statement. There are no fines or penalties that can directly be issued under the Act in relation to a non-compliant public statement. There is no provision under the Act for a private right of action.

However, NGOs, unions and other pressure groups will monitor reporting under the Act. A failure to report fully or the discovery in a supply chain of modern slavery contradicting a statement is likely to cause reputational and brand damage.

Whilst the statement required under the Act is not a financial statement for the purposes of the UK Companies Act 2006, potentially it could amount to a false or misleading statement made for the purpose of inducing a person to invest or to hold onto their investment.

In the US, consumer actions have been filed against companies for knowingly making false statements when making disclosures about the steps taken to prevent the use of slave labour in their supply chains.

EXAMPLE

3. Risk Calculations

Eversheds Sutherland utilise a 5x5 Risk Matrix to identify levels/severities of risk. This is calculated by considering the category of probability or 'likelihood' on a scale of 0-5, against the consequence or 'impact' of the risk on a scale of 0-5. This type of risk matrix allows each business risk to be scored on a 0-25 scale of severity and ensures that risk is measured in a consistent format across the assessment scope.

A full overview of each risk scoring and associated severity can be found below:

		OVERALL IMPACT SCORING				
		1	2	3	4	5
L I K E L I H O O D	5	MEDIUM 5	HIGH 10	HIGH 15	CRITICAL 20	CRITICAL 25
	4	MEDIUM 4	MEDIUM 8	HIGH 12	HIGH 16	CRITICAL 20
	3	LOW 3	MEDIUM 6	MEDIUM 9	HIGH 12	CRITICAL 15
	2	LOW 2	MEDIUM 4	MEDIUM 6	HIGH 8	HIGH 10
	1	LOW 1	LOW 2	MEDIUM 3	MEDIUM 4	HIGH 5

Risk Impact Areas

Each organisational risk used within the assessment scope has been assigned impact scoring using an index of 5 impact areas. An overview of the impact areas used within this assessment and the associated scoring definitions can be found below:

- Asset or Financial Loss**

Used to measure the financial loss to the organisation if the risk was to occur.

1 - Negligible	2 - Minor	3 - Moderate	4 - Significant	5 - Acute
No or insignificant impact to revenue stream, loss or assets. No or insignificant financial penalties applied.	Impact to revenue stream or assets easily absorbed. Financial penalties noticeable but not going to cause undue duress to the business.	Impact to revenue stream or assets may impact other business areas or key processes. Financial penalties may cause damage.	Impact to revenue stream or assets causes significant impact to other business areas or key processes. Financial penalties cause significant damage.	Impact to revenue stream or assets causes acute damage throughout the organisation. Financial penalties or sanctions severely hinder the business.

- Continuation of Services**

The impact to the ongoing operation and services provided by the organisation.

1 - Negligible	2 - Minor	3 - Moderate	4 - Significant	5 - Acute
Minimal impact to availability or continuity of supporting systems or processes.	Minor impact to availability or continuity of supporting systems/processes which can be rectified.	Impact to availability or continuity of supporting systems/processes which cannot be rectified. Impact to limited environment.	Significant impact to availability or continuity which cannot be rectified. Impacts the wider community and/or public facing systems.	Severe impact to availability or continuity which cannot be rectified. Impacts a vast majority of services or processes within the business.

EXAMPLE

- Quality of the Services**

What would be the impact on the product and/or service provided by the organisation.

1 - Negligible	2 - Minor	3 - Moderate	4 - Significant	5 - Acute
Minimal impact to the quality of services provided by the business or third parties operating on the behalf of the business.	Quality of services is perceived to be reduced by a small number of clients or third parties. Limited processes are affected.	Quality of services is perceived to be partially reduced by a large number of clients or third parties. May extend to a wider number of processes.	Quality of services is perceived to be significantly reduced by most clients or third parties. Either a specific service process is severely affected or a wider number to a lesser degree.	Severe impact to a majority of services provided by the business or third parties operating on the behalf of the business. A vast majority of clients or third parties affected.

- Health & Safety**

Is there an impact to the health and safety of the staff, client, third party, or public

1 - Negligible	2 - Minor	3 - Moderate	4 - Significant	5 - Acute
Minimal impact to health or potential for injury.	Minor, short term impact to health or potential injury which does not result in work absence.	Non-permanent impact to health or potential injury which results in temporary work absence.	Potentially permanent impact to health or injury which can result in permanent work absence.	Potential loss of life or permanent disability.

- Reputation**

Used to define the reputational damage to the organisation, or brand of the organisation.

1 - Negligible	2 - Minor	3 - Moderate	4 - Significant	5 - Acute
Minimal detrimental impact to the reputation of the business. No impact to relations with third parties.	Minor impact to the reputation of the business within a smaller community or focus area.	Detrimental impact to a wider community or region. Impact to relations with clients or third parties.	Detrimental impact on a national scale resulting in wide scale loss of confidence.	Severe detrimental impact on a national or international scale. Widespread loss of confidence with the the business brand.

Risk Likelihood Scorings

In addition to measuring the impact of organisational risks, Eversheds Sutherland utilise a 'likelihood' score to determine the possibility of the risk occurring based on the current controls or scenario of the organisation. This is also measured on a 0-5 scale.

Definitions of how these values have been assigned to organisational scenarios are detailed below:

Likelihood score	Descriptor	Frequency How often might it/does it happen
1	Rare	This will probably never happen/ recur
2	Unlikely	Do not expect it to happen/ recur but it is possible it may do so
3	Possible	Might happen/ recur occasionally
4	Likely	Will probably happen/recur but it is not a persisting issue/ instances
5	Almost certain	Will undoubtedly happen/recur, possibly frequently

EXAMPLE

4. Dashboard Results

The following reporting has been created using the risk data generated across the entire assessment scope. Creating reports at this level enables Eversheds Sutherland to make observations at an organisational level, understanding key areas within the business where remediation efforts should be prioritised or where commonalities of risk can be addressed.

Assessment Scope Averages

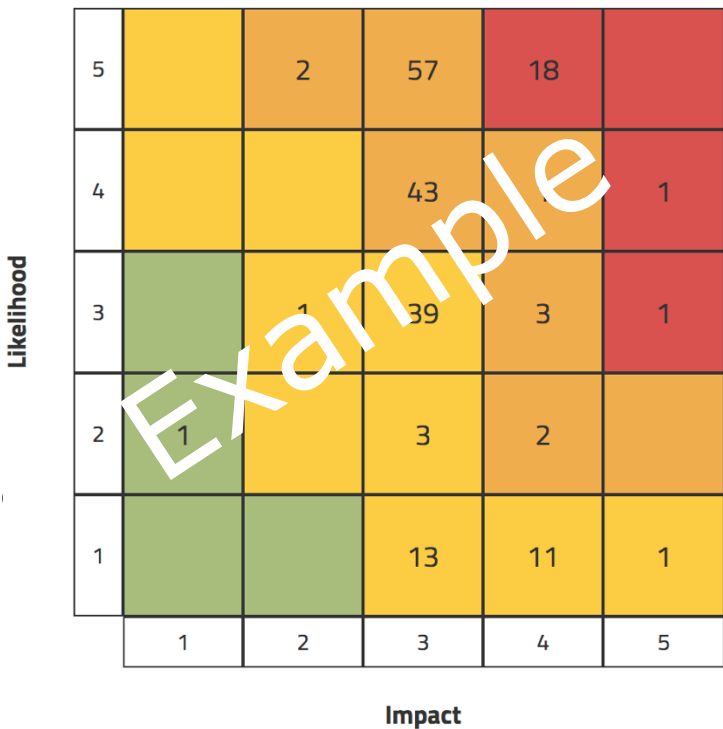
The data below summarises the average risk score, likelihood, and overall impact across the entirety of the assessment scope. As detailed within the above 'Risk Calculations' section, Average Risk Score is measured on a 0-25 scale, and Average Likelihood and Impact are each measured on a 0-5 scale.



[Summary Text] The average risk score of the organisation is currently determined as 11.52, which is a **High Severity** rating. An average likelihood score of 3.84 indicates that controls to mitigate the organisational risks are consistently insufficient, triggering at a near 'Likely' occurrence of the risk occurring or being exposed.

Risk Heatmap

The Risk Heatmap shows where the highest number of individual risks features within the Likelihood vs Impact Risk Matrix. Organisations should prioritise addressing risks present within the upper right area of the heatmap, as this indicates where the highest impact organisational risks also have the highest likelihood of occurring.



[Summary Text] A total of 20 risks have been identified as 'Critical' to the business. There are 18 risks with an impact rating of 4, which have been issued with an 'Almost Certain' likelihood of occurring.

There are also an additional 2 risks with an Impact Rating of 5, which have 'Likely' and 'Possible' chance of occurring.

EXAMPLE

Organisational Summary

The organisational unit summary details the number of risks, total risk score, and average risk score across the assessment scope.

Name	Number of risks	Total risk score	Average risk score
Acme Inc	121	1416	12
ACME Third Party	55	656	12
Third Party 6	18	212	12
Third Party 2		15	15
Third Party 3	1	12	12
Third Party 4	1	8	8

Providing this data in order of risk score, provides the organisation with key organisation units where remediation efforts should be prioritised. It should also be noted that where a small number of risks are shown associated to a business unit, and a high average or total risk score is present, there is likely to be a high-risk score associated to individual risks which could be 'quick wins' for remediation exercises.

[Summary Text] Acme Inc is responsible for a significantly higher number of risks across the assessment scope. An average risk score of 12 indicates that these may be commonly 'High' severity and that there is considerable work to be done in resolving risks and reducing these down to a level which is viewed as 'Acceptable' by the organisation.

Risk Commonalities

Identifying commonalities of risk across the assessment scope can provide huge value in reducing risk across a larger scale. Targeted awareness/educational packs of information that can easily be distributed to all organisational units can help business units reduce risk internally while external remediation efforts are focused on the 'high risk' organisational areas.

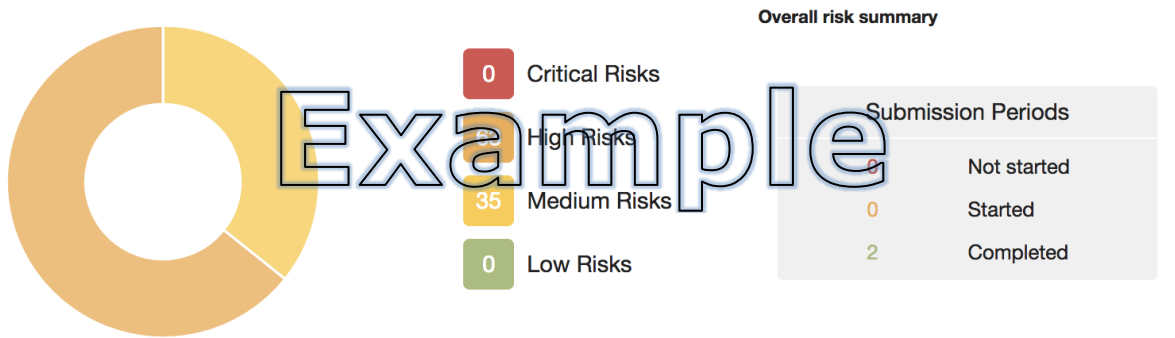
Name	Number of risks	Total risk score	Average risk score
ABMS - 2.1 - Adopting an anti-bribery policy and implementing the ABMS	23	213	9
ABMS - 2.2 - top management statement	1	12	12
Technical control capabilities to enforce tenant data retention	2	24	12
Formal cryptography policy	2	36	18
GDPR - Data controllers	2	28	14
GDPR - International	2	40	20
GDPR - DPO	2	24	12
GDPR - DP by Design and DPIAs	2	28	14

[Summary Text] Anti-Bribery and Modern Slavery risks were most commonly identified across 23 different business units, indicating an immaturity in processes/controls to mitigate this type of risk.

EXAMPLE

5. Assessment Risk Register

The below risk register is an export of all risks generated as a result of the assessment, organised by criticality. Each risk shown has a unique Risk ID for internal reference and to identify the risk details within the platform, the risk severity (including total score), the description of the risk and current organisational status, and the status of the risk. Tracking at what stage in the remediation workflow a risk is at.



Risk ID	Score	Risk Description	Risk Scenario	Risk Register	Status	
125	12 - High	No or Insufficiently Managed Information Security Policy Information Security	Selected options: Our Information Security policy is reviewed on at least an annual basis	Information Security Risk Register	Open	3
129	12 - High	No or Insufficient Consideration of Special Interest Groups Information Security	Selected options: We formally review our special interest groups on at least an annual basis	Information Security Risk Register	Open	0
136	9 - Medium	No or Insufficient Process for Constituents to Review and Accept Policies & Requirements Information Security	Selected options: Constituents are required to review Non-Disclosure or Confidentiality agreements on at least an annual basis	Information Security Risk Register	Open	0
137	15 - High	No or Insufficient Security Awareness Training Programmes Information Security	Selected options: None of the above	Information Security Risk Register	Open	0

EXAMPLE

141	9 - Medium	No or Insufficient Process to Manage Hardware/Software Assets Information Security	Selected options: Our inventory of hardware/software assets is owned by a specific resource or team	Information Security Risk Register	Open	0
142	3 - Medium	No or Insufficient Asset Management Programme Information Security	Yes, our Asset Management programme is reviewed on at least an annual basis	Information Security Risk Register	Open	0
143	9 - Medium	No or Insufficient Accountability for Information Assets Information Security	Selected options: Our assets handled by the business are reviewed and accounted for on at least an annual basis	Information Security Risk Register	Open	0
144	9 - Medium	No or Insufficient Acceptable Use Policy for the Use of Assets Information Security	Selected options: An Acceptable Use policy is in place and reviewed on at least an annual basis; An Acceptable Use policy is communicated to all relevant users	Information Security Risk Register	Open	0
145	9 - Medium	No or Insufficient Asset Return Policy Information Security	Selected options: Our Asset Return policy or procedure includes formal processes for changes, migrations and leavers to return assets	Information Security Risk Register	Open	0
146	9 - Medium	No or Insufficient Classification Policy Information Security	Selected options: An Information Classification policy is in place and reviewed on at least an annual basis; Our Information Classification policy is supported by processes for handling and transmission	Information Security Risk Register	Open	0
147	9 - Medium	No or Insufficient Security Labelling Process Information Security	Selected options: Our userbase is made aware of the Information Security Labelling process upon employment and on at least an annual basis; Conformity of our users against the Information Security Labelling process is audited on at least an annual basis	Information Security Risk Register	Open	0
148	6 - Medium	No or Insufficient Policy to Manage the Handling of Assets Information Security	Selected options: Access restrictions are in place for sensitive or critical assets; Authorised recipients of assets are documented	Information Security Risk Register	Open	0
153	12 - High	No or Insufficient Policy in Place to Manage Access Control Information Security	Selected options: Our Access Control policy is approved by senior management	Information Security Risk Register	Open	0
154	9 - Medium	No or Insufficient Controls to Manage and Monitor Remote Access Information Security	Selected options: Our organisation has remote access in use and is subject to two factor authentication for users connecting to systems or assets containing sensitive information	Information Security Risk Register	Open	0
155	6 - Medium	No or Insufficient Process to Manage Unique User ID's Information Security	Yes, unique IDs are used for all non-administrative functions (not auditable)	Information Security Risk Register	Open	0

EXAMPLE

Example Appendix

Provided responses to support the above assessment and risk data are found below:

No.	Answered by	Question	Answer
1	Emma Lawrence	If your organisation has an an Anti-Bribery policy in place, which of the following elements are included?	Our Anti-Bribery policy is reviewed on at least an annual basis
2	Emma Lawrence	If your organisation has a competent Compliance Manager (with access to top management) in place to implement the Anti-Bribery Management System (ABMS) and provide advice and guidance to staff relating to bribery, which of the following elements best describe this?	None of the above
3	Emma Lawrence	Have top management made a statement to staff, and in the public domain, to demonstrate its support for the Anti-Bribery policy?	The Executive Management Team have made a statement to staff The Executive Management Team have made a statement to the public domain
4	Emma Lawrence	Has education, training or guidance been provided to all staff associated with the Anti-Bribery policy in relation to avoiding bribery?	None of the above
5	Emma Lawrence	Have responsibilities for overseeing compliance with the Anti-Bribery policy on a day-to-day basis been established?	Day-to-day responsibilities have been defined Responsibilities are reviewed on at least an annual basis
6	Emma Lawrence	Are there established bribery risk assessment procedures?	Formal bribery risk assessment procedures have been documented Bribery risk assessment procedures are reviewed on at least an annual basis
7	Emma Lawrence	Is there evidence of risk assessment controls to reduce risks to an acceptable level?	Risk reduction over time is demonstrable Acceptable thresholds are defined
8	Emma Lawrence	If your organisation comprises of more than one independently managed component organisation, are there competent managers appointed in each component organisation to oversee compliance with the Anti-Bribery policy?	None of the above

Confidential and privileged

For more information, please contact:



Lee O'Connell MSc CIA
Consulting Director
ES/Consulting

t: +44 7789 005 320

e: leeoconnell@eversheds-sutherland.com

eversheds-sutherland.com

© Eversheds Sutherland (International) LLP 2018

Eversheds Sutherland (International) LLP is a limited liability partnership