INFORMATION TECHNOLOGY
RISK ASSESSMENT.COM

Information Technology Risk Assessment

Name:	Anthony	**Assessment Type:**	External Threat Assessment Only
E-mail:	anthony_quinn@me.com	**Assessment Name:**	Demo - Sample Report - External Threats - Company XYZ
Position/Title:	Director	**Date Started:**	02-Feb-2014 21:23
Telephone:	0431 221006	**Date Completed:**	02-Feb-2014 21:29
Company:	Company XYZ	**Period From:**	27-Feb-2014
Sector:	Banking and Finance	**Period To:**	28-Feb-2014

This is a sample of the IT Risk Assessment report

Disclaimer:

The contents contained within the Online Information Technology Risk Assessment Tool are provided for general information only and does not constitute the provision of professional advice.

The content of the risk assessment tool contains information that will assist organisations to assess their information technology risks and has been designed to inform areas of vulnerabilities that should be the focus of the Information Technology Programme.

Before any action or decision is taken on the basis of any materials the user should obtain appropriate independent professional advice. Links to other web sites are provided for the user's convenience and do not constitute endorsement of material at those sites, or any associated organisation, product or service.

Financial Crimes Consulting Pty Ltd accepts no responsibility or liability for any loss suffered as a result of reliance on the materials contained within this product.

The end user herein indemnifies Financial Crimes Consulting Pty Ltd and all associated business partners or companies against all loss, damages, claims, liability, expenses, payments or outgoings incurred by or awarded against the end user arising directly or indirectly from any third party, including but not limited to:

(i) The end users use of the Online Money Laundering and Terrorism Financing Risk Assessment Tool. For the avoidance of doubt, this means that if the end user is ever sued or the subject of criminal or civil penalties from other third parties and/or Information Technology or other regulators, including but not limited to fines or compensation that Financial Crimes Consulting Pty Ltd will be fully indemnified.

(ii) Any act or omission of Financial Crimes Consulting Pty Ltd (including any negligence, unlawful conduct or wilful conduct) by Financial Crimes Consulting Pty Ltd relating to this agreement or arising as a consequence of the performance or non-performance of the products or services, intellectual property infringement, breach of confidentiality, misleading and deceptive conduct or other legal liability).

(iii) Any action taken by international Information Technology or other regulatory bodies or third parties against the end users of the Online Information Technology Risk Assessment Tool, the end user indemnifies Financial Crimes Consulting Pty Ltd against any liability and indemnifies and protects Financial Crimes Consulting Pty Ltd against any liability as outlined in any Information Technology legislation.

End users that use our products are taken to have agreed to the above terms and conditions and indemnities outlined.

Overall - Inherent Risk Rating - Matrix

The Overall Inherent Risk Rating Matrix contains two dimensions - likelihood (meaning the likelihood of a risk occurring based on previous experiences) and the impact (meaning the impact that the risk would have, in terms of operational, risk, compliance, financial, reputation or other risk factors). The Overall Inherent Risk Rating Matrix simply plots the answers provided during the risk assessment into the appropriate cells in the matrix, to highlight the concentration of risks across the entire model. Organisations can use this to understand the number of inherent risk factors that exist within each of the dimensions and identify the areas which have the highest need for effective mitigating controls. If the concentration of risks appear in the top right, then it is recommended that the Organisation focuses efforts in these areas to implement mitigating controls which will have the effect of reducing overall risks.

Likelihood	Ratings	0 - Not Applicable	1 - Insignificant	2 - Low	3 - Moderate	4 - High	5 - Extreme
	5 - Guaranteed	Not Applicable 0	Medium Risk 0	High Risk 0	High Risk 0	Very High Risk 0	Extreme Risk 1
	4 - Very Likely	Not Applicable 0	Medium Risk 0	Medium Risk 0	High Risk 0	Very High Risk 2	Very High Risk 0
	3 - Likely	Not Applicable 0	Low Risk 0	Medium Risk 1	Medium Risk 2	High Risk 1	Very High Risk 2
	2 - Unlikely	Not Applicable 0	Low Risk 0	Low Risk 3	Medium Risk 4	High Risk 1	High Risk 1
	1 - Rare	Not Applicable 0	Low Risk 0	Low Risk 0	Low Risk 0	Medium Risk 0	High Risk 0
	0 - Not Applicable	Not Applicable 0	Not Applicable 0	Not Applicable 0	Not Applicable 0	Not Applicable 0	Not Applicable 0
		Impact					

Key

Likelihood

Score	Rating	Description
0	Not Applicable	The risk factor is not relevant to the inherent risk rating matrix
1	Rare	The risk event is very unlikely to occur but may occur on rare occurrences.
2	Unlikely	The risk event is unlikely to occur based on previous experiences.
3	Likely	The risk event may occur based on previous experiences.
4	Very Likely	The risk event is very likely to occur based on previous experiences.
5	Guaranteed	The risk event Is either guaranteed or almost certain to occur.

Impact

Score	Rating	Description
0	Not Applicable	The risk factor is not relevant to inherent risk rating matrix
1	Insignificant	The risk event would have very insignificant or no impact on the business.
2	Low	The risk event would have a low impact on the business.
3	Moderate	The risk event would have a moderate impact on the business.
4	High	The risk event would have a major impact on the business.
5	Extreme	The risk event would have a catastrophic effect on the business.

Overall Inherent Risk Rating

Score	Rating	Description
0	Not Applicable	The risk factor is not relevant to inherent risk rating matrix
1	Low Risk	No regulatory impact, no client or staff impact, no financial loss, no impact on targets
2	Medium Risk	Minor regulatory impact (i.e. updates to regulators), medium customer and staff impacts, moderate financial loss (i.e. hundreds of thousands), some effect on business operations (i.e. minor disruptions to service), significant amounts of negative press, business remains viable and sales targets impacted by >5%
3	High Risk	Moderate regulatory impact (i.e. close monitoring but no regulatory action for breaches), medium customer and staff impacts, moderate financial loss (i.e. hundreds of thousands), some effect on business operations (i.e. minor disruptions to service), significant amounts of negative press, business remains viable and sales targets impacted by >10%
4	Very High Risk	High regulatory impact (i.e. enforceable undertaking or remedial action), medium customer impact (i.e. some loss of customers), medium staff impact (i.e. some staff leave), high financial losses (i.e. multi-million), major effect on business operations (i.e. closure or suspension of business operations, management attention diverted to managing regulatory oversight) and on-going viability (i.e. regulators may seek closure of business, becomes unprofitable), adverse media attention (i.e. negative press), continuation of business jeopardised (i.e. business continuity threatened) and sales targets impacted by >25%
5	Extreme Risk	High regulatory impact (i.e. enforceable undertaking or remedial action), high customer impact (i.e. law suits, loss of customers), high staff impact (i.e. high staff turnover), high financial losses (i.e. multi-million), major effect on business operations (i.e. closure or suspension of business operations, management attention diverted to managing regulatory oversight) and on-going viability (i.e. regulators may seek closure of business, becomes unprofitable), adverse media attention (i.e. negative press), continuation of business jeopardised (i.e. business continuity threatened) and sales targets impacted by >35%

Overall - Residual Risk Rating - Matrix

The Overall Residual Risk Rating Matrix contains two dimensions - inherent risk rating (which is derived from the likelihood x

the risk impact) and the effectiveness of any mitigating controls. The Overall Residual Risk Rating Matrix simply plots the resulting risk profile once the effectiveness of any mitigating control factors have been taken into consideration, which often reduces the overall risk score and highlights the concentration of risks across the entire model. Organisations can use this to understand the impact of implementing highly effective controls to reduce the overall inherent risks and to determine the number of risk factors that remain to focus resources on improving mitigating controls in these areas. If the concentration of risks appear in the top left (excluding risk factors that are not applicable), then it is recommended that the Organisation focuses efforts in these areas to implement more effective mitigating controls.

Inherent Risk Rating							
	Ratings	0 - Not Applicable	1 - None	2 - Poor / Ineffective	3 - Fair / Moderately Effective	4 - Good / Effective	5 - Excellent / Highly Effective
	5 - Extreme Risk	Not Applicable 0	Extreme Risk 0	Extreme Risk 0	Very High Risk 0	High Risk 0	Medium Risk 1
	4 - Very High Risk	Not Applicable 0	Extreme Risk 0	Very High Risk 2	High Risk 1	Medium Risk 1	Low Risk 0
	3 - High Risk	Not Applicable 0	Very High Risk 2	Very High Risk 0	High Risk 0	Low Risk 0	Low Risk 1
	2 - Medium Risk	Not Applicable 0	High Risk 3	Medium Risk 0	Medium Risk 1	Low Risk 1	Low Risk 2
	1 - Low Risk	Not Applicable 0	Medium Risk 0	Low Risk 2	Low Risk 0	Low Risk 1	Low Risk 0
	0 - Not Applicable	Not Applicable 0	Not Applicable 0	Not Applicable 0	Not Applicable 0	Not Applicable 0	Not Applicable 0
	Effectiveness Of Control						

Key

Effectiveness of existing controls

Score	Rating	Description
0	Not Applicable	The existence or not of mitigating controls is not applicable for this risk factor.
1	None	There are no mitigating controls currently in existence.
2	Poor / Ineffective	There are ad-hoc controls currently in place which are ineffective at mitigating the identified risks and are incomplete with a major amount of improvement required. Systems have not been implemented or if they have are poorly executed, poorly documented policies and procedures are defined and sometimes followed but there are many occurrences where they are not, some staff have been trained but not all, controls have not been independently tested and a major amount of improvement has been identified. Roles and responsibilities for managing and overseeing the mitigating controls is poorly documented and largely not understood.
3	Fair / Moderately Effective	There are some controls currently in place which are moderately effective at mitigating the identified risks but are incomplete with a fair amount of improvement required. Systems to some extent are in-place, policies and procedures are defined and sometimes followed but there are occurrences where they are not, some staff have been trained but not all, controls have not been independently tested and a moderate amount of improvement has been identified. Roles and responsibilities for managing and overseeing the mitigating controls may be documented and may be understood.
4	Good / Effective	There are good controls currently in place which are effective at mitigating the identified risks but there is room for improvement. Systems to a large extent are in-place, policies and procedures are fairly well defined and mostly followed, most staff have been trained, controls may have been independently tested and areas for improvement identified. Roles and responsibilities for managing and overseeing the mitigating controls are fairly well documented and more or less understood.

5	Excellent / Highly Effective	There are excellent controls currently in place which are highly effective at mitigating the identified risks. Systems are in-place, policies and procedures are defined and followed, staff have been trained, controls have been independently tested and continuous improvement monitored. Roles and responsibilities for managing and overseeing the mitigating controls are well documented and understood.

Overall Residual Risk Rating

Score	Rating	Description
0	Not Applicable	The risk factor is not relevant to inherent risk rating matrix
1	Low Risk	Low inherent risk rating with excellent or highly effective mitigating controls where actions require minimal or no management oversight
2	Medium Risk	Medium inherent risk rating with good or effective mitigating controls where actions require a moderate priority and some degree of ongoing active management and support
3	High Risk	High inherent risk rating, with fair or moderate mitigating controls where actions require a high priority and fair amount of ongoing active management and support
4	Very High Risk	Very high inherent risk rating, with poor or ineffective mitigating controls where actions require very high priority and a high-level of ongoing active management and support
5	Extreme Risk	Extreme inherent risk rating, with non-existent mitigating controls where actions require immediate priority and significant amounts of management oversight and support.

Model Assessment Rating Scores

Group	Categorization	Sub-Categorization	% Weighting	Normalized Score	Maximum Score	Actual Score	Low	Medium	High
External			100 %	8					
	External Threat Assessment		100 %	8					
		External Organisational Level			30	0	<9	9 to 19	>19
		External Operational / Business Process Level			30	30	<9	9 to 19	>19
		External Information / System Level			30	0	<9	9 to 19	>19
		External Technical Threats -> Hardware and Software Usage			30	0	<9	9 to 19	>19
		External Technical Threats -> Electronic Data - Accidental damage, destruction or misuse of data			30	0	<9	9 to 19	>19
		External Technical Threats -> Electronic Data - Deliberate (Interference)			30	30	<9	9 to 19	>19
		External Technical Threats -> Electronic Data - Deliberate (Interception)			30	0	<9	9 to 19	>19
		External Technical Threats -> Electronic Data - Deliberate (Impersonation)			30	0	<9	9 to 19	>19
		External Technical Threats -> Electronic Data - Deliberate damage, destruction or misuse of data			30	30	<9	9 to 19	>19
		External Physical Threats -> Loss from theft, vandalism or sabotage or accidental damage			30	0	<9	9 to 19	>19
		External Physical Threats -> Unauthorised access			30	30	<9	9 to 19	>19
		External Physical Threats -> Other			30	0	<9	9 to 19	>19
		Environmental Threats -> Natural Disasters			30	30	<9	9 to 19	>19
		External Environmental Threats -> Other			30	30	<9	9 to 19	>19
		External Support Infrastructure Threats -> Power Supply			30	30	<9	9 to 19	>19
		External Support Infrastructure Threats -> Telecommunications			30	0	<9	9 to 19	>19

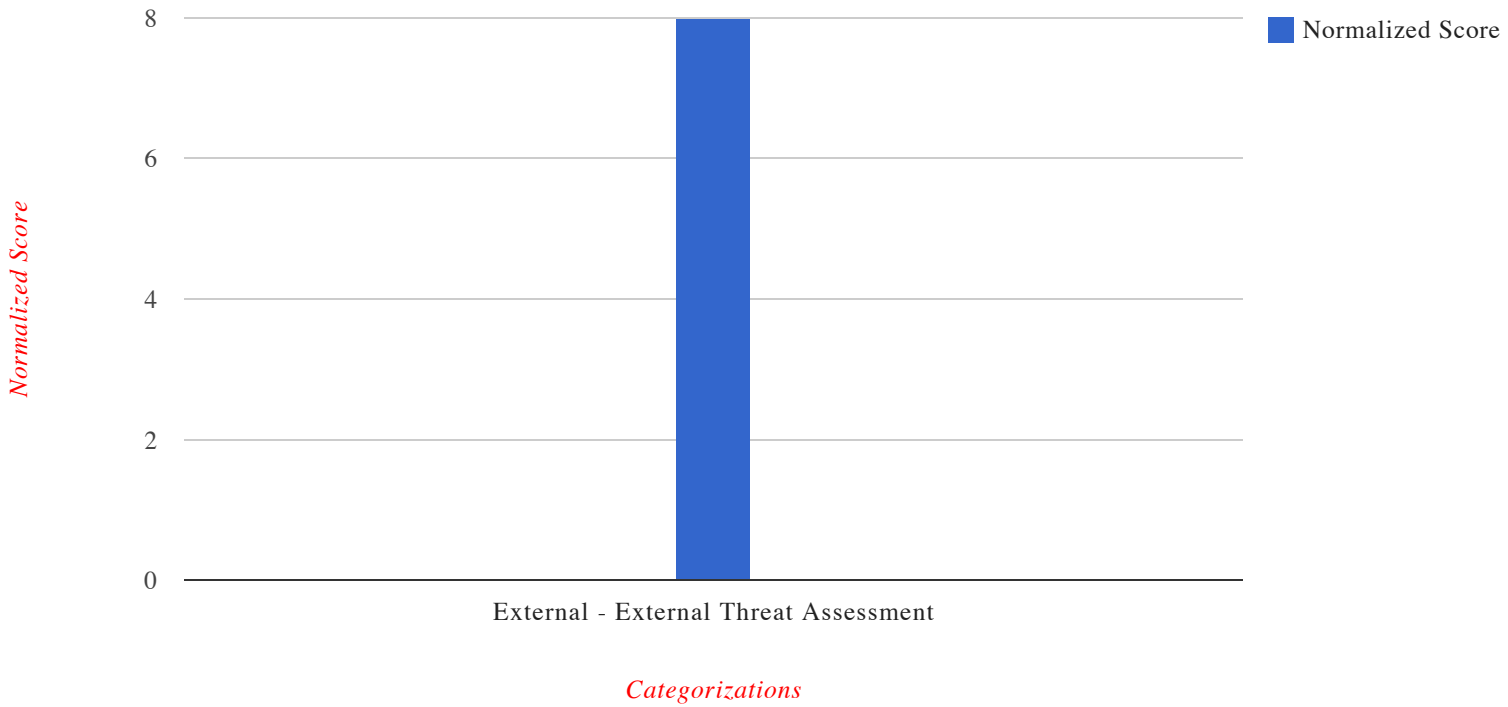
External Support Infrastructure Threats -> Support Environment	30	0	<9	9 to 19	>19
Other Threats -> Third Party	30	30	<9	9 to 19	>19

Maximum Score
This is the maximum score possible and is calculated from the individual risk factor weights.

Actual Score
This is the actual score for the risk assessment based on answering questions as being relevant to the organisation or not.

Score Range (Low-Medium-High)
This is the score range bands of risk score for each Sub-Categorization.

Model Assessment Chart



Model Assessment

External

External Threat Assessment

External Organisational Level

Question	Is the network of external vendors or third party IT service providers likely to be the target of any external denial of service threats from 'hacktivists' based on the organisations actions (e.g. industrial action, sabotage, rogue employees. political support, controversial positions taken)?				
Assumption	Organisations that use the services of external vendors or third parties that are likely to be the target of threats due to other business actions face higher risks than Organisations that do not rely on external vendors or third parties that do have a history of IT disruption undertaken because of the organisations positions on certain issues.				
Category	External - Threat Assessment - Organisational Level	**Weight**	3	**Value**	0
Answer	Yes				
Inherent Risk Rating					
Likelihood	Very Likely	**Impact**	High	**Overall Inherent Risk Rating**	Very High Risk
Risk Assessment Comments	Insert comments				
Residual Risk Rating					
Is there a mitigating control?	Yes	**Effectiveness of control**	Poor / Ineffective	**Overall Residual Risk Rating**	Very High Risk
Describe the control	Insert comments				
General Comments	Insert comments				

External

External Threat Assessment

External Operational / Business Process Level

Question	Does the external vendor or IT service provider have appropriate documentation and training for foreseeable events to ensure that operational risks associated with inadequate procedures in respect of managing IT outsourced services (i.e. hosting, development, support) is mitigated?				
Assumption	Organisations that employ external vendors or third party IT service providers that have appropriate documentation and staff training in how to respond to credible threats are more likely to reduce the impact of a credible threat on both organisations.				
Category	External - Threat Assessment - Operational / Business Process Level	**Weight**	3	**Value**	10
Answer	No				
Inherent Risk Rating					
Likelihood	Likely	**Impact**	Moderate	**Overall Inherent Risk Rating**	Medium Risk
Risk Assessment Comments	Insert comments				
Residual Risk Rating					
Is there a mitigating control?	Yes	**Effectiveness of control**	Excellent / Highly Effective	**Overall Residual Risk Rating**	Low Risk
Describe the control	Insert comments				
General Comments	Insert comments				

External

External Threat Assessment

External Information / System Level