



Heatmap Report

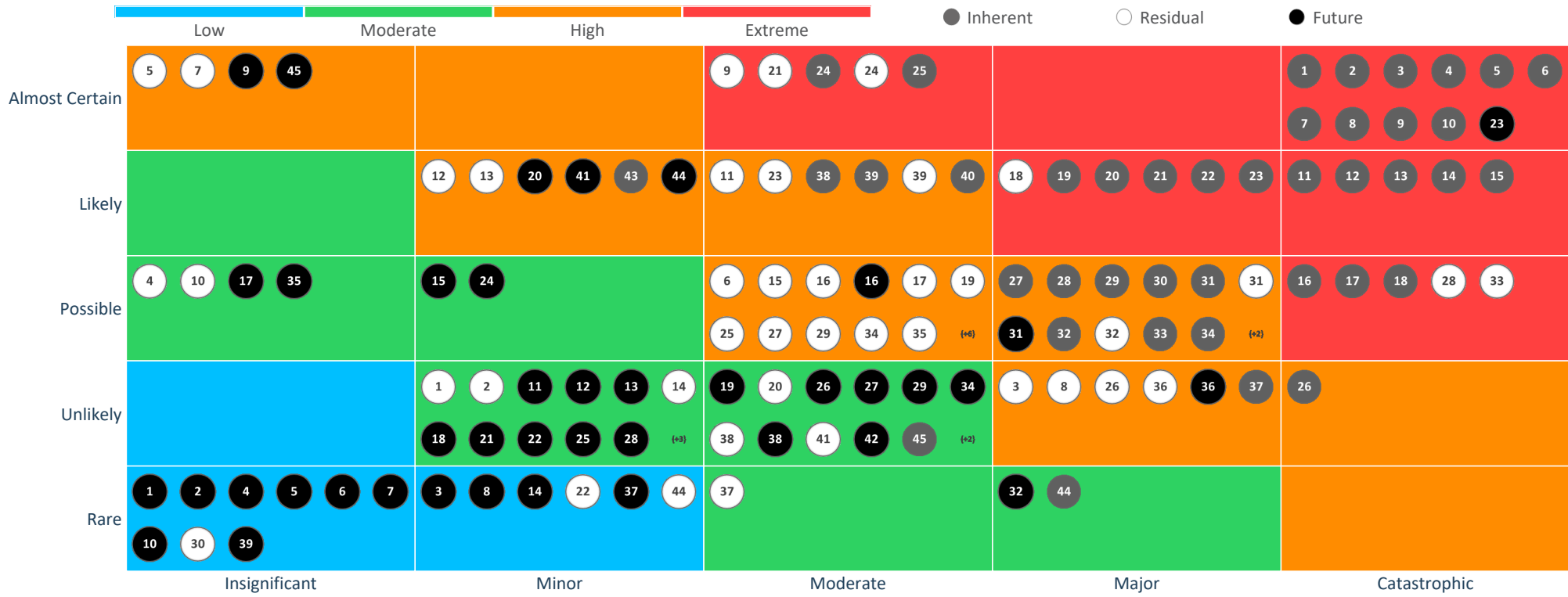
Atlantis Group

camms**risk**

Print Date: 27-Jun-2022

HEATMAP

Likelihood



Consequence

Additional overflowing risks denoted by the (+) icon:

Major x Possible	PR4, PR1
Minor x Unlikely	OR8, OR8,
Moderate x Possible	PR2, PR2, PR25, PR25, IT3, IT6
Moderate x Unlikely	IT3, PR1

RISK SUMMARY

Strategic

No.	Risk Event	Inherent	Residual	Future	Trend
14	SR1 - Failure to reduce direct greenhouse gas emissions	Extreme	Moderate	Low	↔
	Risk Comment: Addressing climate change is a major focus of the CEO and the Board. Organisation set its current emissions reduction target in 2019, to deliver a 7% reduction in our greenhouse gas emissions by 2024. In 2020, a 2.3% reduction was achieved.				
15	SR2 - Change in Industry conditions leads to financial loss	Extreme	High	Moderate	↔
	Risk Comment: Controls put in place to monitor industry conditions to prevent any unplanned loss.				
21	SR3 - Efficiency caused by procedural flexibility	Extreme	Extreme	Moderate	↔
	Risk Comment: Implementation of our latest control has significantly reduced the chances of occurrence in the future as it may take a certain time to become very effective. Though there is no improvement currently showcased in the risk rating, due to the new controls in place, we are confident that by the end of the year the risk rating will be much lower.				
44	SR4 - Inability for the organisation to meet its strategic goals due to inability to negotiate with interested parties	Moderate	Low	High	↔
	Risk Comment: New negotiation strategies are in place to further increase the chances of the organization to impress the interested parties, such as to ensure that no miscommunications or no data is left out during translations. Also to make sure that the negotiation terms are fair and has a positive outcome on all the involved parties. We have also improved our communication and transparency to ensure that the related parties will receive all the required information clearly.				
37	SR5 - Reduced transaction costs due to harmonious working practices	High	Moderate	Low	↔
	Risk Comment: The team is looking on managing the master plan outcomes.				
11	SR6 - Intellectual Property Theft	Extreme	High	Moderate	↔
	Risk Comment: There has been substantial improvements in the way the organisation prevents and manages digital loss or theft of intellectual property - including recent initiatives to upgrade staff laptops and other work devices. There does remain a gap in how physical information is secured and the adequacy and execution of HR policies to prevent inadvertent data loss. In the last month, the team have identified several actions to implement including a review of the currency of existing physical and HR intellectual property practices.				
2	SR7 - Insider Trading	Extreme	Moderate	Low	↔
	Risk Comment: There is still perceived risk among decision-makers that the process and rigor around financial and non-financial evaluations of target companies is not mature enough with regards to the insider trading. Effort will be made next quarter to address these.				
1	SR8 - Unauthorised release of confidential information	Extreme	Moderate	Low	↔
	Risk Comment: There has been substantial improvements in the way the organisation prevents and manages digital loss or theft of intellectual property - including recent initiatives to upgrade staff laptops and other work devices. There does remain a gap in how physical information is secured and the adequacy and execution of HR policies to prevent inadvertent data loss. In the last month, the team have identified several actions to implement including a review of the currency of existing physical and HR intellectual property practices.				

Operational

No.	Risk Event	Inherent	Residual	Future	Trend
29	OR1 - Systems - Unauthorized access to company information	High	High	Moderate	↔
	Risk Comment: There has been substantial improvements in the way the organisation prevents and manages digital loss or theft of intellectual property - including recent initiatives to upgrade staff laptops and other work devices. There does remain a gap in how physical information is secured and the adequacy and execution of HR policies to prevent inadvertent data loss. In the last month, the team have identified several actions to implement including a review of the currency of existing physical and HR intellectual property practices.				
16	OR2 - Inefficient document control process results in the accidental release of sensitive, confidential data	Extreme	High	High	↔
	Risk Comment: Efficient document control processes have been introduced with actions put in place to reduce risk.				
34	OR3 - Unauthorized access to company information	High	High	Moderate	↔
	Risk Comment: Control and action progress due for review next quarter.				
38	OR4 - Compliance breach resulting in high reputational damage	High	Moderate	Moderate	↔
	Risk Comment: Progress on track to mitigate risk with quarterly reviews.				
25	OR5 - Currency fluctuations affecting foreign debit/credit	Extreme	High	Moderate	↔
	Risk Comment: Currency fluctuations is not something the company has control over, but the team has implemented effective actions and controls to overcome problem.				
22	OR6 - An unsafe working environment leading to accidents and possible injury to people and staff	Extreme	Low	Moderate	↔
	Risk Comment: Controls and Actions implemented are having a significant impact on a positive direction.				
31	OR7 - Failure of critical Enterprise ICT System(s) and / or Application(s)	High	High	High	↔
	Risk Comment: -				
40	OR8 - Failure to appropriately implement business continuity program/policy	High	Moderate	Moderate	↔
	Risk Comment: Controls and actions put in place and monitored to implement continuity plan and program.				
6	OR9 - Contact with live electrical source during operations	Extreme	High	Low	
	Risk Comment: Risk is currently being managed through a variety of strategies being implemented and the controls are currently effective.				
27	OR10 - Finance & Administration - Loss or theft of critical information	High	High	Moderate	

Risk Comment: There has been substantial improvements in the way the organisation prevents and manages digital loss or theft of intellectual property - including recent initiatives to upgrade staff laptops and other work devices. There does remain a gap in how physical information is secured and the adequacy and execution of HR policies to prevent inadvertent data loss. In the last month, the team have identified several actions to implement including a review of the currency of existing physical and HR intellectual property practices.

Project

No.	Risk Event	Inherent	Residual	Future	Trend
12	- Scope Creep	Extreme	High	Moderate	
	Risk Comment: -				
33	- Corporate Strategy - Estimates are inaccurate	High	Extreme	Moderate	
	Risk Comment: -				
8	- Users don't adopt the system	Extreme	High	Low	
	Risk Comment: -				
5	- Timeline slippage	Extreme	High	Low	
	Risk Comment: -				
4	- Staff leaving during implementation	Extreme	Moderate	Low	
	Risk Comment: -				
35	PR1 - Low Product quality and safety from the third party vendors	High	High	Moderate	↔
	Risk Comment: There were two acquisitions last year that have since yielded positive to the company. This may attest to the effectiveness of controls but is not a significant enough sample size to be sure. Staff perceptions of these acquisitions is positive - staff understand the value of acquisitions despite effect of their work and largely confirmed that internal communications were sufficient.				
45	PR1 - Branch Staff exposed to other types of hospital claims other than public hospital claims	Moderate	Moderate	High	↔
	Risk Comment: -				
13	PR-1 - Scope Creep	Extreme	High	Moderate	↔
	Risk Comment: -				
42	PR2 - Inappropriate overriding of assessing messages	High	High	Moderate	↔
	Risk Comment: -				

No.	Risk Event	Inherent	Residual	Future	Trend
10	PR-2 - Staff leaving during implementation	Extreme	Moderate	Low	↔
	Risk Comment: -				
9	PR3 - Employee data being hacked by an unauthorized access	Extreme	Extreme	High	↔
	Risk Comment: There were two acquisitions last year that have since yielded positive to the company. This may attest to the effectiveness of controls but is not a significant enough sample size to be sure. Staff perceptions of these acquisitions is positive - staff understand the value of acquisitions despite effect of their work and largely confirmed that internal communications were sufficient.				
32	PR3 - Incorrect Assessment of Public Hospital Claims	High	High	Moderate	↔
	Risk Comment: -				
3	PR-3 - Users don't adopt the system	Extreme	High	Low	↔
	Risk Comment: -				
7	PR-3 - Timeline slippage	Extreme	High	Low	↔
	Risk Comment: -				
36	PR4 - Incorrect Payment of Public Hospital Claims	High	High	High	↔
	Risk Comment: -				
20	PR 20 - Inadequate debtor management	Extreme	Moderate	High	↔
	Risk Comment: The risk is towards a yellow (Monitor) Stage. But expecting it to move into greener stage.				
17	PR23 - Executive turnover disrupts project	Extreme	High	Moderate	↔
	Risk Comment: The risk is towards a yellow (Monitor) Stage. But expecting it to move into greener stage.				
24	PR23 - Executive turnover disrupts project	Extreme	Extreme	Moderate	↔
	Risk Comment: -				
28	PR24 - Estimates are inaccurate	High	Extreme	Moderate	↔
	Risk Comment: Team have done a great job in implementing the required controls and mitigating actions. Management do not yet endorse future mitigating actions and controls around acquisition evaluations as further discovery and analysis is required.				
26	PR25 - Project team misunderstand requirements	High	High	Moderate	↔
	Risk Comment: Team have done a great job in implementing the required controls and mitigating actions. Management do not yet endorse future mitigating actions and controls around acquisition evaluations as further discovery and analysis is required.				

No.	Risk Event	Inherent	Residual	Future	Trend
43	PR25 - Project team misunderstand requirements	High	High	High	↔
	Risk Comment: -				
19	PR 56 - Budget Constraints	Extreme	High	Moderate	↔
	Risk Comment: -				

Corporate

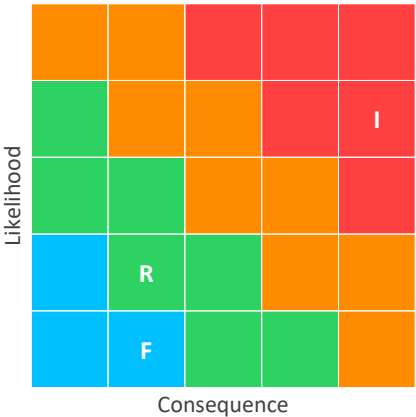
No.	Risk Event	Inherent	Residual	Future	Trend
30	IT1 - Frequent inability to meet sprint deliverables	High	Low	Extreme	↔
	Risk Comment: Team have done a great job in implementing the required controls and mitigating actions. Management do not yet endorse future mitigating actions and controls around acquisition evaluations as further discovery and analysis is required.				
23	IT2 - Unauthorised access of data stored in our internal systems	Extreme	High	Extreme	↔
	Risk Comment: It is suggested that the nature of this risk does not lend itself to simple quantitative measurement and that management performance is better made by means of the manager's qualitative judgement.				
46	IT3 - Critical Infrastructure Failures	Moderate	High	High	↔
	Risk Comment: Team have done a great job in implementing the required controls and mitigating actions. Management do not yet endorse future mitigating actions and controls around acquisition evaluations as further discovery and analysis is required.				
18	IT4 - Completed projects shortchanging security and controls	Extreme	Extreme	Moderate	↔
	Risk Comment: Significant change has happened to the risk.				
39	IT5 - Failure to comply with corporate IT policies and controls	High	High	Low	↔
	Risk Comment: -				
41	IT6 - Failure to appropriately implement business continuity program/policy	High	Moderate	High	↔
	Risk Comment: -				

RISK OVERVIEW

Strategic

SR1 Failure to reduce direct greenhouse gas emissions			
Risk Category: Environmental - Government Regulations, Brand, Provision of Service / Performance		Responsible person: Joe Smith	Next Review Date: 26 Mar, 2024
Last Reviewed Date: 12 May, 2022			
Organisation > Operations and IT			

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Aggregated Rating	
I	High
R	Moderate
F	High

Effectiveness of control	
I	Poor or non-existent – Controls Require Improvement
R	Fair – Controls Require Improvement
F	Good – Controls Working Effectively

Causes

- Action by regulators
- Insufficient investment
- Changes in community / customer expectations

Consequences

- Carbon price penalty
- Loss of investor confidence
- Higher cost of financing insurance
- Financial and operational harm

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Review and confirm natural disaster zones	David Murray	N/A	
Substitution of alternative cementitious materials for clinker	Elizabeth McMahon	Partially Effective	07 Oct, 2021
Key assets are not located in Natural Catastrophe Zones in Australia and alternate suppliers identified if disruptions occur	Elizabeth McMahon	Fully Effective	06 Aug, 2021
Implementation of alternative fuel usage strategy	David Murray	Substantially Effective	19 Nov, 2021

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Develop and present Roadmap towards 2050 net zero carbon plan.	Elizabeth McMahon	In Progress	89	13 Apr, 2022	13 Apr, 2022	AMBER
Research and present details on technology solutions available (or likely to be) for longer term abatement	Paul Max	In Progress	19	22 Oct, 2021	22 Oct, 2021	RED
Review and confirm natural disaster zones	David Murray	Completed	100	31 Aug, 2021	31 Aug, 2021	GREEN
Scope out the alternative strategies for fuel usage	Paul Max	In Progress	55	10 Aug, 2022	10 Aug, 2022	RED

Risk Appetite



KPIs

KPI Name	KPI Unit	Owner	Actuals	Target	Performance
Carbon Emissions (CO2)	#	Paul Max	150,000.00	120,000.00	RED
Increase in alternative raw materials used (%)	%	Michelle Jonas	26.00	25.00	GREEN
Reduction in Carbon Emissions (%)	%	Clarke Chan	2.00	7.00	RED
Kiln fuel sourced from alternative sources (%)	%	Riccardo Melton	50.00	50.00	GREEN

Incidents

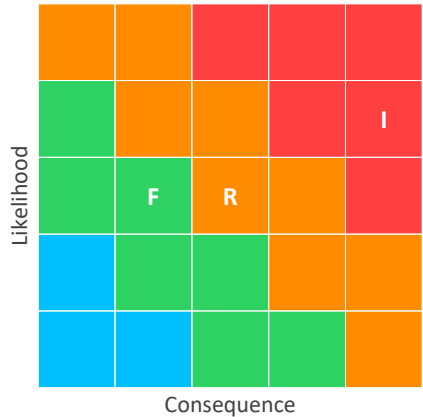
Code	Title	Type	Reported Date/Time	Responsible Officer	Status
INJ - 1	Inhaling toxic fumes	Injury	20 Oct, 2021	Andrew James	Open
INS - 10	Factory Inspection - Headland	Inspection	01 Feb, 2022	Joe Smith	Open
ISS - 5	Green house gas emission from factories	Environment	26 Oct, 2021	Elizabeth McMahon	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR4	Compliance breach resulting in high reputational damage	Joe Smith	04 Feb, 2022	High	Moderate	Moderate	Moderate	
SR4	Inability for the organisation to meet its strategic goals due to inability to negotiate with interested parties	Andrea West	08 Sep, 2022	Moderate	Low	High	High	

SR2Change in Industry conditions leads to financial loss			
Risk Category: Financial (Revenue & Costs)		Responsible person: Michelle Jonas	Last Reviewed Date: 21 Apr, 2022Next Review Date: 31 May, 2022
Organisation			

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Aggregated Rating	
I	High
R	High
F	Moderate

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite



Causes

- Poor management of invoices. Ineffectively invoicing and not chasing or providing incentives.
- No pre-plan methods were adapted
- Lack knowledge to the Staff

Consequences

- Financial Department and its members lose support.
- Action by regulators
- Impact to reputation due to loss of customer information
- Impact of other future investments and acquisitions
- Delays

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Additional staff training on minimising errors	Andrew James	Fully Effective	09 Aug, 2022
Annual budgeting process and ongoing monitoring to identify variances to expected revenue	Michelle Jonas	Substantially Effective	14 Aug, 2021
Business improvement plan developed and reviewed annually for each Department.	Joe Smith	Partially Effective	23 Oct, 2020
Develop and deliver a debtors management plan process.	Michelle Jonas	Substantially Effective	18 Sep, 2019

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Further review of Asset Accounting procedures to be programmed.	Michelle Jonas	In Progress	10	09 Feb, 2021	N/A	RED
Further review of the Asset Register to be undertaken by an external consultant in 2019 and 2020	Michelle Jonas	In Progress	10	14 Jul, 2021	N/A	RED
Review of tenancy and lease arrangements	Michelle Jonas	Completed	100	21 May, 2021	N/A	GREEN

KPIs

KPI Name	KPI Unit	Owner	Actuals	Target	Performance
\$ YTD Actual to Budget - Services Delivered	\$	Jack Watts	1,364.00	2,750.00	RED
\$ YTD Actual to Budget - Revenue from New Clients	\$	Andrea West	2,442.00	5,081.12	RED
\$ estimated profit from past year mergers and acquisitions	\$	Jack Watts	343.00	300.00	RED

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
INJ - 1	Inhaling toxic fumes	Injury	20 Oct, 2021	Andrew James	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
IT1	Frequent inability to meet sprint deliverables	Riccardo Melton	24 Apr, 2021	 High	 Low	 Extreme	N/A	
PR2	Inappropriate overriding of assessing messages	Andrea West	27 Oct, 2021	 High	 High	 Moderate	N/A	
PR3	Incorrect Assessment of Public Hospital Claims	Andrea West	01 Jun, 2022	 High	 High	 Moderate	N/A	
SR4	Inability for the organisation to meet its strategic goals due to inability to negotiate with interested parties	Andrea West	08 Sep, 2022	 Moderate	 Low	 High	 High	
SR7	Insider Trading	James Best	17 Sep, 2022	 Extreme	 Moderate	 Low	 High	

SR3

Efficiency caused by procedural flexibility

Risk Category: Service Delivery

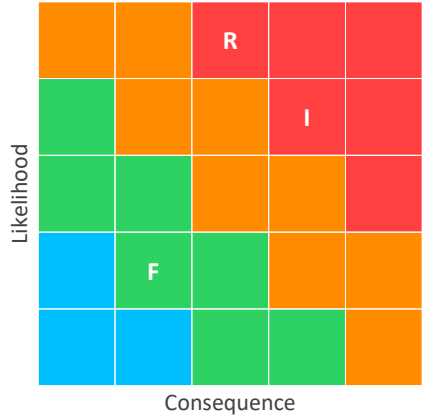
Responsible person: Elizabeth McMahon

Last Reviewed Date: 15 Dec, 2021

Next Review Date: 10 May, 2022

Organisation > Operations and IT

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Aggregated Rating	
I	Extreme
R	High
F	Extreme

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Causes

- Lack knowledge to the Staff
- No pre-plan methods were adapted

Consequences

- Workplace communication breakdown
- Impact of other future investments and acquisitions
- Workplace communication breakdown
- Impact to reputation due to loss of customer information

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Agreed timeframes for strategic initiatives	Susan Wright	Largely Ineffective	13 Apr, 2021
Business improvement plan developed and reviewed annually for each Department.	Andrea West	Fully Effective	26 Sep, 2019

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Building skills and knowledge through specific provisions such as the EBA provisions for employees with Certificates III and IV	Madeline Jones	Not Started	0	10 Sep, 2021	N/A	<div><div></div><div></div><div></div></div> RED
Development of Staff Consultative Committee	Madeline Jones	In Progress	15	15 May, 2021	N/A	<div><div></div><div></div><div></div></div> RED

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
ISS - 1	Failure to develop key competencies and behaviors.	Issues	19 Dec, 2019	Jack Watts	Open
VT - 2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	Vulnerability	14 Jan, 2022	David Murray	Open
VT - 9	HTTP Security Header Not Detected	Vulnerability	15 Jan, 2022	Joe Smith	Open

Risks

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
IT1	Frequent inability to meet sprint deliverables	Riccardo Melton	24 Apr, 2021	 High	 Low	 Extreme	N/A	
IT4	Completed projects shortchanging security and controls	Jack Watts	18 Aug, 2022	 Extreme	 Extreme	 Moderate	N/A	
OR4	Compliance breach resulting in high reputational damage	Joe Smith	04 Feb, 2022	 High	 Moderate	 Moderate	 Moderate	
OR5	Currency fluctuations affecting foreign debit/credit	Joe Smith	05 Apr, 2022	 Extreme	 High	 Moderate	N/A	
OR8	Failure to appropriately implement business continuity program/policy	Michelle Jonas	08 Apr, 2022	 High	 Moderate	 Moderate	 High	

SR4

Inability for the organisation to meet its strategic goals due to inability to negotiate with interested parties

Risk Category: Service Delivery

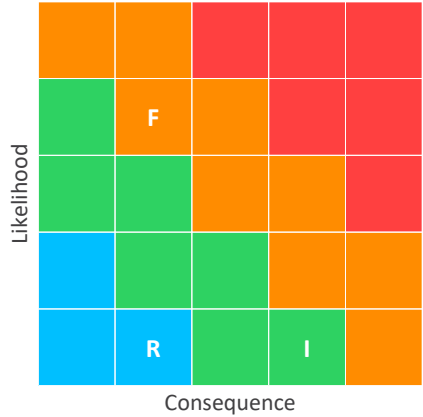
Responsible person: Andrea West

Last Reviewed Date: 08 Sep, 2020

Next Review Date: 08 Sep, 2022

Organisation > Legal & General

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Aggregated Rating	
I	Extreme
R	High
F	Moderate

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Risk action	Andrea West	Completed	100	17 Jul, 2021	N/A	<div><div></div><div></div><div></div></div> GREEN

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR5	Currency fluctuations affecting foreign debit/credit	Joe Smith	05 Apr, 2022	Extreme	High	Moderate	N/A	
SR1	Failure to reduce direct greenhouse gas emissions	Joe Smith	26 Mar, 2024	Extreme	Moderate	Low	Moderate	
SR2	Change in Industry conditions leads to financial loss	Michelle Jonas	31 May, 2022	Extreme	High	Moderate	High	

SR5

Reduced transaction costs due to harmonious working practices

Risk Category: Service Delivery

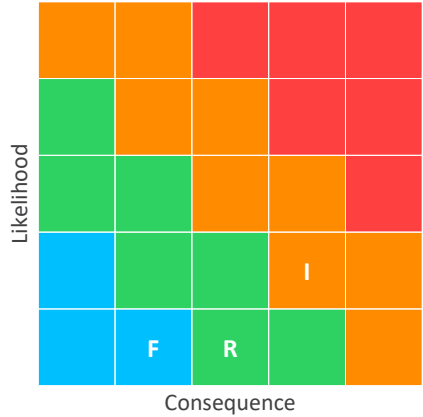
Responsible person: Susan Wright

Last Reviewed Date: 11 Oct, 2019

Next Review Date: 11 Jan, 2020

Organisation > Sales > USA

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Aggregated Rating	
I	Extreme
R	High
F	Moderate

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Contracting out certain aspects of the business that provide instant resources	Elizabeth McMahon	In Progress	10	23 Apr, 2022	N/A	<div><div></div><div></div><div></div></div> RED

KPIs

KPI Name	KPI Unit	Owner	Actuals	Target	Performance
# of IP loss incidents	#	Jack Watts	55.00	45.00	<div><div></div><div></div><div></div></div> RED

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR2	Inefficient document control process results in the accidental release of sensitive, confidential data	Andrea West	04 Jun, 2022	<div><div></div></div> Extreme	<div><div></div></div> High	<div><div></div></div> High	<div><div></div></div> Moderate	<div><div></div></div>
OR5	Currency fluctuations affecting foreign debit/credit	Joe Smith	05 Apr, 2022	<div><div></div></div> Extreme	<div><div></div></div> High	<div><div></div></div> Moderate	N/A	<div><div></div></div>

SR6

Intellectual Property Theft

Risk Category: Business Continuity, Brand, Financial (Revenue & Costs), Service Delivery

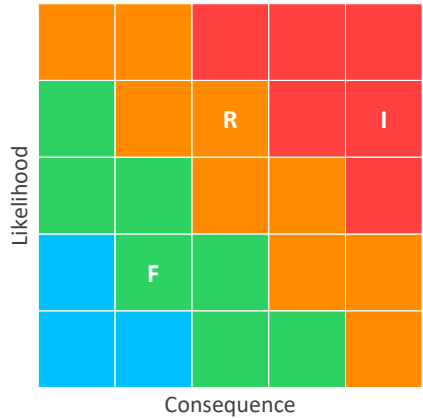
Responsible person: Elizabeth McMahon

Last Reviewed Date: 01 Mar, 2022

Next Review Date: 25 Mar, 2022

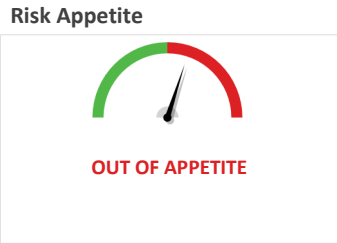
Organisation > Operations and IT

Individual Heatmap



Aggregated Rating	
I	High
R	High
F	Extreme

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A



Causes

- Inadequate ICT systems and practices to prevent loss or theft of IP
- Inadequate HR policies to prevent loss or theft of IP
- Failure to monitor critical plant and equipment
- Theft of critical information by external party

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and privacy incidents to reduce the likelihood or impact of future incidents.	James Hunt	Substantially Effective	10 Nov, 2021
Mechanisms exist to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures.	Joe Smith	Largely Ineffective	28 Apr, 2021
Safeguarding of assets	Elizabeth McMahon	Partially Effective	01 Jul, 2020
Controlled access to offices and other data storage sites	Elizabeth McMahon	Substantially Effective	31 Jan, 2022
Proactively monitor infrastructure for data breaches and theft	Clarke Chan	Partially Effective	20 Dec, 2020





Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Develop and Implement policies to address the risk of people bringing personal devices to work.	Joe Smith	In Progress	91	31 Jul, 2020	N/A	<div><div></div><div></div><div></div></div> RED
Encryption to be installed on all company laptops, mobile devices and removable media	Clarke Chan	In Progress	93	29 May, 2020	N/A	<div><div></div><div></div><div></div></div> RED
Establish procedures for the management and operation of all information processing resources in the control systems domain	Tom Jones	Completed	100	18 Jul, 2020	N/A	<div><div></div><div></div><div></div></div> GREEN

Consequences

- Impact to reputation due to loss of customer information
- Opportunity cost for time/money that could have been spent elsewhere
- External inquiries and investigations
- Loss of revenue

KPIs

KPI Name	KPI Unit	Owner	Actuals	Target	Performance
# of returning IT issues	#	Joe Smith	1.00	1.00	 GREEN
# of cyber attacks	#	Joe Smith	2.00	4.00	 GREEN
# of Critical IT system related issues	#	Joe Smith	651.00	617.00	 RED
# of IP loss incidents	#	Jack Watts	55.00	45.00	 RED

Incidents

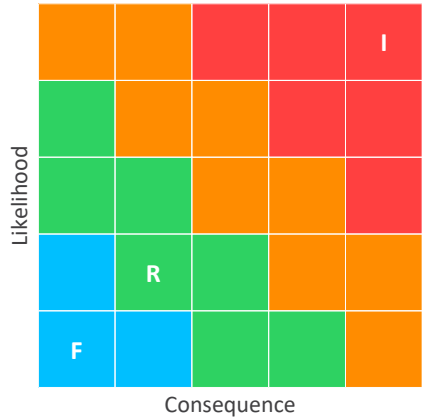
Code	Title	Type	Reported Date/Time	Responsible Officer	Status
SIE - 1	Web Server Attack - Multiple Web Attacks	SIEM Incident	14 Jan, 2022	Joe Smith	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
IT2	Unauthorised access of data stored in our internal systems	Jack Watts	22 Oct, 2020	 Extreme	 High	 Extreme	N/A	
IT5	Failure to comply with corporate IT policies and controls	Andrea West	25 May, 2022	 High	 High	 Low	N/A	
OR1	Systems - Unauthorized access to company information	Jack Watts	21 Apr, 2022	 High	 High	 Moderate	High	
OR10	Finance & Administration - Loss or theft of critical information	Jean Pierre	03 Jul, 2022	 High	 High	 Moderate	N/A	
OR7	Failure of critical Enterprise ICT System(s) and / or Application (s)	Joe Smith	21 Apr, 2022	 High	 High	 High	Moderate	
SR7	Insider Trading	James Best	17 Sep, 2022	 Extreme	 Moderate	 Low	High	

SR7 Insider Trading			
Risk Category: Financial (Revenue & Costs), Business Continuity		Responsible person: James Best	Last Reviewed Date: 21 Jun, 2021
			Next Review Date: 17 Sep, 2022
Organisation > Operations and IT			

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Aggregated Rating	
I	Extreme
R	High
F	Moderate

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite



Causes

- Inadequate financial Information controls
- Market manipulation
- Disclosure of false or misleading information to the market

Consequences

- Sharing of confidential information
- Reputation damage
- Information not publicly available

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Additional staff training on minimising errors	Andrew James	Fully Effective	09 Aug, 2022
Leverage technology to prevent insider trading	Riccardo Melton	Fully Effective	16 Sep, 2021
Established and independent investigation team for insider trading breaches	Joe Smith	Partially Effective	14 Sep, 2021
Ensure that employees are educated on insider trading	Paul Max	Partially Effective	11 Sep, 2021
Appoint an in-house watchdog,	Andrew James	Partially Effective	11 Sep, 2021
Restrict Risky Trade	Clarke Chan	Substantially Effective	02 Sep, 2021

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Appropriate measures in risky trade	Riccardo Melton	In Progress	10	17 Jul, 2021	17 Jul, 2021	RED
Employee training plan	Michelle Jonas	In Progress	55	18 Dec, 2021	18 Dec, 2021	RED

KPIs

KPI Name	KPI Unit	Owner	Actuals	Target	Performance
# of prohibited trading events	#	Madeline Jones	121.00	100.00	RED
# of insider trading events	#	Madeline Jones	5.00	10.00	GREEN

Incidents

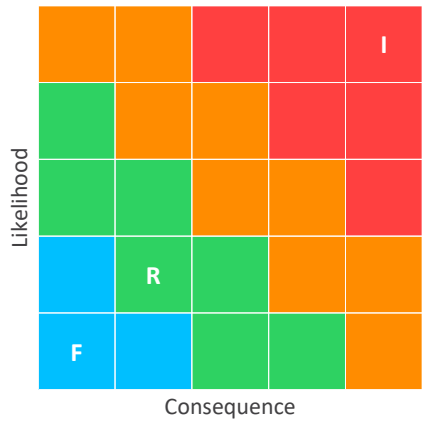
Code	Title	Type	Reported Date/Time	Responsible Officer	Status
SIE - 2	Anomalous User Behavior - Permissive File Sharing	SIEM Incident	16 Mar, 2022	Madeline Jones	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR4	Compliance breach resulting in high reputational damage	Joe Smith	04 Feb, 2022	 High	 Moderate	 Moderate	 Moderate	
OR8	Failure to appropriately implement business continuity program/policy	Michelle Jonas	08 Apr, 2022	 High	 Moderate	 Moderate	 High	
PR23	Executive turnover disrupts project	Jack Watts	18 Jun, 2022	 Extreme	 High	 Moderate	N/A	
SR2	Change in Industry conditions leads to financial loss	Michelle Jonas	31 May, 2022	 Extreme	 High	 Moderate	 High	
SR6	Intellectual Property Theft	Elizabeth McMahon	25 Mar, 2022	 Extreme	 High	 Moderate	 High	
SR8	Unauthorised release of confidential information	Paul Max	09 Sep, 2021	 Extreme	 Moderate	 Low	 High	

SR8 Unauthorised release of confidential information			
Risk Category: Financial (Revenue & Costs), Brand		Responsible person: Paul Max	Last Reviewed Date: 09 Sep, 2021
Next Review Date: 09 Sep, 2021			
Organisation > Operations and IT			

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Aggregated Rating	
I	Extreme
R	High
F	Moderate

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Causes

- Inadequate HR policies to prevent loss or theft of IP
- Lack of consensus on the nature of problems facing the team
- Misunderstood mission
- Failure to monitor critical plant and equipment
- Lack of knowledge of IP protection from staff
- Requirement changes across specialties.

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Restrict access to sensitive commercial data in line with Principle of Least Privilege (POLP)	David Murray	Partially Effective	30 Aug, 2022
Mechanisms exist to facilitate the implementation of operational security controls.	James Hunt	Largely Ineffective	06 Dec, 2022
Mechanisms exist to develop, report and monitor cybersecurity and privacy program measures of performance.	David Murray	Largely Ineffective	05 Nov, 2021
Proactively monitor infrastructure for data breaches and theft	Tom Jones	Substantially Effective	26 Jul, 2022
ICT asset evaluation and renewal system	Riccardo Melton	Substantially Effective	06 May, 2021
Data loss incident management system	Joe Smith	Largely Ineffective	21 Aug, 2020
Controlled access to offices and other data storage sites	Susan Wright	Substantially Effective	07 May, 2021


Consequences

- Legal Repercussions
- Opportunity cost for time/money that could have been spent elsewhere
- People lose trust over the organisation
- Employees health problems
- Financial loss due to poorer operational success
- Financial and operational harm

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Develop and Implement policies to address the risk of people bringing personal devices to work.	Joe Smith	In Progress	91	31 Jul, 2020	N/A	RED
Encryption to be installed on all company laptops, mobile devices and removable media	Clarke Chan	In Progress	93	29 May, 2020	N/A	RED
Establish procedures for the management and operation of all information processing resources in the control systems domain	Tom Jones	Completed	100	18 Jul, 2020	N/A	GREEN
Implement restriction to the USB Ports	David Murray	In Progress	67	09 Oct, 2021	09 Oct, 2021	RED

KPIs

KPI Name	KPI Unit	Owner	Actuals	Target	Performance
# of cyber attacks	#	Joe Smith	2.00	4.00	 GREEN
# of Critical IT system related issues	#	Joe Smith	651.00	617.00	 RED
# of IP loss incidents	#	Jack Watts	55.00	45.00	 RED

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
BI - 1	A networking device crashes, bringing down several services	Business Incidents	26 Nov, 2020	Clarke Chan	Open
BI - 12	Noted failure to report a fraudulent transaction	Incident	08 Nov, 2021	Jack Watts	Open
BI - 5	The system was access by an unauthorised third party	Business Incidents	03 Sep, 2020	Elizabeth McMahon	Open
BI - 6	Privacy Compliance Breach	Business Incidents	26 Mar, 2021	Elizabeth McMahon	Open
BI - 7	Data Loss arising from IT System Malfunction	Incident	09 Oct, 2019	Tom Jones	Open
DSB - 1	The system was accessed by an unauthorised third party	Data Breach	11 Feb, 2022	Madeline Jones	Open
VT - 1	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	Vulnerability	05 Jan, 2022	Madeline Jones	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR1	Systems - Unauthorized access to company information	Jack Watts	21 Apr, 2022	 High	 High	 Moderate	 High	
OR10	Finance & Administration - Loss or theft of critical information	Jean Pierre	03 Jul, 2022	 High	 High	 Moderate	N/A	
OR2	Inefficient document control process results in the accidental release of sensitive, confidential data	Andrea West	04 Jun, 2022	 Extreme	 High	 High	 Moderate	

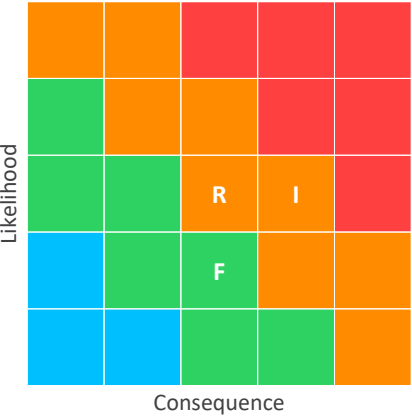
Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR3	Unauthorized access to company information	Jack Watts	11 Jan, 2022	 High	 High	 Moderate	N/A	
OR4	Compliance breach resulting in high reputational damage	Joe Smith	04 Feb, 2022	 High	 Moderate	 Moderate	 Moderate	
SR7	Insider Trading	James Best	17 Sep, 2022	 Extreme	 Moderate	 Low	 High	

Operational

OR1 Systems - Unauthorized access to company information			
Risk Category: Financial (Revenue & Costs) - Expenditure Management		Responsible person: Jack Watts	Last Reviewed Date: 21 Jan, 2022
			Next Review Date: 21 Apr, 2022
Organisation > Operations and IT > Systems			

Individual Heatmap



I	Inherent Risk Assessment
R	Residual Risk Assessment
F	Future Risk Assessment

Aggregated Rating	
I	Extreme
R	High
F	Moderate

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Causes

- Failure to comply with corporate IT policies and controls
- Insufficient IT security management
- Poor management of invoices. Ineffectively invoicing and not chasing or providing incentives.
- Insufficient financial due diligence on target company
- Lack knowledge to the Staff

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Restrict access to sensitive commercial data in line with Principle of Least Privilege (POLP)	David Murray	Partially Effective	30 Aug, 2022
Controlled access to offices and other data storage sites	Elizabeth McMahon	Substantially Effective	31 Jan, 2022
Proactively monitor infrastructure for data breaches and theft	Tom Jones	Substantially Effective	26 Jul, 2022
Executive data protection regime	Elizabeth McMahon	Partially Effective	03 Feb, 2022
Maintain a separate server for confidential financial information.	Jean Pierre	Substantially Effective	29 Jan, 2022

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Investigate the software market offerings for financial document security management	Jean Pierre	In Progress	90	10 Mar, 2022	N/A	<div><div></div><div></div><div></div></div> AMBER
Password changes should be system enforced and occur at least every 2 months, with strict password policy in place	Joe Smith	In Progress	70	23 Mar, 2022	N/A	<div><div></div><div></div><div></div></div> RED
Repeat periodic review and testing in 2 months	Andrew James	In Progress	40	31 Jan, 2022	N/A	<div><div></div><div></div><div></div></div> RED

Risk Appetite



Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
BI - 1	A networking device crashes, bringing down several services	Business Incidents	26 Nov, 2020	Clarke Chan	Open
DSB - 1	The system was accessed by an unauthorised third party	Data Breach	11 Feb, 2022	Madeline Jones	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
CR1	Failure to achieve legal and regulatory compliance with relevant Australian Standards	Joe Smith	03 Jan, 2020	High	Moderate	Moderate	N/A	
CR1	Failure to achieve legal and regulatory compliance with relevant Australian Standards	Joe Smith	03 Jan, 2020	High	Moderate	Moderate	N/A	
CR1	Failure to achieve legal and regulatory compliance with relevant Australian Standards	Joe Smith	03 Jan, 2020	High	Moderate	Moderate	N/A	
CR1	Failure to achieve legal and regulatory compliance with relevant Australian Standards	Joe Smith	03 Jan, 2020	High	Moderate	Moderate	N/A	
OR10	Finance & Administration - Loss or theft of critical information	Jean Pierre	03 Jul, 2022	High	High	Moderate	N/A	
OR7	Failure of critical Enterprise ICT System(s) and / or Application (s)	Joe Smith	21 Apr, 2022	High	High	High	Moderate	
PR3	Employee data being hacked by an unauthorized access	Madeline Jones	18 Aug, 2020	Extreme	Extreme	High	N/A	
SR6	Intellectual Property Theft	Elizabeth McMahon	25 Mar, 2022	Extreme	High	Moderate	High	
SR8	Unauthorised release of confidential information	Paul Max	09 Sep, 2021	Extreme	Moderate	Low	High	

OR2

Inefficient document control process results in the accidental release of sensitive, confidential data

Risk Category: Brand - Corporate Relations and Partnerships, People / WHS

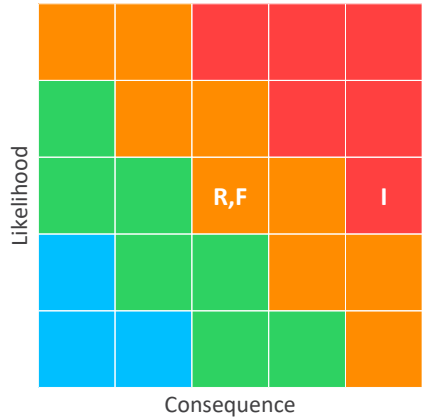
Organisation > Sales > USA

Responsible person: Andrea West

Last Reviewed Date: 03 Jun, 2022

Next Review Date: 04 Jun, 2022

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Aggregated Rating	
I	High
R	Moderate
F	Low

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite



Causes

- No pre-plan methods were adapted
- Insufficient financial due diligence on target company
- Lack knowledge to the Staff
- No pre-plan methods were adapted

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Restrict access to sensitive commercial data in line with Principle of Least Privilege (POLP)	David Murray	Partially Effective	30 Aug, 2022
Provision of 'global' resource pool, to accommodate for fluctuations in demand across various teams	Elizabeth McMahon	Partially Effective	18 May, 2022
Business improvement plan developed and reviewed annually for each Department.	Andrea West	Fully Effective	26 Sep, 2019

Consequences

- Impact to reputation due to loss of customer information
- Impact of other future investments and acquisitions
- Legal repercussions and costs
- Unhappy Clients

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Investigate the software market offerings for financial document security management	Jean Pierre	In Progress	90	10 Mar, 2022	N/A	<div><div></div><div></div><div></div></div> AMBER

KPIs

KPI Name	KPI Unit	Owner	Actuals	Target	Performance
# of IP loss incidents	#	Jack Watts	55.00	45.00	<div><div></div><div></div><div></div></div> RED

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
INJ - 5	An senior tech staff was stumbled in the restroom.	Injury	22 Jul, 2021	Tom Jones	Open

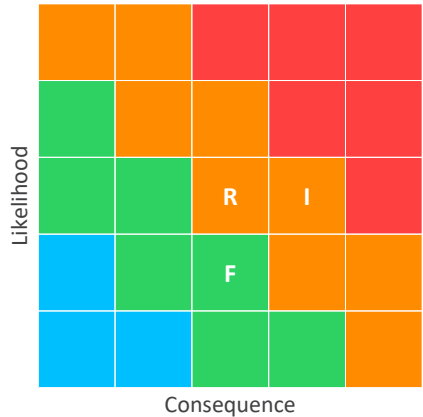
Risks

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR8	Failure to appropriately implement business continuity program/policy	Michelle Jonas	08 Apr, 2022	 High	 Moderate	 Moderate	 High	
SR5	Reduced transaction costs due to harmonious working practices	Susan Wright	11 Jan, 2020	 High	 Moderate	 Low	 High	
SR8	Unauthorised release of confidential information	Paul Max	09 Sep, 2021	 Extreme	 Moderate	 Low	 High	

OR3 Unauthorized access to company information			
Risk Category: Financial (Revenue & Costs) - Expenditure Management		Responsible person: Jack Watts	Last Reviewed Date: 19 Jan, 2022
			Next Review Date: 11 Jan, 2022

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Causes

- Insufficient IT security management
- Insufficient financial due diligence on target company
- Failure to comply with corporate IT policies and controls
- Lack knowledge to the Staff
- Poor management of invoices. Ineffectively invoicing and not chasing or providing incentives.

Consequences

- Impact to reputation due to loss of customer information
- Impact to current and future cashflow
- Legal repercussions and costs
- Financial Department and its members lose support.
- Impact to Brand Image

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Executive data protection regime	Elizabeth McMahon	Partially Effective	03 Feb, 2022

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Password changes should be system enforced and occur at least every 2 months, with strict password policy in place	Joe Smith	In Progress	70	23 Mar, 2022	N/A	<div><div></div><div></div><div></div><div></div></div> RED
Repeat periodic review and testing in 2 months	Andrew James	In Progress	40	31 Jan, 2022	N/A	<div><div></div><div></div><div></div><div></div></div> RED

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
BI - 1	A networking device crashes, bringing down several services	Business Incidents	26 Nov, 2020	Clarke Chan	Open
DSB - 1	The system was accessed by an unauthorised third party	Data Breach	11 Feb, 2022	Madeline Jones	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
CR1	Failure to achieve legal and regulatory compliance with relevant Australian Standards	Joe Smith	03 Jan, 2020	High	Moderate	Moderate	N/A	

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
CR1	Failure to achieve legal and regulatory compliance with relevant Australian Standards	Joe Smith	03 Jan, 2020	 High	 Moderate	 Moderate	N/A	
CR1	Failure to achieve legal and regulatory compliance with relevant Australian Standards	Joe Smith	03 Jan, 2020	 High	 Moderate	 Moderate	N/A	
CR1	Failure to achieve legal and regulatory compliance with relevant Australian Standards	Joe Smith	03 Jan, 2020	 High	 Moderate	 Moderate	N/A	
OR7	Failure of critical Enterprise ICT System(s) and / or Application (s)	Joe Smith	21 Apr, 2022	 High	 High	 High	 Moderate	
SR8	Unauthorised release of confidential information	Paul Max	09 Sep, 2021	 Extreme	 Moderate	 Low	 High	

OR4

Compliance breach resulting in high reputational damage

Risk Category: Business Continuity

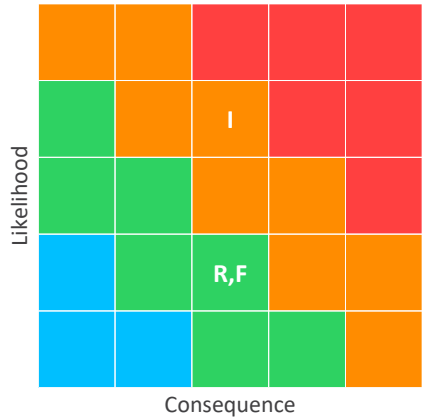
Responsible person: Joe Smith

Last Reviewed Date: 24 Apr, 2020

Next Review Date: 04 Feb, 2022

Organisation > Sales > APAC

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Aggregated Rating	
I	Extreme
R	Moderate
F	Low

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Establish team to liaise with local authority to review delivery routes in advance of road closures	Jack Watts	Substantially Effective	17 Jun, 2020

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Share logistics data with subsidiaries	Joe Smith	In Progress	89	03 Oct, 2018	N/A	<div><div></div><div></div><div></div></div> RED

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
SR1	Failure to reduce direct greenhouse gas emissions	Joe Smith	26 Mar, 2024	<div><div></div></div> Extreme	<div><div></div></div> Moderate	<div><div></div></div> Low	<div><div></div></div> Moderate	<div><div></div></div>
SR3	Efficiency caused by procedural flexibility	Elizabeth McMahon	10 May, 2022	<div><div></div></div> Extreme	<div><div></div></div> Extreme	<div><div></div></div> Moderate	<div><div></div></div> High	<div><div></div></div>
SR7	Insider Trading	James Best	17 Sep, 2022	<div><div></div></div> Extreme	<div><div></div></div> Moderate	<div><div></div></div> Low	<div><div></div></div> High	<div><div></div></div>
SR8	Unauthorised release of confidential information	Paul Max	09 Sep, 2021	<div><div></div></div> Extreme	<div><div></div></div> Moderate	<div><div></div></div> Low	<div><div></div></div> High	<div><div></div></div>

OR5

Currency fluctuations affecting foreign debit/credit

Risk Category: Environmental

Responsible person: Joe Smith

Secondary Risk Owner(s): Jean Pierre

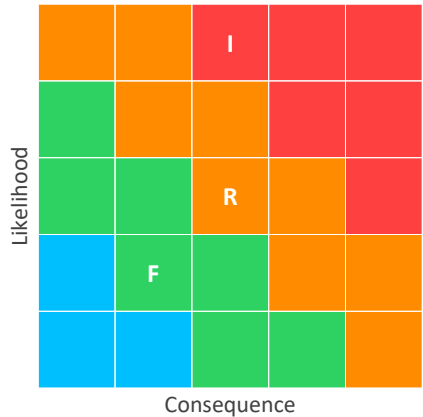
Last Reviewed Date: 20 Jan, 2022

Next Review Date: 05 Apr, 2022

Organisation > Corporate Strategy > Finance

Organisation > Operations and IT > Support

Individual Heatmap



Causes

- Failure to monitor critical plant and equipment
- Changes in government and legislation
- Insufficient financial due diligence on target company
- Miscalculations in the evaluation of financial position
- No pre-plan methods were adapted

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Establish a hedge for project costs to protect against currency fluctuations	Jean Pierre	Largely Ineffective	04 Jun, 2022

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Extend hedging strategy to include subsidiaries	Jean Pierre	In Progress	84	28 Dec, 2022	N/A	<div><div></div><div></div><div></div><div></div><div></div></div> GREEN

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
BI - 2	Breach of Compliance under the Financial Stability Standards	Incident	12 Dec, 2020	Andrew James	Open
ISS - 1	IT System Malfunction	Property	09 Jul, 2018	Joe Smith	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
SR3	Efficiency caused by procedural flexibility	Elizabeth McMahon	10 May, 2022	<div><div></div></div> Extreme	<div><div></div></div> Extreme	<div><div></div></div> Moderate	<div><div></div></div> High	<div><div></div></div>
SR4	Inability for the organisation to meet its strategic goals due to inability to negotiate with interested parties	Andrea West	08 Sep, 2022	<div><div></div></div> Moderate	<div><div></div></div> Low	<div><div></div></div> High	<div><div></div></div> High	<div><div></div></div>

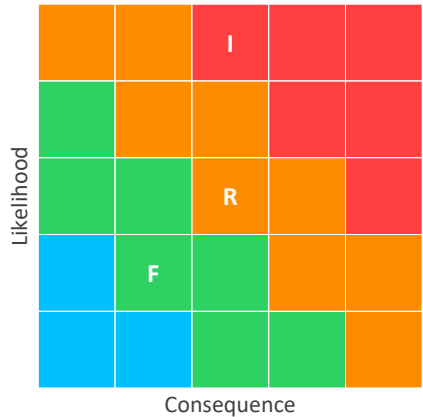
OR5 Currency fluctuations affecting foreign debit/credit

Risk Category: Environmental Responsible person: Joe Smith Secondary Risk Owner(s): Jean Pierre Last Reviewed Date: 20 Jan, 2022 Next Review Date: 05 Apr, 2022

Organisation > Corporate Strategy > Finance

Organisation > Operations and IT > Support

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Causes

- Failure to monitor critical plant and equipment
- Changes in government and legislation
- Insufficient financial due diligence on target company
- Miscalculations in the evaluation of financial position
- No pre-plan methods were adapted

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Establish a hedge for project costs to protect against currency fluctuations	Jean Pierre	Largely Ineffective	04 Jun, 2022

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Extend hedging strategy to include subsidiaries	Jean Pierre	In Progress	84	28 Dec, 2022	N/A	<div><div></div><div></div><div></div><div></div><div></div></div> GREEN






Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
BI - 2	Breach of Compliance under the Financial Stability Standards	Incident	12 Dec, 2020	Andrew James	Open
ISS - 1	IT System Malfunction	Property	09 Jul, 2018	Joe Smith	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
SR3	Efficiency caused by procedural flexibility	Elizabeth McMahon	10 May, 2022	<div><div></div></div> Extreme	<div><div></div></div> Extreme	<div><div></div></div> Moderate	<div><div></div></div> High	<div><div></div></div>
SR4	Inability for the organisation to meet its strategic goals due to inability to negotiate with interested parties	Andrea West	08 Sep, 2022	<div><div></div></div> Moderate	<div><div></div></div> Low	<div><div></div></div> High	<div><div></div></div> High	<div><div></div></div>

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
SR5	Reduced transaction costs due to harmonious working practices	Susan Wright	11 Jan, 2020	 High	 Moderate	 Low	 High	

OR6

An unsafe working environment leading to accidents and possible injury to people and staff

Risk Category: Financial (Revenue & Costs) - Budget 21/22, Brand

Responsible person: Elizabeth McMahon

Secondary Risk Owner(s): Joe Smith

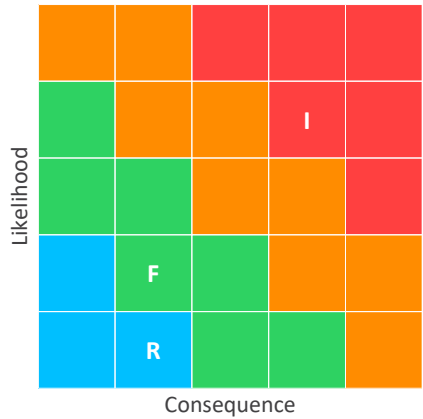
Last Reviewed Date: 20 Jan, 2022

Next Review Date: 08 Jul, 2022

Organisation > Operations and IT

Organisation > Sales > EMEA

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Good – Controls Working Effectively
F	N/A

Risk Appetite



Causes

- Lack knowledge to the Staff
- No pre-plan methods were adapted
- WHS Guidelines not followed
- Hazard signage requirements not followed

Consequences

- Workplace communication breakdown
- Unhappy Clients
- Delays

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Induction training on customer relationship	Madeline Jones	Partially Effective	28 Oct, 2020
Customer Satisfaction surveys on counters	Elizabeth McMahon	Substantially Effective	31 Jan, 2019

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Additional training on customer relationship	Elizabeth McMahon	In Progress	55	28 Feb, 2019	N/A	<div><div></div><div></div><div></div></div> RED
Staff motivation and recognition process initiation	Susan Wright	In Progress	20	30 Oct, 2019	N/A	<div><div></div><div></div><div></div></div> RED

KPIs

KPI Name	KPI Unit	Owner	Actuals	Target	Performance
# of cyber attacks	#	Joe Smith	2.00	4.00	<div><div></div><div></div><div></div></div> GREEN
\$ YTD Actual to Budget - Services Delivered	\$	Jack Watts	1,364.00	2,750.00	<div><div></div><div></div><div></div></div> RED
\$ YTD Actual to Budget – Value of Approved Work	\$	Jack Watts	29,000.00	65,000.00	<div><div></div><div></div><div></div></div> RED





Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
COM - 1	Verbal abuse allegedly directed towards child	Complaint	23 Aug, 2019	Andrew James	Open
INJ - 3	Colliding with an object	Injury	29 Oct, 2021	Paul Max	Open

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
INJ - 4	Tripping injury to member of the staff in breakroom	Injury	27 Dec, 2021	Clarke Chan	Open
INJ - 7	Slipped on Water Hurt Back	Injury	16 Mar, 2022	Madeline Jones	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
PR1	Branch Staff exposed to other types of hospital claims other than public hospital claims	Andrew James	27 Dec, 2019	 Moderate	 Moderate	 High	N/A	

OR7

Failure of critical Enterprise ICT System(s) and / or Application(s)

Risk Category: Brand - Public Relations

Responsible person: Joe Smith

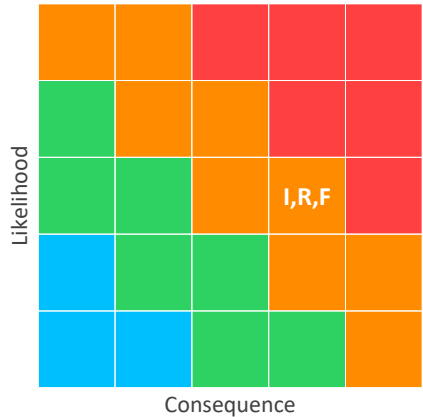
Secondary Risk Owner(s): Jack Watts

Last Reviewed Date: 27 Dec, 2021

Next Review Date: 21 Apr, 2022

Organisation > Operations and IT > Systems

Individual Heatmap



- I
- Inherent Risk Assessment
- R
- Residual Risk Assessment
- F
- Future Risk Assessment

Aggregated Rating	
I	Extreme
R	Moderate
F	High

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite



Causes

- Lack of knowledge regarding critical systems and information
- Unplanned downtime as a result of poorly executed changes

Consequences

- internal financial models
- Exfiltration of market-sensitive data including M&A
- Loss or unavailability of company data

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Business Impact Assessment	Joe Smith	Fully Effective	30 Jun, 2021
ICT asset evaluation and renewal system	Tom Jones	Largely Ineffective	27 May, 2020

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Develop a new policy for BIAs to be undertaken every 3 months for all critical systems across OZ Minerals	Jack Watts	Not Started	0	31 Aug, 2021	31 Aug, 2021	RED
Review code management protocols across key systems	Joe Smith	Completed	100	30 Jun, 2021	30 Jun, 2021	GREEN

KPIs

KPI Name	KPI Unit	Owner	Actuals	Target	Performance
# of cyber attacks	#	Joe Smith	2.00	4.00	GREEN
# of Critical IT system related issues	#	Joe Smith	651.00	617.00	RED
# of IP loss incidents	#	Jack Watts	55.00	45.00	RED


Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
BI - 12	Noted failure to report a fraudulent transaction	Incident	08 Nov, 2021	Jack Watts	Open
HAZ - 10	Lifting matts at pedestrian crossing	Hazard	05 Apr, 2017	Andrea West	Open
SIE - 1	Web Server Attack - Multiple Web Attacks	SIEM Incident	14 Jan, 2022	Joe Smith	Open

Incidents

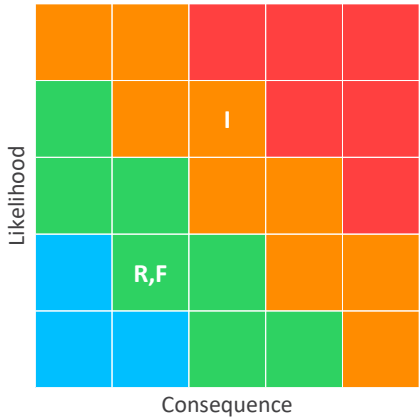
Code	Title	Type	Reported Date/Time	Responsible Officer	Status
VT - 1	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	Vulnerability	05 Jan, 2022	Madeline Jones	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR1	Systems - Unauthorized access to company information	Jack Watts	21 Apr, 2022	 High	 High	 Moderate	 High	
OR10	Finance & Administration - Loss or theft of critical information	Jean Pierre	03 Jul, 2022	 High	 High	 Moderate	N/A	
OR3	Unauthorized access to company information	Jack Watts	11 Jan, 2022	 High	 High	 Moderate	N/A	
PR 20	Inadequate debtor management	Madeline Jones	24 Jul, 2020	 Extreme	 Moderate	 High	N/A	
PR2	Inappropriate overriding of assessing messages	Andrea West	27 Oct, 2021	 High	 High	 Moderate	N/A	
SR6	Intellectual Property Theft	Elizabeth McMahon	25 Mar, 2022	 Extreme	 High	 Moderate	 High	

<div>OR8</div> <div>Failure to appropriately implement business continuity program/policy</div>				
Risk Category: Financial (Revenue & Costs) - Expenditure Management		Responsible person: Michelle Jonas	Secondary Risk Owner(s): Joe Smith, Susan Wright, Andrew James	Last Reviewed Date: 10 Apr, 2019
Next Review Date: 08 Apr, 2022				

Individual Heatmap



- I** Inherent Risk Assessment
- R** Residual Risk Assessment
- F** Future Risk Assessment

Aggregated Rating	
I	Extreme
R	High
F	Moderate

Effectiveness of control	
I	N/A
R	Good – Controls Working Effectively
F	N/A

Risk Appetite



Causes

- Lack knowledge to the Staff
- No pre-plan methods were adapted
- Poor management of invoices. Ineffectively invoicing and not chasing or providing incentives.



Consequences

- Legal repercussions and costs
- Impact to reputation due to loss of customer information
- Workplace communication breakdown

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Provision of 'global' resource pool, to accommodate for fluctuations in demand across various teams	Elizabeth McMahon	Partially Effective	18 May, 2022
Agreed timeframes for strategic initiatives	Susan Wright	Largely Ineffective	13 Apr, 2021






KPIs

KPI Name	KPI Unit	Owner	Actuals	Target	Performance
\$ YTD Actual to Budget - Services Delivered	\$	Jack Watts	1,364.00	2,750.00	 RED
\$ YTD Actual to Budget – Value of Approved Work	\$	Jack Watts	29,000.00	65,000.00	 RED

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR2	Inefficient document control process results in the accidental release of sensitive, confidential data	Andrea West	04 Jun, 2022	 Extreme	 High	 High	 Moderate	
PR 56	Budget Constraints	Madeline Jones	18 Jun, 2022	 Extreme	 High	 Moderate	N/A	
SR3	Efficiency caused by procedural flexibility	Elizabeth McMahon	10 May, 2022	 Extreme	 Extreme	 Moderate	 High	

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
SR7	Insider Trading	James Best	17 Sep, 2022	 Extreme	 Moderate	 Low	 High	

OR9

Contact with live electrical source during operations

Risk Category: People / WHS - Resource Allocation

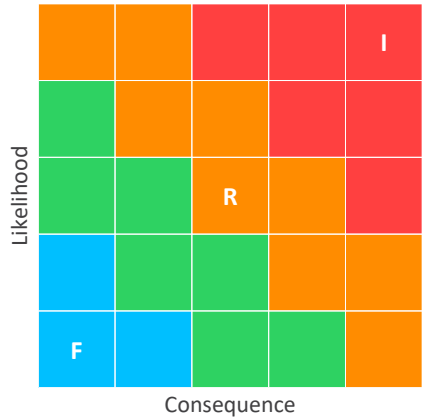
Responsible person: Shannon Roma

Last Reviewed Date: 10 May, 2022

Next Review Date: 17 Sep, 2023

Organisation > Operations and IT > Support

Individual Heatmap



Causes

- Unsafe acts
- Hazard signage requirements not followed
- Failure to appropriately complete pre-start checklists

Consequences

- Employees health problems
- Electric shock
- Permanent Injury

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Emergency management plan and procedures	Elizabeth McMahon	Partially Effective	31 Aug, 2022
Equipment of a fall arrest system in construction sites	Andrew James	Fully Effective	31 May, 2022
Co-ordinated approach to training and development of all staff	Clarke Chan	Substantially Effective	27 Jul, 2022

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Identification of potential sources of fault occurrence and how they can be controlled	Andrew James	In Progress	65	30 Jun, 2022	N/A	<div><div></div><div></div><div></div><div></div></div> GREEN
Implementation of a system for monitoring the control measures within the electrical system	David Murray	Completed	100	23 Jun, 2022	N/A	<div><div></div><div></div><div></div><div></div></div> GREEN
Review error detection procedures	Elizabeth McMahon	In Progress	10	15 Jun, 2022	15 Jun, 2022	<div><div></div><div></div><div></div><div></div></div> RED

KPIs

KPI Name	KPI Unit	Owner	Actuals	Target	Performance
# Lost Time Injury Frequency Rate (LTIFR)	#	Clarke Chan	12,722,222.22	12,824,000.00	<div><div></div><div></div><div></div><div></div></div> GREEN
# Lost Time Injuries YTD	#	Clarke Chan	126.00	125.00	<div><div></div><div></div><div></div><div></div></div> RED

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
INJ - 4	Tripping injury to member of the staff in breakroom	Injury	27 Dec, 2021	Clarke Chan	Open

- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

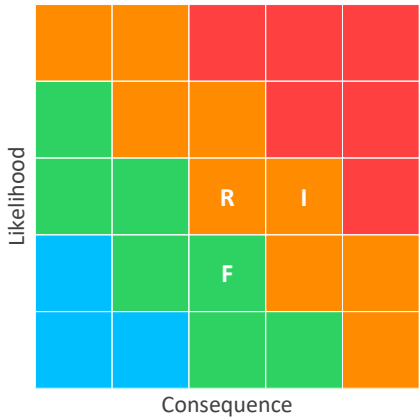
Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite



<div>OR10</div> <div>Finance & Administration - Loss or theft of critical information</div>				
Risk Category: Business Continuity, Corporate Relations and Partnerships, Public Relations		Responsible person: Jean Pierre	Secondary Risk Owner(s): Paul Max	Last Reviewed Date: 03 Jun, 2022
Next Review Date: 03 Jul, 2022				
Organisation > Corporate Strategy > Finance				
Organisation > Operations and IT > Systems				

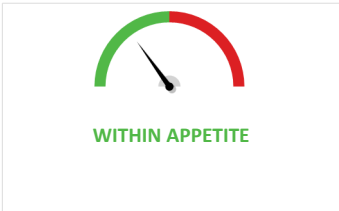
Individual Heatmap



I Inherent Risk Assessment
R Residual Risk Assessment
F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Causes

- Insufficient IT security management
- Poor management of invoices. Ineffectively invoicing and not chasing or providing incentives.
- Failure to comply with corporate IT policies and controls
- Lack knowledge to the Staff
- Insufficient financial due diligence on target company

Consequences

- Impact to reputation due to loss of customer information
- Impact to current and future cashflow
- Financial Department and its members lose support.
- Legal repercussions and costs
- Impact to Brand Image

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Restrict access to sensitive commercial data in line with Principle of Least Privilege (POLP)	David Murray	Partially Effective	30 Aug, 2022
Proactively monitor infrastructure for data breaches and theft	Tom Jones	Substantially Effective	26 Jul, 2022
Executive data protection regime	Elizabeth McMahon	Partially Effective	03 Feb, 2022
Controlled access to offices and other data storage sites	Elizabeth McMahon	Substantially Effective	31 Jan, 2022
Maintain a separate server for confidential financial information.	Jean Pierre	Substantially Effective	29 Jan, 2022





































Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Investigate the software market offerings for financial document security management	Jean Pierre	In Progress	90	10 Mar, 2022	N/A	AMBER
Password changes should be system enforced and occur at least every 2 months, with strict password policy in place	Joe Smith	In Progress	70	23 Mar, 2022	N/A	RED
Repeat periodic review and testing in 2 months	Andrew James	In Progress	40	31 Jan, 2022	N/A	RED

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
BI - 1	A networking device crashes, bringing down several services	Business Incidents	26 Nov, 2020	Clarke Chan	Open
DSB - 1	The system was accessed by an unauthorised third party	Data Breach	11 Feb, 2022	Madeline Jones	Open

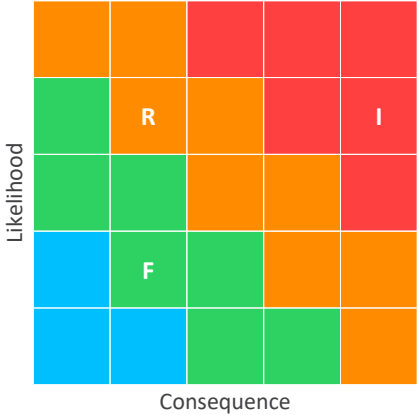
Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
CR1	Failure to achieve legal and regulatory compliance with relevant Australian Standards	Joe Smith	03 Jan, 2020	 High	 Moderate	 Moderate	N/A	
CR1	Failure to achieve legal and regulatory compliance with relevant Australian Standards	Joe Smith	03 Jan, 2020	 High	 Moderate	 Moderate	N/A	
CR1	Failure to achieve legal and regulatory compliance with relevant Australian Standards	Joe Smith	03 Jan, 2020	 High	 Moderate	 Moderate	N/A	
OR1	Systems - Unauthorized access to company information	Jack Watts	21 Apr, 2022	 High	 High	 Moderate	 High	
OR7	Failure of critical Enterprise ICT System(s) and / or Application (s)	Joe Smith	21 Apr, 2022	 High	 High	 High	 Moderate	
PR3	Employee data being hacked by an unauthorized access	Madeline Jones	18 Aug, 2020	 Extreme	 Extreme	 High	N/A	
SR6	Intellectual Property Theft	Elizabeth McMahon	25 Mar, 2022	 Extreme	 High	 Moderate	 High	
SR8	Unauthorised release of confidential information	Paul Max	09 Sep, 2021	 Extreme	 Moderate	 Low	 High	

Project

Scope Creep			
Risk Category: Environmental		Responsible person: Jack Watts	Last Reviewed Date:
			Next Review Date: 12 Apr, 2023

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Corporate Strategy - Estimates are inaccurate

Risk Category: Financial (Revenue & Costs)

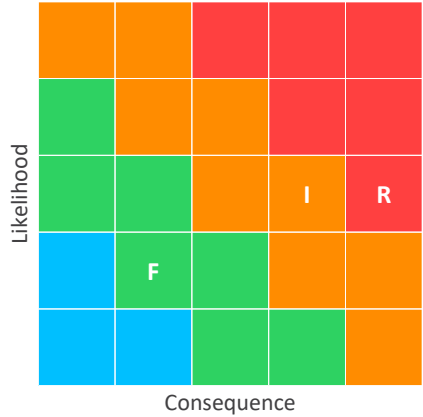
Responsible person: Andrew James

Last Reviewed Date:

Next Review Date:

Organisation > Corporate Strategy

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

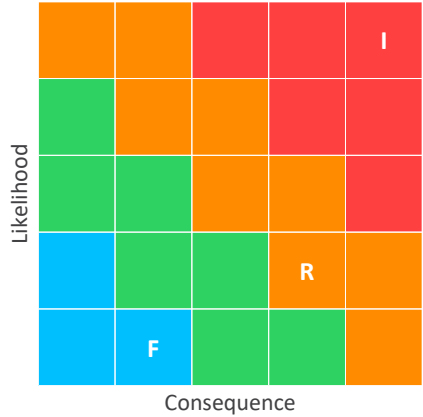
Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
PR24	Estimates are inaccurate	Andrew James	01 Jun, 2022	High	Extreme	Moderate	N/A	

Users don't adopt the system			
Risk Category: Service Delivery	Responsible person: James Best	Last Reviewed Date:	Next Review Date: 26 Apr, 2022

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite

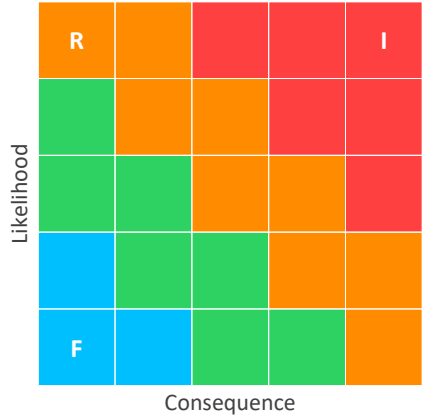


Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Timeline slippage			
Risk Category: Provision of Service / Performance	Responsible person: Shannon Roma	Last Reviewed Date:	Next Review Date: 19 Apr, 2022

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Good – Controls Working Effectively
F	N/A

Risk Appetite

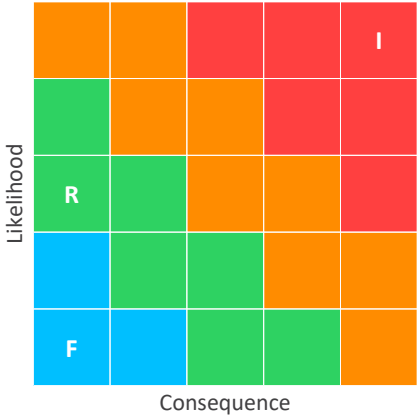


Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Staff leaving during implementation			
Risk Category: Financial (Revenue & Costs)	Responsible person: Riccardo Melton	Last Reviewed Date:	Next Review Date: 12 May, 2022

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Good – Controls Working Effectively
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

PR1

Low Product quality and safety from the third party vendors

Risk Category: Environmental

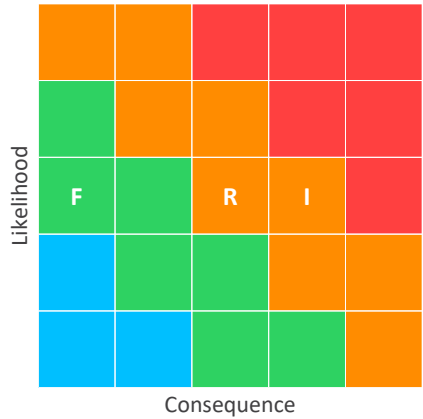
Responsible person: Madeline Jones

Last Reviewed Date: 02 Mar, 2022

Next Review Date: 24 May, 2022

Organisation > Corporate Strategy > Finance > Accounts Receivable

Individual Heatmap



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
VT - 6	Changes in firewall configuration within the IBM Cloud	Vulnerability	20 Jan, 2022	Andrew James	Open
VT - 8	Birthday attacks against TLS ciphers with 64bit block size vulnerability	Vulnerability	20 Jan, 2022	Jack Watts	Open

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



PR1

Branch Staff exposed to other types of hospital claims other than public hospital claims

Risk Category: Business Continuity

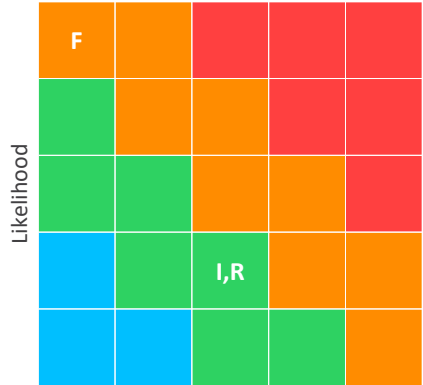
Responsible person: Andrew James

Last Reviewed Date: 27 Sep, 2019

Next Review Date: 27 Dec, 2019

Organisation > Corporate Strategy > Finance > Accounts Receivable

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Good – Controls Working Effectively
F	N/A

Risk Appetite



Existing Risk Controls

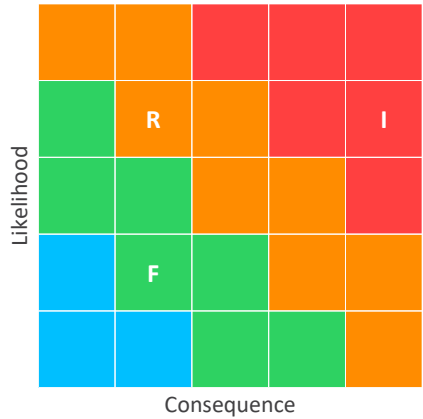
Control Title	Control Owner	Control Owner Rating	Next Review Date
E5 permissions only allowing access to public hospital claims	Joe Smith	Substantially Effective	13 Jul, 2022
New HAMBs role set with permissions restricted to public hospital claims	Joe Smith	Partially Effective	30 Oct, 2019

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR6	An unsafe working environment leading to accidents and possible injury to people and staff	Elizabeth McMahon	08 Jul, 2022	Extreme	Low	Moderate	N/A	

PR-1Scope Creep			
Risk Category: Environmental		Responsible person: Jack Watts	Last Reviewed Date:
			Next Review Date: 12 Apr, 2023
Organisation > Corporate Strategy > Finance > Accounts Payable			

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

PR2

Inappropriate overriding of assessing messages

Risk Category: Service Delivery

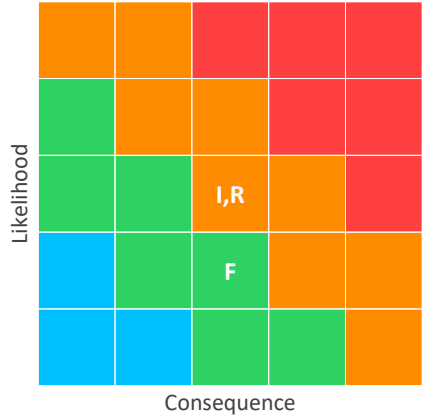
Responsible person: Andrea West

Last Reviewed Date: 19 Jan, 2021

Next Review Date: 27 Oct, 2021

Organisation > Corporate Strategy > Finance > Accounts Receivable

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR7	Failure of critical Enterprise ICT System(s) and / or Application (s)	Joe Smith	21 Apr, 2022	High	High	High	Moderate	
SR2	Change in Industry conditions leads to financial loss	Michelle Jonas	31 May, 2022	Extreme	High	Moderate	High	

PR-2

Staff leaving during implementation

Risk Category: Financial (Revenue & Costs)

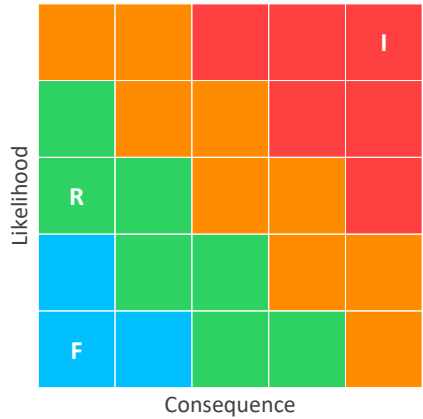
Responsible person: Riccardo Melton

Last Reviewed Date:

Next Review Date: 12 May, 2022

Organisation > Corporate Strategy > Finance > Accounts Payable

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Good – Controls Working Effectively
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

PR3

Employee data being hacked by an unauthorized access

Risk Category: Business Continuity

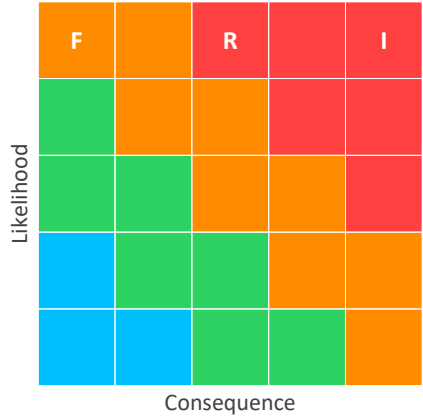
Responsible person: Madeline Jones

Last Reviewed Date: 11 Aug, 2020

Next Review Date: 18 Aug, 2020

Organisation > Corporate Strategy > Finance > Accounts Receivable

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR1	Systems - Unauthorized access to company information	Jack Watts	21 Apr, 2022	High	High	Moderate	High	
OR10	Finance & Administration - Loss or theft of critical information	Jean Pierre	03 Jul, 2022	High	High	Moderate	N/A	

PR3

Incorrect Assessment of Public Hospital Claims

Risk Category: Service Delivery

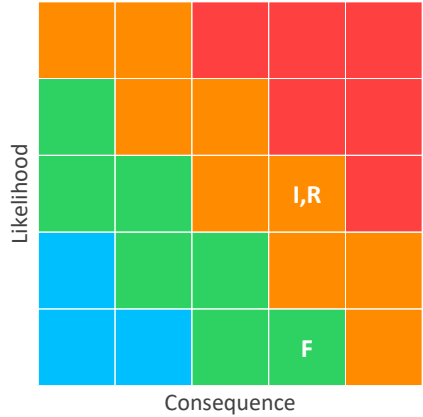
Responsible person: Andrea West

Last Reviewed Date: 18 May, 2022

Next Review Date: 01 Jun, 2022

Organisation > Corporate Strategy > Finance > Accounts Receivable

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Good – Controls Working Effectively
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
VT - 7	Suspicious registry entries within the SAP solution	Vulnerability	28 Jan, 2022	Joe Smith	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
SR2	Change in Industry conditions leads to financial loss	Michelle Jonas	31 May, 2022	Extreme	High	Moderate	High	

PR-3

Users don't adopt the system

Risk Category: Service Delivery

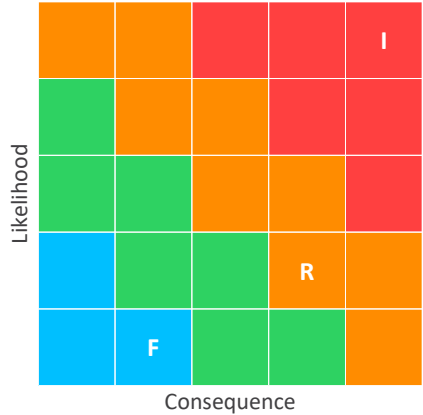
Responsible person: James Best

Last Reviewed Date:

Next Review Date: 26 Apr, 2022

Organisation > Corporate Strategy > Finance > Accounts Payable

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

PR-3

Timeline slippage

Risk Category: Provision of Service / Performance

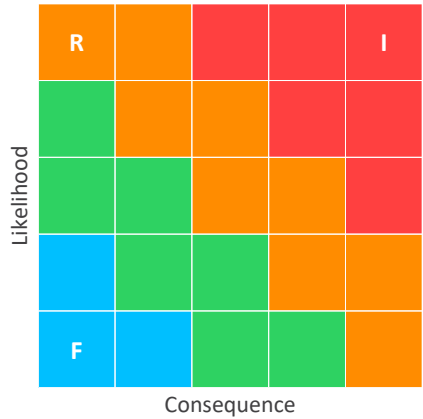
Responsible person: Shannon Roma

Last Reviewed Date:

Next Review Date: 19 Apr, 2022

Organisation > Corporate Strategy > Finance > Accounts Payable

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Good – Controls Working Effectively
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

PR4

Incorrect Payment of Public Hospital Claims

Risk Category: Financial (Revenue & Costs)

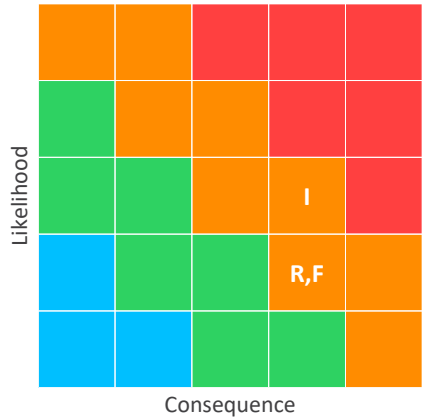
Responsible person: Andrew James

Last Reviewed Date: 17 Sep, 2020

Next Review Date: 17 Oct, 2020

Organisation > Corporate Strategy > Finance > Accounts Receivable

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

PR 20

Inadequate debtor management

Risk Category: Financial (Revenue & Costs)

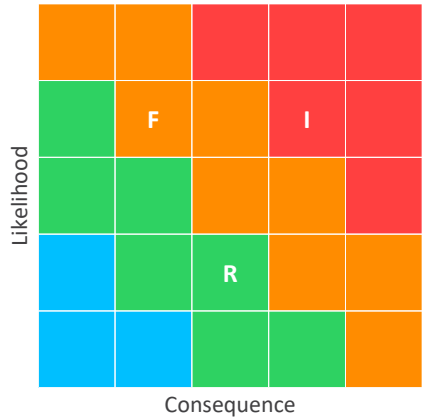
Responsible person: Madeline Jones

Last Reviewed Date: 24 Apr, 2020

Next Review Date: 24 Jul, 2020

Organisation > Corporate Strategy > Finance > Accounts Payable

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite



Causes

- Lack knowledge to the Staff
- Insufficient financial due diligence on target company
- No pre-plan methods were adapted

Consequences

- Legal repercussions and costs
- Delays
- Impact to reputation due to loss of customer information
- Action by regulators
- Unhappy Clients

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR7	Failure of critical Enterprise ICT System(s) and / or Application (s)	Joe Smith	21 Apr, 2022	High	High	High	Moderate	

PR23

Executive turnover disrupts project

Risk Category: Provision of Service / Performance

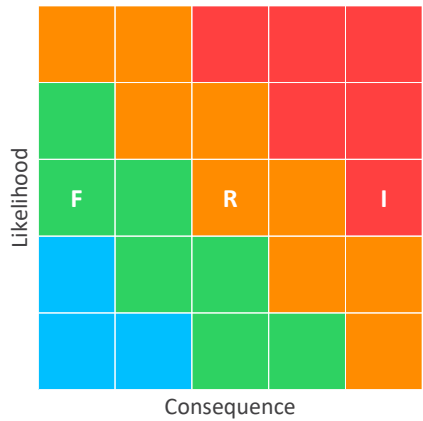
Responsible person: Jack Watts

Last Reviewed Date: 18 May, 2022

Next Review Date: 18 Jun, 2022

Organisation > Marketing > PR and Branding > Brand

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Inability to guarantee rebranding success	Andrew James	In Progress	9	01 Jun, 2021	N/A	RED
Incorrect marketing perception	Michelle Jonas	Completed	100	05 Feb, 2021	N/A	GREEN
Marketing resource deficiency	Andrew James	In Progress	50	15 Mar, 2021	N/A	RED
Reallocation of funds	Michelle Jonas	Completed	63	30 Apr, 2021	N/A	GREEN

Incidents

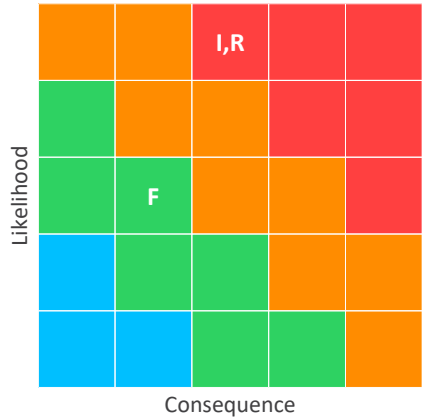
Code	Title	Type	Reported Date/Time	Responsible Officer	Status
BI - 12	Noted failure to report a fraudulent transaction	Incident	08 Nov, 2021	Jack Watts	Open
HAZ - 10	Lifting matts at pedestrian crossing	Hazard	05 Apr, 2017	Andrea West	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
SR7	Insider Trading	James Best	17 Sep, 2022	Extreme	Moderate	Low	High	

<div>PR23</div> <div>Executive turnover disrupts project</div>				
Risk Category: Provision of Service / Performance		Responsible person: Jack Watts	Secondary Risk Owner(s): Elizabeth McMahon	Next Review Date: 16 Dec, 2021
Last Reviewed Date:				
Organisation > Marketing > PR and Branding > Brand				

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

PR24

Estimates are inaccurate

Risk Category: Financial (Revenue & Costs)

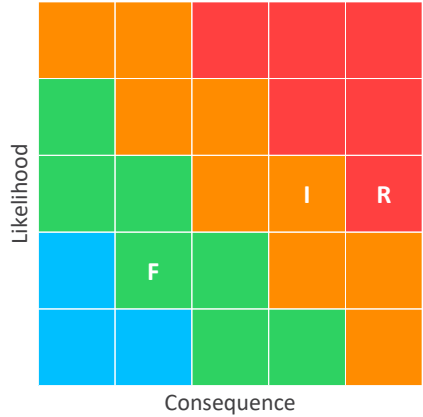
Responsible person: Andrew James

Last Reviewed Date: 18 May, 2022

Next Review Date: 01 Jun, 2022

Organisation > Marketing > PR and Branding > Brand

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Providing accurate estimates	Jack Watts	In Progress	1	03 Jan, 2020	N/A	

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
	Corporate Strategy - Estimates are inaccurate	Andrew James		High	Extreme	Moderate	N/A	

PR25

Project team misunderstand requirements

Risk Category: Service Delivery

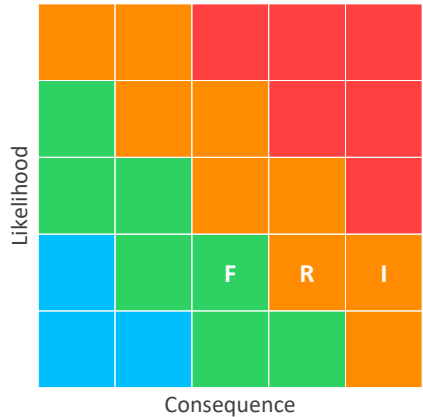
Responsible person: Jack Watts

Last Reviewed Date: 24 Apr, 2020

Next Review Date: 24 May, 2020

Organisation > Marketing > PR and Branding > Brand

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Good – Controls Working Effectively
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Procedures and guidelines with regard to the work	Riccardo Melton	Fully Effective	15 Apr, 2021
Provision of 'global' resource pool, to accommodate for fluctuations in demand across various teams	Elizabeth McMahon	Partially Effective	18 May, 2022

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Enlighten the team with the exact requirement.	Andrew James	Completed	100	03 Jan, 2020	N/A	<div><div></div><div></div><div></div></div> GREEN

PR25

Project team misunderstand requirements

Risk Category: Service Delivery

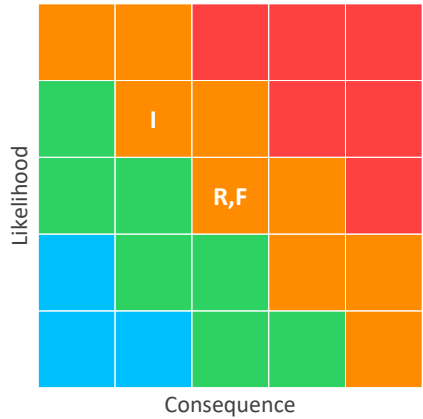
Responsible person: Jack Watts

Last Reviewed Date:

Next Review Date: 29 Nov, 2021

Organisation > Marketing > PR and Branding > Brand

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Good – Controls Working Effectively
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

PR 56

Budget Constraints

Risk Category:

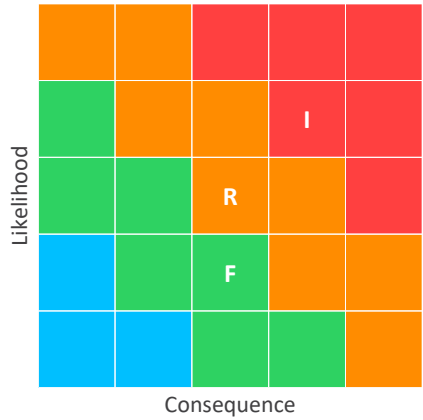
Responsible person: Madeline Jones

Last Reviewed Date: 18 May, 2022

Next Review Date: 18 Jun, 2022

Organisation > Sales > APAC > Western

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

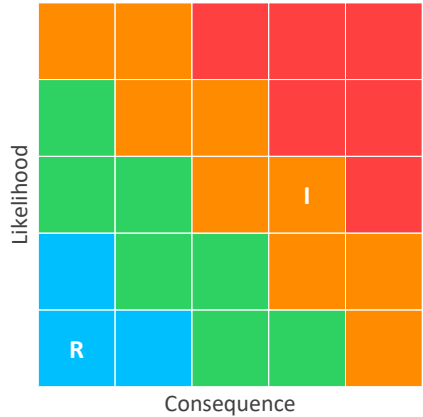
Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
OR8	Failure to appropriately implement business continuity program/policy	Michelle Jonas	08 Apr, 2022	High	Moderate	Moderate	High	

Corporate

IT1	Frequent inability to meet sprint deliverables				
Risk Category: Business Continuity		Responsible person: Riccardo Melton		Last Reviewed Date: 24 Apr, 2020	Next Review Date: 24 Apr, 2021

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Excellent – Controls Working Effectively
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
SR2	Change in Industry conditions leads to financial loss	Michelle Jonas	31 May, 2022	Extreme	High	Moderate	High	
SR3	Efficiency caused by procedural flexibility	Elizabeth McMahon	10 May, 2022	Extreme	Extreme	Moderate	High	

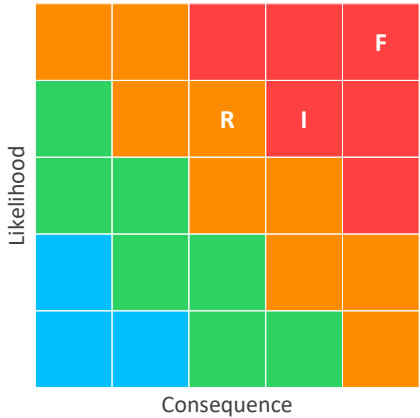
IT2

Unauthorised access of data stored in our internal systems

Risk Category: Provision of Service / Performance, Service Delivery	Responsible person: Jack Watts	Secondary Risk Owner(s): Elizabeth McMahon	Last Reviewed Date: 15 Oct, 2020	Next Review Date: 22 Oct, 2020
---	--------------------------------	--	----------------------------------	--------------------------------

Organisation > Corporate Strategy

Individual Heatmap



Causes

- Insufficient IT security management
- PCs still provide local admin access
- Providing the flexibility to work-from-home

Consequences

- Disruption to business operations
- Penalty payments and legal liabilities
- Impact to Brand Image
- Hardware Impacts

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Ongoing implementation of restricted user access practices, limited to specific functions of a given role	Elizabeth McMahon	Fully Effective	30 Nov, 2022
Employment of third party security vendor, to monitor systems 24/7	Joe Smith	Substantially Effective	26 May, 2020

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Develop and Implement policies to address the risk of people bringing personal devices to work.	Madeline Jones	In Progress	60	11 May, 2020	N/A	RED
Encryption to be installed on all company laptops, mobile devices and removable media	Elizabeth McMahon	In Progress	75	17 Oct, 2020	N/A	RED
Implement and enforce a policy prohibiting employees from keeping working papers, passwords or any sensitive documents in view while they are away from their desks	Andrea West	In Progress	67	31 Jul, 2021	N/A	RED
Train employees on the various techniques used by fraudsters, such as “phishing” and “smishing” and to never open attachments or download anything from an unknown source.	Andrea West	Completed	100	24 May, 2020	N/A	GREEN

IT2

Unauthorised access of data stored in our internal systems

Risk Category: Provision of Service / Performance, Service Delivery

Responsible person: Jack Watts

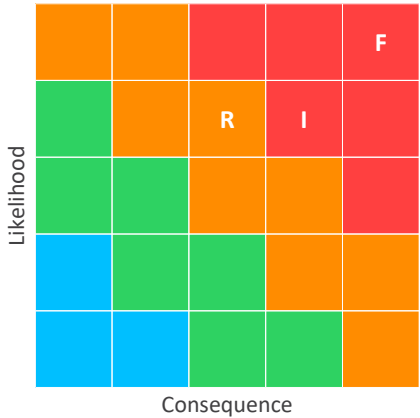
Secondary Risk Owner(s): Elizabeth McMahon

Last Reviewed Date: 15 Oct, 2020

Next Review Date: 22 Oct, 2020

Organisation > Corporate Strategy

Individual Heatmap







- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite








KPIs

KPI Name	KPI Unit	Owner	Actuals	Target	Performance
# of returning IT issues	#	Joe Smith	1.00	1.00	 GREEN
# of cyber attacks	#	Joe Smith	2.00	4.00	 GREEN
# of Critical IT system related issues	#	Joe Smith	651.00	617.00	 RED
# of IP loss incidents	#	Jack Watts	55.00	45.00	 RED

Incidents

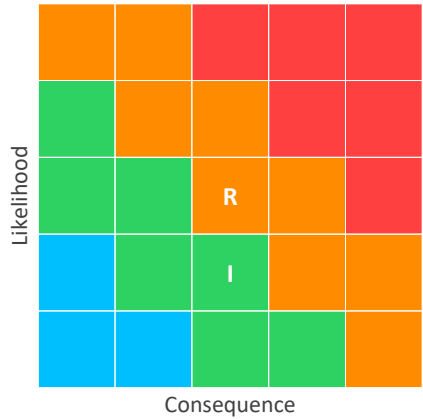
Code	Title	Type	Reported Date/Time	Responsible Officer	Status
BI - 4	Emailing of inappropriate information to staff without sufficient security privileges	Business Incidents	03 Jul, 2018	Madeline Jones	Open
BI - 5	The system was access by an unauthorised third party	Business Incidents	03 Sep, 2020	Elizabeth McMahon	Open
BI - 7	Data Loss arising from IT System Malfunction	Incident	09 Oct, 2019	Tom Jones	Open
VT - 1	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	Vulnerability	05 Jan, 2022	Madeline Jones	Open
VT - 3	Anomalies in outbound network traffic within the Azure Server	Vulnerability	20 Jan, 2022	Andrew James	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
SR6	Intellectual Property Theft	Elizabeth McMahon	25 Mar, 2022	 Extreme	 High	 Moderate	 High	

IT3Critical Infrastructure Failures			
Risk Category: Financial (Revenue & Costs)		Responsible person: Elizabeth McMahon	Last Reviewed Date: 11 Aug, 2020Next Review Date: 11 Sep, 2020
Organisation > Operations and IT			

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
N/A			

IT4

Completed projects shortchanging security and controls

Risk Category: Business Continuity

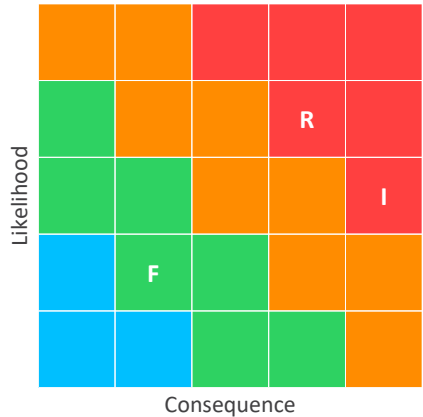
Responsible person: Jack Watts

Last Reviewed Date: 18 May, 2022

Next Review Date: 18 Aug, 2022

Organisation > Corporate Strategy

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Good – Controls Working Effectively
F	N/A

Risk Appetite



Causes

- Lack knowledge to the Staff
- Lack of controls that reach the legal and regulatory standards

Consequences

- Legal repercussions and costs
- Impact of other future investments and acquisitions
- Unhappy Clients

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
LexisNexis Database	Joe Smith	Substantially Effective	07 Jun, 2019
Proper knowledge on handling the legal and regulatory compliance.	Susan Wright	Partially Effective	09 Jan, 2020

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Implementation of a Compliance management system	Jack Watts	In Progress	51	29 Feb, 2020	N/A	<div><div></div><div></div><div></div></div> RED

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
VT - 4	Traffic sent to or from unknown locations in the US AWS server	Vulnerability	13 Jan, 2022	Susan Wright	Open

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
SR3	Efficiency caused by procedural flexibility	Elizabeth McMahon	10 May, 2022	<div></div> Extreme	<div></div> Extreme	<div></div> Moderate	<div></div> High	<div></div>

ITS

Failure to comply with corporate IT policies and controls

Risk Category: Business Continuity

Responsible person: Andrea West

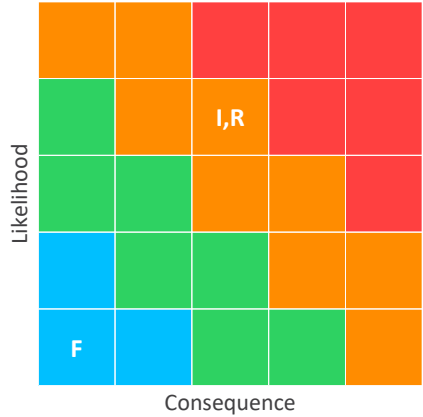
Secondary Risk Owner(s): Joe Smith

Last Reviewed Date: 18 May, 2022

Next Review Date: 25 May, 2022

Organisation > Legal & General

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Marginal – Controls Require Improvement
F	N/A

Risk Appetite



Causes

- Failure to comply with corporate IT policies and controls
- Reduced enterprise IT support

Consequences

- Regulatory violations
- Multiple “shadow IT” organizations within enterprises, Shadow groups tend to not follow established control procedures

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Monitor and Control duplicative systems, licensing, and support issues.	Andrew James	Substantially Effective	04 May, 2020

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Engage with an expert consultant for guidance.	Elizabeth McMahon	In Progress	64	14 Aug, 2021	N/A	<div><div></div><div></div><div></div></div> RED

Risks

Risk Code	Risk Title	Responsible person	Next Review Date	Inherent	Residual	Future	Aggregated Residual	Link Type
SR6	Intellectual Property Theft	Elizabeth McMahon	25 Mar, 2022	<div><div></div></div> Extreme	<div><div></div></div> High	<div><div></div></div> Moderate	<div><div></div></div> High	<div><div></div></div>

IT6

Failure to appropriately implement business continuity program/policy

Risk Category: Business Continuity

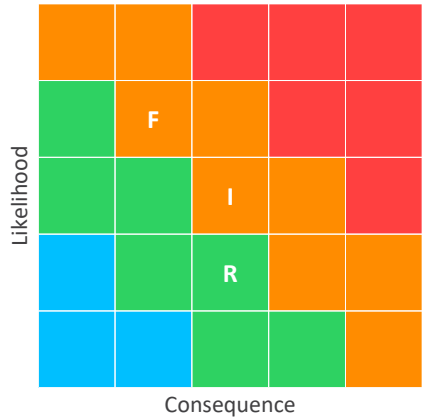
Responsible person: Madeline Jones

Last Reviewed Date: 27 May, 2020

Next Review Date: 27 Jun, 2020

Organisation > Sales

Individual Heatmap



- I Inherent Risk Assessment
- R Residual Risk Assessment
- F Future Risk Assessment

Effectiveness of control	
I	N/A
R	Fair – Controls Require Improvement
F	N/A

Risk Appetite



Causes

- Insufficient IT security management
- Reduced enterprise IT support
- Weak project management oversight

Consequences

- Disruption to business operations
- Regulatory violations

Existing Risk Controls

Control Title	Control Owner	Control Owner Rating	Next Review Date
Insufficient resources available to perform work	Joe Smith	Partially Effective	03 Jan, 2020

Risk Actions

Risk Action Title	Responsible Officer	Action Status	% Completed	End Date	Revised End Date	Performance
Build controls into projects	Madeline Jones	In Progress	10	14 Aug, 2021	N/A	<div><div></div><div></div><div></div></div> RED

Incidents

Code	Title	Type	Reported Date/Time	Responsible Officer	Status
BI - 1	A networking device crashes, bringing down several services	Business Incidents	26 Nov, 2020	Clarke Chan	Open



| cammsrisk

The entire contents of this document are subject to copyright with all rights reserved. All copyrightable text and graphics, the selection, arrangement and presentation of all information and the overall design of the document are the sole and exclusive property of CAMMS. Copyright © 2017 CAMMS. All rights reserved.