SWINBURNE AUSTRALIAN GRADUATE SCHOOL OF ENTREPRENEURSHIP

Faculty of Business and Enterprise

Assignment Cover Sheet for Postgraduate Courses

(for individual and group assignments)

This cover sheet is to be attached to all assignments, both hard copy and electronic format.

STUDENT(S) DETAILS					
	Student 1	**Student 2**	**Student 3**	**Student 4**	**Student 5**
Student ID Number(s)	4917561	100666059	179695X	100671354	
Family Name(s)	Fulham	Gopathi	Sharma	Bhardwaj	
Given name (s)	Thomas	Srinath	Gagan	Srinivas	

PROGRAM TITLE

SUBJECT DETAILS			
Subject Code	INF80043	**Subject Title**	IS-IT Risk Management
Lecturer's Name	Adi Prananto		

ASSIGNMENT DETAILS			
Title or Topic Addressed	Organix IS/IT Risk Assessment		
Due Date	19/10/2016	**Date Received**	16/10/2016

DECLARATION

1. I/We hold a photocopy or electronic copy of this assignment which can be produced if the original is lost/damaged;
2. To the best of my/our belief, no part of this assignment has been copied from any other student's work or from any other source except where acknowledgement is made in the text;
3. No part of this assignment has been written for me/us by any other person except where such collaboration has been authorised by the lecturer concerned and where acknowledgement is made in the text;
4. No part of this assignment has been previously submitted as an assessable item, except where authorised by the lecturer concerned and where acknowledgement is made in the text;
5. **SAFE ASSIGN: For units where Safe Assign facility is available in the Blackboard site**

   1/we declare that this assignment has been submitted to Safe Assign, both in draft and final form, and all identified matches and referencing have been checked and corrected.

☒ I / We accept that electronic submission of this cover sheet will be taken as consent to the terms outlined in Points 1 to 4 of the above declaration by the student/submitting this assignment.

Student Signature(s)	Thomas Fulham	Srinath Gopathi	Gagan Sharma	Srinivas Bhardwaj	

MARKER'S MAIN COMMENTS

Marker's Signature	**Date**	**Grade/Mark**	

Organix
Enterprise Systems Risk Management Review

Author: Thomas Fulham, Srinath Gopathi, Gagan Sharma, Srinivas Bhardwaj
Date: 16th October 2016

Table of Contents

1. Executive Summary

Following tabled directive 1.6 of the Executive Leadership Team (ELT) September 2016 quarterly meeting, a thorough Enterprise Systems Risk Review was commissioned in response to concerns raised around organisational arrangements regarding the effective management of risk associated with Organix enterprise infrastructure, hardware, software and its ability meet current and future demands to support the Organix business in its next stage of growth.

The following report has been produced in consultation with a cross section of organisational representatives. The task force wishes to acknowledge the cooperation and assistance of the following departments;

- Information, Communication & Technology (ICT)
- Research & Development (R&D)
- Logistics & Supply
- Retail
- Business Development/ Global Expansion

This report was developed as per the terms of reference provided to the Enterprise Risk Review team and is not an exhaustive risk assessment of all Organix Risks rather a targeted assessment within the scope of those elements of the Organix business that rely on or could be impacted by Organix enterprise system arrangements.

We believe, the current Risk position of the Organix business has not been driven by failure of processes, rather a normalisation of the risk associated with the organisations undertaking during a period of consistent expansion and growth. (Meigs, 2016) This reports mark a turning point in Organix approach to managing IS/IT related risks and provides practicable controls that encourage proactive action to mitigate the impact these threats present to Organix business.

Key control proposals are identified in section 6 in addition to a comprehensive risk register contained in Appendix 9.1. Key Threat sources identified include;

- Introduction of non-certified products or techniques In the supply chain
- Manipulation of legacy virtual private network (VPN) infrastructure between Organix and supply chain partners
- Absence of internal capability to maintain and develop Organix enterprise applications

During the risk assessment process, a number of risks were identified that appeared to have poor or nil controls implemented to mitigate the impact in the event of occurrence. In the interest of business continuity, immediate actions were undertaken to implement appropriate controls or isolate the risk until appropriate controls could be implemented.

Enclosed within this report are a number of immediate actions submitted for ELT approval in addition to a number of recommendations for subsequent risk assessment activities to ensure the longevity and integrity of the Organix business is secured.

2. Organisational Introduction

Organix is a medium sized organic supplement and health food manufacturer founded in 1995 with operations in Australia, New Zealand and the broader Asia Pacific Region. Organix directly employees approximately 107 employees across R&D, Marketing & Sales, Accounts & Finance, Contract & Vendor Management, Business Information Systems, Logistics Management and a further indirect workforce within two independent contract manufacturing entities.

Orgnanix annualised revenue exceeds 180 million dollars per annum with recent multiplied earnings valuing the Organix business in excess of 1.08 billion dollars. Organix has recently revised its longer term strategy and has placed the distribution markets of North America, Europe and Japan in its sites supported by launching an Initial Public Offering (IPO) within the next three years.

To further support its expansion, Organix is also considering the diversification of its product offering by launching products targeting niche positions within the broader snackfood category. Key to the success of Organix has been its ability to foster genuine relationships with its suppliers, distributors and customers to a lesser extent and its stable brand image projecting a 100% certified organic food and supplement point of difference.

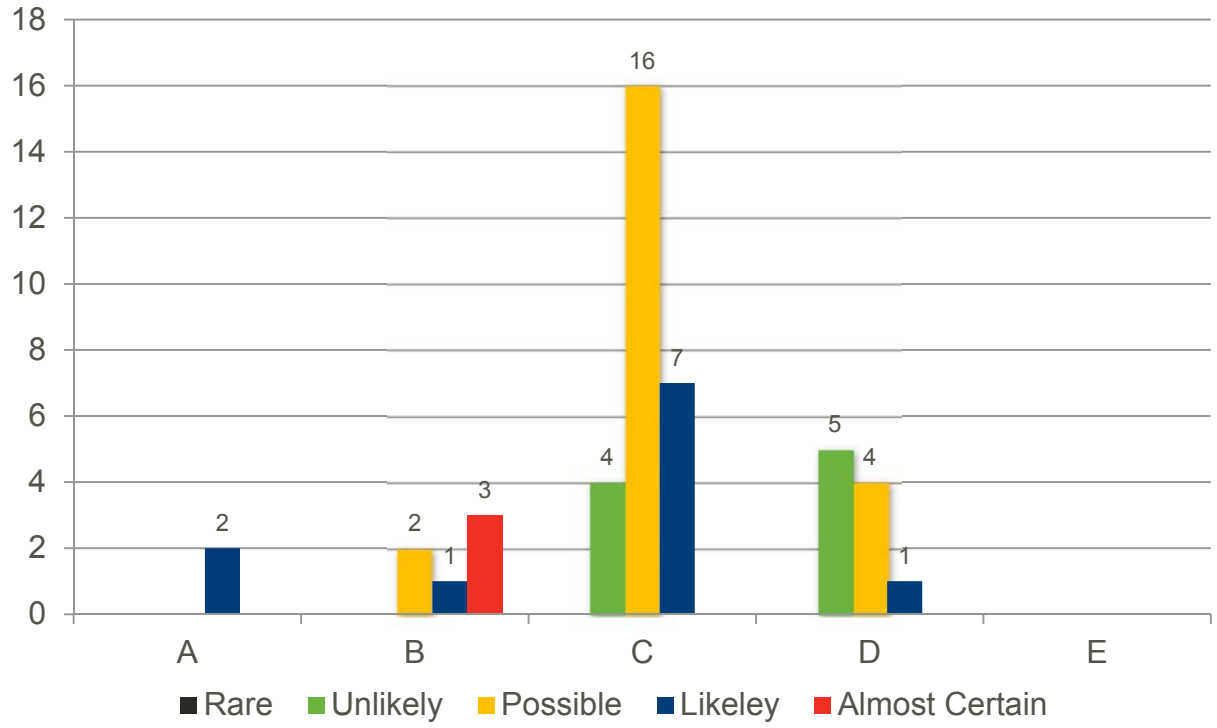
Within the Information Technology function, Organix suite of enterprise applications are well entrenched with many implemented shortly after Organix inception in 1995. Although these applications have adapted to met business requirements for over a decade, advancements in technology combined with Organix revised business strategy and complex international supply chain has meant the Organix Enterprise applications are failing to meet business needs and in turn there obsoleteness is exposing the Organix business to higher than acceptable risks.

3. Risk Review Snapshot

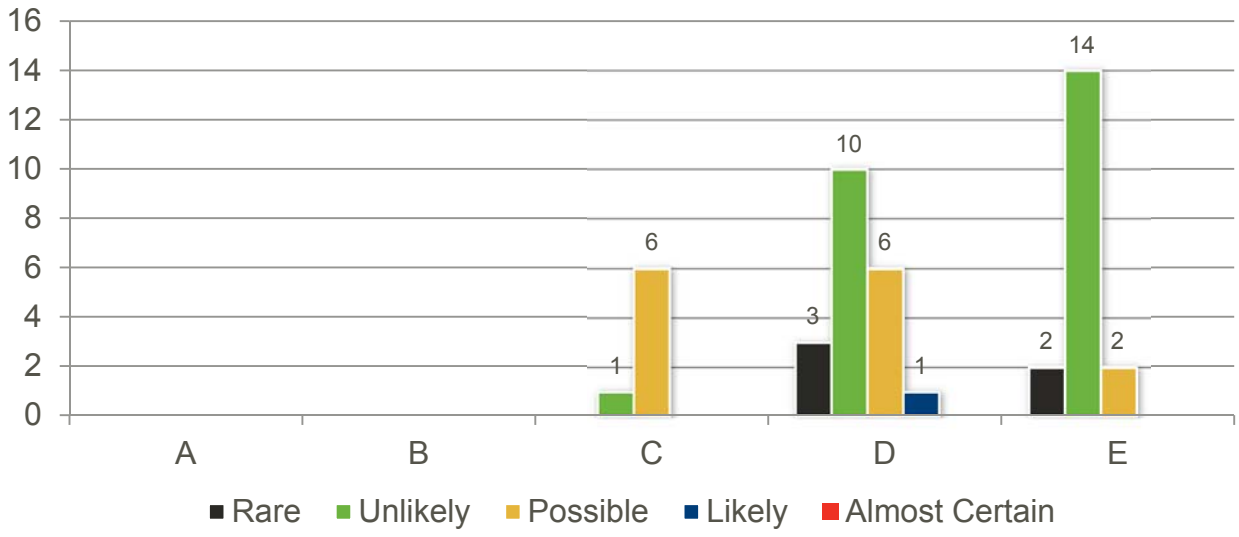
The following graphs provide an executive overview of Organix risks identified by the task force both before controls are implemented (2.1) and after implementing the proposed controls (2.2) included in this report.

Risks are rated in terms of impact: 'A' being Very High/ Almost certain through to 'E' Very Low/ Rare. (National Insitute of Standards and Technology, 2012). The objective of this process is to ultimately drive the potential impact of these risks as far to the right as possible. Further information on Risk Impact classification is included in section 4.

3.1. Inherent Risk Profile (uncontrolled)



3.2. Residual Risk Profile (proposed controls implemented)



4. Framing our Risk Management Approach

An organisations ability to identify, assess and contextualise risk is key to ensuring organisational success. The Enterprise Risk Review Team in determining the normalised risk assessment approach and method consulted the following industry and globally recognised standards;

- AS/NZS ISO 31000 Risk Management – Principles and guidelines
- SP 800-30 Guide for Conducting Risk Assessments
- ISO 27010 Security Techniques for Information Security for inter-organisational communications

The intent of the normalised risk assessment approach is to provide a meaningful method of risk assessment and identification for the Organix business and in turn identify the effectiveness of controls implemented in order to ascertain a realistic indication of the Organix residual risk profile. This approach is aligned to the principles of risk management (Standards Australia, 2009);

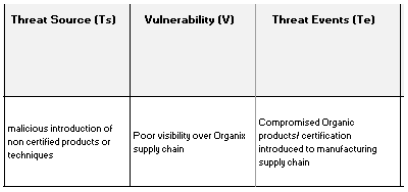
1. Risk Assessment & Evaluation
2. Cost Benefit Analysis
3. Cost of protection does not outweigh benefit
4. No unnecessary risk is accepted into the Organix business
5. Appropriate authorisation structure Risk Acceptance

Risks were identified, evaluated and treated using the following process;

Threat Source, Events, Vulnerabilities	•The identification of the Threat and how it could be introduced to the Organix business
Department Owner	•The functional owner of the Risk, this helps to provide context to Risk profile of the Organix business
Consequance Type	•In the event of the threat event occuring, what would be primary imapct to the Organix Busines. e.g: Management Impact, Budget, Reputation & Community
Immpact	•Attributing an overal rating to the Risk by evaluating it against two attributes: Consequance of Occurance and Liklihood of occurance. These two attributes are guided by both qualitative and quantitative perspectives
Control Requirements	•Identification of suitable controls to be implemented in order to lower the consequance and/or liklihood of the threat event occuring
Residual ImpactRating	•Attributing an overal rating to the Risk after the controls have been implimeneted. This is evaluated against two attributes: Consequance of Occurance and Liklihood of occurance. These two attributes are guided by both qualitative and quantitative perspectives.
Action	•Following the identification of Residual Risk, actions include seeking approrpiate approval for Risk acceptance and implementation of controls and other governance activites

The following provides an overview of the Risk Assessment tool and how risks were captured and evaluated for this report.

1. Input Threat Source (Ts), Vulnerability (V), Threat Event (Te)

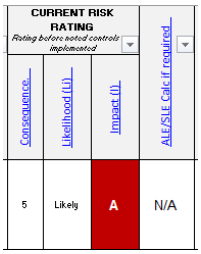


Threat Source (Ts)	Vulnerability (V)	Threat Events (Te)
malicious introduction of non certified products or techniques	Poor visibility over Organix supply chain	Compromised Organic products/ certification introduced to manufacturing supply chain

2. Identify functional department owner & consequence category (most impacted by risk occurrence)

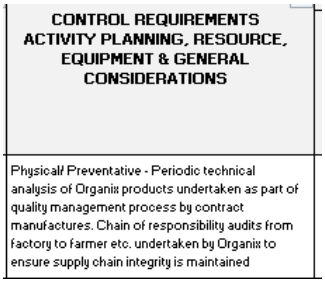
Department Owner R&D, Logistics & Supply, Retail, Business Development/ Global Expansion, All	Select. Conseq Type
Logistic & Supply	Reputation & Community

3. Evaluate the risk consequence and likelihood (Li) in its current uncontrolled state. The Risk register will then provide an overall impact (I) based on the defined matrix included in section 4. An ALE can also be nominated to be completed.



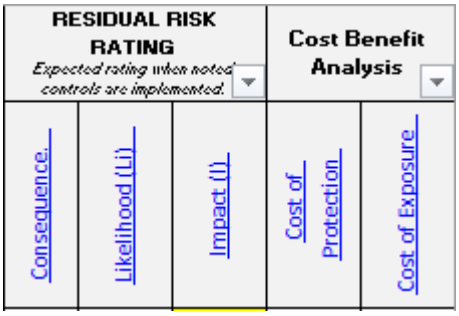
CURRENT RISK RATING *Rating before noted controls implemented*			
Consequence	Likelihood (Li)	Impact (I)	ALE/SLE Calc if required
5	Likely	A	N/A

4. This section captures proactive controls that can be implemented to reduce the overall impact of the risk occurrence. Control categories used are defined below.



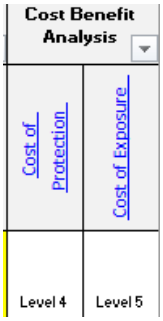
CONTROL REQUIREMENTS ACTIVITY PLANNING, RESOURCE, EQUIPMENT & GENERAL CONSIDERATIONS
Physical/ Preventative - Periodic technical analysis of Organix products undertaken as part of quality management process by contract manufactures. Chain of responsibility audits from factory to farmer etc. undertaken by Organix to ensure supply chain integrity is maintained

5. With controls in mind, the risk consequence and likelihood (Li) is re-evaluated. The Risk register provides revised overall impact (I) based on the defined matrix included in section 4.



RESIDUAL RISK RATING *Expected rating when noted controls are implemented*			Cost Benefit Analysis	
Consequence	Likelihood (Li)	Impact (I)	Cost of Protection	Cost of Exposure

6. A Cost Benefit Analysis (CBA) is conducted to ensure the cost of protection/ mitigation associated with implementing the control does not outweigh the cost of exposure. This provides management with a ready 'litmus' test when prioritising which controls to implement. See below for CBA scale.



Cost Benefit Analysis	
Cost of Protection	Cost of Exposure
Level 4	Level 5

This report covers an extensive list of risks associated with Organix business. The risk register appendix 9.1 was used systematically to outline the threat source, vulnerability associated with the risk and parameters that could provoke a threat event occurrence. The risk register is also used to highlight the likelihood and the impact on the business in terms of quantitative & qualitative values (International Standards Organisation, 2009) depending upon the severity of the risk. This risk register is founded on the following principle;

Threat Source (Ts) * Vulnerability * Threat event (Te) * Likelihood (L) * Impact (I) = Risk (Prananto, 2016)

4.1. Impact Definitions

The following risk matrix was established by the task force to provide suitable qualitative and quantitative context to identified risks and impact (I)

Impact (I)	Definition
A – Very High/ Almost Certain	Attributed to a risk that presents significant disruption to the Organix Business typically in excess of 10% of the business revenue, significant regulatory penalties or threatens the continuity of the Organix business.
B – High/ Likely	Presents reasonable risk to the continuity attracting attention from the media, regulator investigation, deployment of the Disaster Response Plan (DRP)
C – Moderate/ Possible	Elevated risk falling outside of BAU controls requiring the effective implementation of specific controls to prevent damage to the Organix business. These risk typically present a revenue impact up to 5%
D – Low/ Unlikely	Minor impact to the Organix business with most risks effectively controlled with BAU processes.
E – Very Low/ Rare	Considered very minor impacts effectively managed by Business as Usual Controls (BAU)

Note: *Refer to section 4.5 for appropriate risk acceptance hierarchy.*

4.2. Controls

The following control categories were adopted from the PCI Security Standards Council to assist in the consistent formulations of effective controls;

Control effectiveness	Preventative (Highest order control)	Attempt to avoid occurrence of unwanted events
	Detective	Attempt to identify unwanted events after post occurrence
	Deterrent	Discourage individuals from intentional violating information security policies or procedures
	Corrective	Attempt to remedy the circumstances that allowed the unauthorised activity or return conditions to what they were before the event
	Recovery	Restore lost computing resources or capabilities and help the organisation recover monetary loss caused by event occurrence
	Compensating (Lowest order control)	Attempt to reduce the risk that an existing or potential control weakness will result in failure to meet a control objective

4.3. Cost Benefit Analysis Scale

Cost Benefit Analysis Table

Cost of Exposure/ Cost of Protection	Cost Guidance
Level One	$0 - < $9,999
Level Tw o	$10,000 - < $19,999
Level Three	$20,000 - < $29,999
Level Four	$30,000 - < $99,999
Level Five	> $100,000

4.4. Rating Matrix

CONSEQUENCE - RISK					
RATING	**1**	**2**	**3**	**4**	**5**
Information Technology	* Outage/ failure impact to business of less than or equal to 10K	* Outage/ failure impact to business of less than or equal to 20K	* Outage/ failure impact to business of less than or equal to 30K	* Outage/ failure impact to business of less than or equal to 100K	* Outage/ failure impact to business of greater than 100K
Budget ($AUD)	(<1%) of business revenue	(1% to 5%) over business revenue	(3% to 5%) of business revenue	(5% to 10%) of business revenue	Greater than (10%) of business revenue
Time Schedule/ Production Schedule Impact	**(<1% of production)** over the production schedule	**(1% to 2% of production)** over the production schedule	**(2% to 3% of production) over the production schedule**	**(3% to 5% of production)** over the production schedule	**(>5% production)** over the production schedule
Environment & Natural Resources	* Low severity environmental impact(s) or impact on natural resources availablity that are promptly reversible and affected area is within the site boundary	* Nuisance or low severity environmental impact(s) or impact on natural resources availablity that are promptly reversible and affected area is outside the site boundary	* Moderate severity environmental impact(s) or impact on natural resources availablity where the affected area is within the site boundary	Moderate severity environmental impact(s) or impact on natural resources availablity where the affected area is outside the site boundary	High severity environmental impact(s) or impact on natural resources availablity at local scale significance
Workplace Health and Safety	* First aid injury, and/or * Minor safe working issues	* Medical treatment, and/or * Moderate safe working breach likely to impact on operations	* Serious medical / hospital treatment resulting in need alternate working or resulting in lost time injury, and/or * Significant safe working breach with actual impact on operations	* Serious or permanent Injury, and/or * Significant safe working beach with immediate impact on operations on one or more worksites	* 1 or more fatalities, and/or * Major breach of safe working with immediate and extensive impact on one or more worksites
Reputation / Community / Media	* Public concern restricted to local complaints * Lack of contribution to the community	* Minor, adverse local public or media attention and complaints * Employees warned only * Minor change in community amenity values	* Attention from media and/ or heightened concern by local community * Stakeholder action will disrupt planned business activities * Disciplinary action may be taken * Temporary reduced community access to services or employment	* Significant adverse national media / public / NGO attention * Considerable and prolonged adverse community impact and dissatisfaction publicity expressed * Stakeholder action will delay achievement of major elements of the business * Permanently reduced community access to services or employment	* Serious public or media outcry with international coverage * Significant adverse community impact & condemnation * Stakeholder action will prevent achievement of the business objectives * Reduced cohesion of community
Governance / Legal / Regulatory	* Very minor technical breach of regulation or policy or code of ethics. No fine / penalty	* Minor legal issues, non-compliances and breaches of regulation, policy or code of ethics * Enforceable Undertaking	* Moderate breach of regulation, policy or code with investigation or report to authority * Moderate legal proceedings initiated * Several Improvement Notices	* Significant breach of regulation, policy or code with fine or other regulatory action. Significant litigation / legal action * Shut down of part of a business due to regulatory breach * Prohibition Notice	* Major breach of regulation, policy or code with fine * Major litigation * Major investigation by regulatory body * Prosecution / Accreditation loss
Management Impact	* Impact of event absorbed through normal activity	* Will require some local management attention over several days	* Significant event that can be managed with careful attention, will take some business managers much time for several weeks * Local operation of contingency plan	* Major event that requires the implementation of crisis and contingency plans at a business level, regional area or support function (DRP) * Will require the involvement of senior managers and will take up the time of business managers for several weeks	* Critical event or disaster with significant impact on Organix that requires considerable senior management time to handle over several months * Full implementation of an Organix's crisis management plan for days to weeks

PROBABILITY OR CHANCE	QUALITATIVE ASSESSMENT	RECURRENCE TIMEFRAME
≥ 96-100%	Almost certain to occur during the business operations	Less than "Monthly"
80% to 95%	Considered likely to occur during the business operation	"Monthly" to "Yearly"
21% to 79%	Considered a possible occurrence during the business operation	Between 2 and 5 years
5% to 20%	Considered unlikely to occur during the business operation	Between 5 and 20 years
< 5%	Considered a rare occurrence to happen during the business operation	Greater than every 20 years

LIKELIHOOD	CONSEQUENCE					
	RATING	**1**	**2**	**3**	**4**	**5**
	ALMOST CERTAIN/ Very High	D	C	B	A	A
	LIKELY/ High	D	D	C	B	A
	POSSIBLE/ Moderate	E	D	C	C	B
	UNLIKELY/ Low	E	E	D	C	B
	RARE / Very Low	E	E	D	D	C

4.5. Risk Acceptance Authority Levels

The below tables, summaries the appropriate Authority level required to accept risks based on the risks anticipated residual risk rating after controls have been implemented. This table is designed to minimise any instances of unnecessary risk being accepted into the Organix business without first receiving the appropriate oversight required.

Residual risk / opp Rating	Suggested action	Authority to accept or tolerate risk.
A	Take action to eliminate or implement additional controls to reduce it to acceptable level Completion of IS/IT task or activity must not be performed. An alternative solution must be found.	Organix CEO / COO
B	Implement additional controls to reduce The activity or task must not be performed w ithout the explicit concurrence of the Organix CIO	Organix CIO/ General Mgr or EGM / CFO as appropriate.
C	Implement additional controls reduce w here it is cost-effective to do so.	Organix Applications/ Infrastructure Manager / Business Manager
D	Implement additional controls to reduce	Organix Team Leaders
E	Low er priority (likely to be tolerable).	All personnel

5. Internal & External Risks Themes Identified

5.1. Internal Risk Themes

Throughout this risk assessment process, a number of conflict of interests were identified;

- External Back-up provider
- Independent engagement of software as a service providers
- Online Shop & Payment Gateway Vendor

The extent of these conflicts can only be estimated however, it is evident the Organix procurement and vendor qualification and evaluation process is not as effective as it could be. A review of this process in addition to the creation of a Code of Business Conduct will greatly assist the Organix business by setting minimum business standards expected of employees and subcontractors worldwide.

IT focussed training and development opportunities provided to personnel with direct reports may further assist the future stability of the Organix business. By instilling core proficiencies within our people, it is intended situations that have the potential to introduce unnecessary risk to Organix IS/IT infrastructure will be reduced.

5.2. External Industry Risks

As Organix is preparing to expand its international distribution, specific therapeutic and financial regulatory requirements must be satisfied prior to commencing operations within these countries. There have been a number of recent cases within the health food and transport industries that have resulted in local governments actively seeking to limit or prohibit entry to foreign based companies in order to protect domestic product. The following cases are specific to Organix planned expansion within the Chinese market;

Blackmores Takes a hit in the Chinese market (Tasker, 2016)

Blackmores, a well reputed Australian pharmaceutical firm and competitor to Organix first commenced its expansion into the Chinese market in 2014 with the objective of capitalising on the future growth and diversify in the Asian supplement market.

Business was showing strong growth and potential driving the Blackmores share price to unseen heights however, on May 27th 2016 China enforced new regulatory law on the importation of foreign supplement goods meaning companies must pay 11.9 per cent on goods, on top of the law that has been enforced on April 8th which subjectively eliminates the advantage held by offshore websites.

This has significantly impacted Blackmores share price resulting in an 18 per cent decrease in the first two days of the new tax regulation taking effect.

Uber Trying to Enter Chinese market (Wall Street Journal, 2016)

Uber recently attempted to enter the Chinese market through acquisition of a smaller local competitor Didi Chuxing Technology. Whilst gaining the appropriate approvals from the Foreign Investment Review Board, the application was speedily struck out and allegations of Anti-Trust logged against Uber resulting in the planned acquisition being aborted.

6. Proposed Risk Control Strategy Execution

The following represent key priority risks that require immediate attention. Risks have been grouped in stages with indicative costing provided for implementation of controls. Scale of economies could be realised by grouping similar risk control measures and implementing simultaneously.

6.1. Stage One (Key Class A & B Risks)

Register No.	Risk	Control Requirements
1	Compromised Organic products/ certification introduced to manufacturing supply chain	**Technical/ Preventative** - Periodic technical analysis of Organix products undertaken as part of quality management process by contract manufactures. **Physical/ Detective** - Chain of responsibility audits from factory to farmer etc. undertaken by Organix to ensure supply chain integrity is maintained.
10	Compromised network infrastructure/ access	**Detective/ Technical** - Inbound data logging could be configured to detect unusual traffic patterns. This could be further eliminated through limiting traffic to those emanating from specific cod/ retailer suppliers.
17	Inadequate encryption of VPN connection between Organix & CMD	**Preventative/ Technical** - Implementing the secure two step verification methodology using appropriate technological control.
32	Intricate details of back up facility openly published on vendor website	**Recovery/ Administrative** – Assess exposure/extent of compromised privacy. If deemed severe, commerce selection process for new vendor immediately. **Preventative/ Administrative** - Establish clear operating and non-disclosure requirements with vendor.
33	Conflict of interest between IS/IT Management & third party suppliers (back up)	**Compensating/ Administrative** - Competitive tender process undertaken to ensure best value add vendor selected. **Preventative/ Administrative** – Implementation of Code of Business conduct clarifying Organix position on engaging vendors.
34	Organix HQ targeted in physical attack harming Data Centre	**Detective/ Physical** - Security of the data centre should be sophisticated as such that only people with permits allowed into data centre.
36	Absence of internal capability to maintain and develop Organix enterprise applications	**Corrective/ Technical** - Employees should be well trained and certificated.
37	Inadequate Monthly Data Backup regime	**Recovery/ Technical** - Data backup frequency must increase from once monthly to once every two days mitigating the consequence of total loss occurrence.

Maximum Anticipated Cost of Implementation to address Stage One Risks $570,000

6.2. Stage Two (Key Class C Risks)

Register No.	Risk	Control Requirements
2	Unauthorised removal of equipment by staff, contractors and visitors	**Preventative/ Administrative** - Establish comprehensive asset register, conducting periodic audits to ensure shrinkage in asset base is minimal. **Preventative/ Administrative** - Provide training, signage and reference information to personnel issued with company assets on the important of securing equipment when left unattended. **Deterrent/ Physical** - install alarms and surveillance throughout building and asset rooms to prevent malicious harm. **Recovery/ Operational** - Equip portable/ mobile assets with remote wipe capabilities.
11	HQ Data centre hardware failure undermines system integrity	**Preventative/ Technical** - Robust lifecycle, hardware refreshment schedule developed to prevent data centre failures. **Recovery/ Technical** - Robust back up regime implemented to ensure any loss of data centre functionality is mitigated. **Recovery/ Technical** - Additional Data Centre established to ensure seamless fail over of Organix enterprise systems minimising any business disruptions. **Recovery/ Administrative** - Disaster Recovery Plan Implemented to ensure effective management of data centre outage.
15	Reputation Risk	**Preventative/ Administrative**: Creating, implementing and auditing a well-defined social media policy across the enterprise.
19	Absence of PMO	**Preventative/ Administrative**: Implementing central project management and portfolio management.
27	Inadequate governance processes and mismanagement of third party	**Deterrent/ Administrative**- ensuring the third party contracts and governance is robust and cooperative, regular monitoring third party vendors.
41	Breach of Privacy Act	**Deterrent/ Administrative** - Organix has to put some constraint on their Privacy and the amount of information leakage that's been happening.

Maximum Anticipated Cost of Implementation to address Stage Two Risks $150,000

6.3. Stage Three (Key Class D & E Risks)

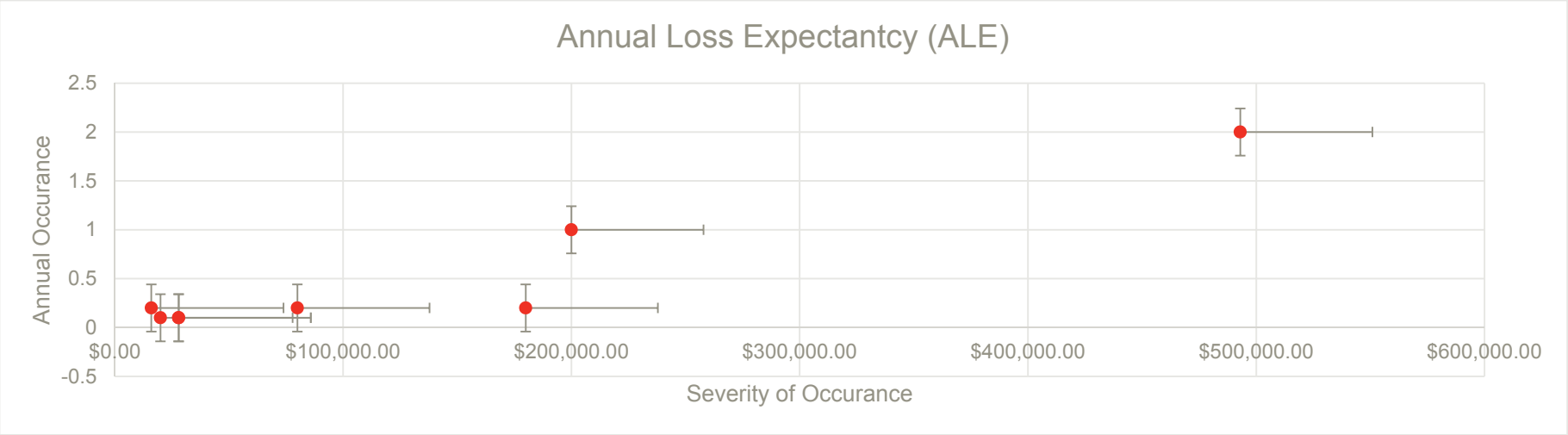
Register No.	Risk	Control Requirements
3	Release of R&D data by Organix employees of 'in production' product to competitors/ open market	**Preventive/ Technical** - In addition to Risk 5 mitigating control, time logging functionality in Enterprise Applications to recall when information was accessed, access control limiting general access to R&D sections of applications. Additional controls also include; **Preventative/ Administrative:** the implementation of non-disclosure/ confidentiality agreements by all R&D workforce, isolation of all personal sound/ video recording technology when entering R&D Deterrent/ Physical: Installation of secure building/ room areas with access limited to R&D persons only.
7	Retail distributors incorrectly enter sales data into POS or stock keeping software	**Detective/ Technical** - online POS interface could trigger verification required alerts if order to be submitted back to Organix exceed 20% of average sales over the past week. This could indicate instance of stock hoarding and potential incorrect stock takes
16	Failure to release information within the required time frames of ASX	**Administrative/ Preventative**: Well defined roles and responsibilities across the organisation to ensure timely notification to ASX occurs. **Administrative/ Preventative**: Develop employee education package clarifying company expectations, release and profiting on market information.
18	Third Party partners (CMD) have Poor or no Security operating Procedures for data parking, data access, data transfer	**Technical/ Administrative**: Well established System acquisition and Design principles across the enterprise with the support of human intervention free technological platform for vendor management.
40	Real time data from online shop unable to be utilised by Organix	**Detective/Technical** - Organix utilise latest and highly sophisticated tools to track real time data from online store.

Maximum Anticipated Cost of Implementation to address Stage Three Risks $120,000

6.4. ALE

Annual Loss Expectancy (ALE's) exercises are designed to provide genuine guidance and point of reference to management when holistically evaluating the Organix Risk profile. ALE's are typically calculated by factoring the total value of the asset by the exposure factor anticipated if the event occurs and multiplying that sum by the number of occurrence in any one year.

The end product is then measured against Organix acceptable/ unacceptable loss tables with the objective being to drive the application of higher order controls in these risks and limit the potential impact on the Organix business.



Register No.	Risk	Single Loss Expectancy (SLE)		Annual Loss Expectancy (ALE)		Total Exposure
		Asset Value (AUD)	Exposure Factor	SLE	Number of occurrences	
9	Compromised network infrastructure/ access from corrupt inbound data.	1 Day Trading approx. ($493,000)	0.5	$246,500	2	$493,000

Register No.	Risk	Single Loss Expectancy (SLE)		Annual Loss Expectancy (ALE)		Total Exposure
		Asset Value (AUD)	Exposure Factor	SLE	Number of occurrences	
11	HQ data room damaged deliberately by Organix Personnel compromises 30%, 60%, 90% functionality	$400,000	0.7	$280,000	.10	$28,000
12	Fire within HQ Data Centre compromises 30%, 60%, 90% functionality	$400,000	0.7	$280,000	.10	$28,000
14	Inappropriate representation of Organix by external parties on social media platforms	$90,000,000 (Assume 50% rev from online)	0.1	$900,000	.2	$180,000
23	Technical downtime event occurs at data centre	$400,000	0.5	$200,000	1.0	$200,000
24	Failure of data centre, loss of property, financial crisis	$400,000	0.5	$200,000	0.1	$20,000
27	Uncontrolled Release of personal information from online shop/ payment gateway	$400,000	1.0	$400,000	0.2	$80,000
36	Redundancy of data back up	$400,000	0.2	$80,000	0.2	$16,000

Note: *It is envisaged that at the conclusion of this process, more detailed threat scenarios may be modelled that will ensure Organix can maintain a proactive approach to the identification, preparation and managed of threat events in the future.*

6.5. Residual Risk

Residual risks represent the final impact a risk presents to the Organix business after all controls have been implemented. Residual risk must not be ignored but instead consultatively managed between all stakeholders to ensure the risk does not become intolerable. Any risks that present residual impacts classed C and higher must be authorised by the appropriate Organix manager defined in section 4.5.

It is also important to note that controls deemed not practicable to implement in today's environment may become more feasible over time therefore, periodic reviews of the risks identified in the report are recommended to ensure the Overall Organix Risk profile remains as low as possible.

7. Business Continuity Considerations

Implementing change whilst maintaining productive business continuity relies on an effective mixture of planning, communication and management. The following recommendations across Financial, Personnel & Operational disciplines are designed to provide practical advice to the Organix ELT when preparing to implement the controls identified in section 6.

7.1. Financial

The recommendations tabled in section 6 require a maximum capital investment of approximately $920,000. This represents less than one percent of company revenue and will in return better protect the Organix business from estimated exposure costs in excess 10 times investment.

Further consideration will need to be made in future budgets beyond FY16-17 to appropriately implement ongoing capital works programs that will address the remainder or risk identified.

7.2. Personnel

The following are suggested approach tactics that can help Organix management implement recommended controls whilst maintaining personnel engagement and business continuity. Human capital resilience is an ability to respond and adapt in an optimal way to threats posed to organizational workforce.

Building resiliency into the organisation via human capital is more likely to protect our organisational resources and maintain continuous operation in the event of a crisis. Organix must consider the impact of both short-term and long-term interruptions and other issues on normal business activities and identifying appropriate actions to maintain critical business processes in the event of a crisis/catastrophe.

Three core areas which can affect significantly personal side of human capital are

- Well defined roles, policies and communications
    - Review policies in accordance to a crisis situation
    - Plan for continual and effective dissemination of information
- Employee education and support
    - Provide preparatory advice prior to crisis situation
    - Provide support for employees and families
- Virtual infrastructure
    - Enable employees to work from anywhere at any time
- Job Training
    - Consider how staff are prepared for any kind of immediate change in role and skill set

- Talent Management
  - Identification of critical roles
  - Plan for seamless leadership transition whenever needed.

7.3. Operational

Organix must maintain certain operational standards to secure further growth including;

- A risk management process that realistically evaluates health related risks and mitigates the safety related risks that are threatening.
- Organix has to impart the skills and knowledge for the employees to fulfil their jobs in a competent manner provided they meet all their regulations
- Organix as an enterprise should encourage the employees to use company's secured devices
- Prioritization on information security has to be enforced in the organization so, if there is a conflict between employees, secure information is not on display.
- Organix has to have a continual improvement to ensure actions are enforced to help improve effectiveness of the organization.
- Organix has to make sure the contracts with the third party vendors are robust and cooperative so that there are no poor relations between the both.

8. References

Brand Crowd, 2016. *Organix Logo.* [Online]
Available at: http://www.brandcrowd.com/logo-design/details/2796
[Accessed 31 August 2016].

Calder, A. & Watkins, S., 2010. *Information Security Risk Management for ISO27001/ISO27002.* s.l.:IT Governance Ltd.

International Standard Orgnisation (ISO), 2013. *ISO-IEC 27002 Information technology — Security techniques — Code of practice for information security controls.* 2nd ed. s.l.:International Standard Orgnisation (ISO).

International Standards Organisation (ISO), 2004. *ISO IEC 13335 Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management.* 1st ed. s.l.:International Standards Organisation (ISO).

International Standards Organisation, 2009. *ISO Guide 73 - Risk Management Vocabulary.* 1st ed. Switzerland: International Standards Organisation.

International Standards Orgnisation (ISO), 2013. *ISO-IEC 27001 Information technology — Security techniques — Information security management systems — Requirements.* 2nd ed. s.l.:International Standards Orgnisation (ISO).

International Standards Orgnisation (ISO), 2016. *ISO-IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary.* 4th ed. s.l.:International Standards Orgnisation (ISO).

John Holland Pty Ltd, 2015. *Information Technology.* 8 ed. Melbourne: John Holland.

Krause, T. &., 2014. *PCI Security Standards Council.* Ilinois: s.n.

Long, J. O., 2011. *ITIL 2011 At a Glance.* s.l.:Springer.

Meigs, J. B., 2016. Blame BP for Deepwater Horizon. But Direct Your Outrage to the Actual Mistake.. *Slate*, 30 September.

National Insitute of Standards and Technology, 2012. *SP 800-30 Information Security.* 1st ed. Gaithersburg: National Insitute of Standards and Technology.

Prananto, A., 2016. *Lecture Slides - Week 8.* Hawthorn: Swinburne.

Standards Australia, 2009. *AS/NZS ISO 31000 Risk Management.* Sydney: Standards Australia.

Tasker, S.-J., 2016. Blackmores suffers bitter pill from new China rules. *The Australian Business*, 12 April.

Wall Street Journal, 2016. China Opens Anti-Trust Investigation of DIdi-Uber Deal. *Wall-Street.*

Word Count: 4187

9. Appendices

9.1. Risk Register

Organix Risk Register

Risk Number/ Risk Manager	Threat Source (Ts)	Vulnerability (V)	Threat Events (Te)	Department Owner R&D, Logistics & Supply, Retail, Business Development/ Global Expansion, All	Select. Conseq Type	CURRENT RISK RATING *Rating before noted controls are implemented*			ALE/SLE Calc if required	CONTROL REQUIREMENTS ACTIVITY PLANNING, RESOURCE, EQUIPMENT & GENERAL CONSIDERATIONS	RESIDUAL RISK RATING *Expected rating when noted controls are implemented.*			Cost Benefit Analysis	
						Consequence.	Likelihood (Li)	Impact (I)			Consequence.	Likelihood (Li)	Impact (I)	Cost of Protection	Cost of Exposure
Tom - 1	Malicious introduction of non certified products or techniques	Poor visibility over Organix supply chain	Compromised Organic products/ certification introduced to manufacturing supply chain	Logistic & Supply	Reputation & Community	5	Likely	A	N/A	Technical/ Preventative - Periodic technical analysis of Organ products undertaken as part of quality management process by contract manufactures. Physical/ Detective - Chain of responsibility audits from factory to farmer etc. undertaken by Organix to ensure supply chain integrity is maintained	4	Possible	C	Level 4	Level 5
Tom - 2	Intentional removal of hardware/ peripherals from site	Poor security, asset tracking arrangements	Unauthorised removal of equipmen by staff, contractors and visitors	ALL	Management Impact	3	Likely	C	N/A	Preventative/ Administrative - Establish comprehensive asset register, conducting periodic audits to ensure shrinkage in asset base is minimal Preventative/ Administrative - Provide training, signage and reference information to personnel issued with company assets on the important of securing equipment when left unattended Deterrent/ Physical - install alarms and surveillance throughout building and asset rooms to prevent malicious harm Recovery/ Operational - Equip portable/ mobile assets with remote wipe capabilities	2	Possible	D	Level 2	Level 4
Tom - 3	R&D data of 'in production' product released to competitors/ open market	System design flaw allows export of documentation to outside sources	Release of R&D data by Organix employees of 'in production' product to competitors/ open market	R&D	Management Impact	3	Unlikely	D	N/A	Preventive/ Technical - In addition to Risk 5 mitigating control, time logging functionality in Enterprise Applications to recall when information was accessed, access control limiting general access to R&D sections of applications. Additional controls also include; Preventative/ Administrative: the implementation of non disclosure/ confidentiality agreements by all R&D workforce, isolation of all personal sound/ video recording technology when entering R&D Deterrent/ Physical: Installation of secure building/ room areas with access limited to R&D persons only.	2	Unlikely	E	Level 3	Level 5
Tom - 4	R&D data of 'in production' product released to competitors/ open market	System design flaw allows export of documentation to outside sources	Release of R&D data by external business partners of Organix of 'in production' product to competitors/ open market	Logistic & Supply/ Retail	Management Impact	3	Possible	C	N/A	Preventive/ Technical - In addition to Risk 5 mitigating control, time logging functionality in Enterprise Applications to recall when information was accessed, access control limiting general access to R&D sections of applications. Additional controls also include; Preventative/ Administrative: the implementation of non disclosure/ confidentiality agreements by all R&D workforce, isolation of all personal sound/ video recording technology when entering R&D Deterrent/ Physical: Installation of secure building/ room areas with access limited to R&D persons only.	3	Unlikely	D	Level 3	Level 5

Organix Risk Register

Tom - 5	R&D data of 'in development' product released to competitors/ open market	System design flaw allows export of documentation to outside sources	Release of R&D data by Organix employees of 'in development' product to competitors/ open market	R&D	Management Impact	4	Unlikely	C	N/A	Preventive/ Technical - In addition to Risk 5 mitigating control, time logging functionality in Enterprise Applications to recall when information was accessed, access control limiting general access to R&D sections of applications. Additional controls also include; Preventative/ Administrative: the implementation of non disclosure/ confidentiality agreements by all R&D workforce, isolation of all personal sound/ video recording technology when entering R&D Deterrent/ Physical: Installation of secure building/ room areas with access limited to R&D persons only.	3	Unlikely	D	Level 3	Level 5
Tom - 6	R&D data of 'in development' product released to competitors/ open market	System design flaw allows export of documentation to outside sources	Release of R&D data by external business partners of Organix of 'in development' product to competitors/ open market	R&D	Management Impact	4	Possible	C	N/A	Preventive/ Technical - all users requiring access to Organix System must register and be approved by Organix Sponsor. All information accessible via portal only which will be unable down load to local client	2	Unlikely	E	Level 3	Level 5
Tom - 7	Incorrect sales data entered into POS and stock keeping software	POS system does not verify irregular input information	Retail distributors incorrectly enter sales data into pos or stock keeping software	Retail	Management Impact	2	Possible	D	N/A	Detective/ Technical - online POS interface could trigger verification required alerts if order to be submitted back to Organix exceed 20% of average sales over the past week. Th could indicate instance of stock hoarding and potential incorrect stock takes	1	Possible	E	Level 1	Level 3
Tom - 8	Sales data withheld from Organix operations	Lack of contractual conditions govern timely release of sales data from vendor	Retail sales data is withheld from Organix operations	Retail	Budget	3	Possible	C	N/A	Deterrent/ Administrative - Memorandum of understanding/ contractual established between retailers and Organix	2	Unlikely	E	Level 1	Level 4
Tom - 9	Sales data maliciously manipulated by retail distributors	No governance/ controls in place monitoring data input from vendors	Data manipulated outside Organix operations	Retail	Budget	4	Possible	C	N/A	Detective/ Technical - online POS interface could trigger verification required alerts if order to be submitted back to Organix exceed 20% of average sales over the past week. Th could indicate instance of stock hoarding and potential incorrect stock takes	3	Unlikely	D	Level 4	Level 5
Tom - 10	Corrupt inbound data compromises Network infrastructure/ access	Firewall weakness	Compromised network infrastructure/ access	Logistic & Supply	Management Impact	5	Possible	B	Yes	Detective/ Technical - Inbound data logging could be configured to detect unusual traffic patterns. This could be further eliminated through limiting traffic to those emanating from specific cod/ retailer suppliers	4	Unlikely	C	Level 4	Level 5
Tom - 11	Internal hardware run to failure undermining system integrity	Poor preventative maintenance regime	HQ Data centre hardware failure undermines system integrity	ALL	Management Impact	3	Possible	C	N/A	Preventative/ Technical - Robust lifecycle, hardware refreshment schedule developed to prevent data centre failures Recovery/ Technical - Robust back up regime implemented to ensure any loss of data centre functionality is mitigated. Recovery/ Technical - Additional Data Centre established to ensure seamless fail over of Organix enterprise systems minimising any business disruptions Recovery/ Administrative - Disaster Recovery Plan Implemented to ensure effective management of data centre outage	1	Possible	E	Level 2	Level 5

Organix Risk Register

Tom - 12	Malicious Damage to HQ data room	Poor facility security	HQ data room damaged deliberately by Organix Personnel compromises 30%, 60%, 90% functionality	ALL	Management Impact	4	Possible	C	Yes	Preventative/ Administrative - Conduct monthly facility audits/ house keeping inspections to proactively identify potential issues before event occurrence Recovery/ Technical - Robust back up regime implemented to ensure any loss of data centre functionality is mitigated. Recovery/ Technical - Additional Data Centre established to ensure seamless fail over of Organix enterprise systems minimising any business disruptions Recovery/ Administrative - Disaster Recovery Plan Implemented to ensure effective management of data centre outage Deterrent/ Physical - Access to infrastructure rooms/ Data centre limited to essential personnel only. Deterrent/ Administrative - Appropriate signage installed delineated authorised personnel only areas	2	Possible	D	Level 5	Level 5
Tom - 13	Non-Adversary damage to HQ Data Centre	Inadequate facility design	Fire within HQ Data Centre compromises 30%, 60%, 90% functionality	ALL	Management Impact	4	Unlikely	C	Yes	Preventative/ Administrative - Conduct monthly facility audits/ house keeping inspections to ensure emergency fire equipment is serviceable and data centre free of clutter Recovery/ Technical - Robust back up regime implemented to ensure any loss of data centre functionality is mitigated. Recovery/ Technical - Additional Data Centre established to ensure seamless fail over of Organix enterprise systems minimising any business disruptions Recovery/ Administrative - Disaster Recovery Plan Implemented to ensure effective management of data centre outage Corrective/ Physical - Appropriate fire suppression installed to mitigate severity of fire event. Corrective/ Physical - Appropriate Test & Tagging/ Electrical Safety inspections undertaken annually on all Organix IS/IT infrastructure	2	Possible	D	Level 4	Level 5
Tom - 14	Release of sensitive information released	Poor control over social media access	Sensitive information released by employees on social media	R&D	Management Impact	4	Possible	C	N/A	Deterrent/ Administrative - Develop Organix external media policy and education package designed to define how employees can responsibly include Organix in their social media activities. Detective/ Technical: Organix to continue to strengthen its social media brand image by active monitoring social media feeds to ensure any damaging releases are identified and acted upon in a timely manner	2	Possible	D	Level 2	Level 5
Gagan - 15	Lack of social media policy for external / internal organisational environment	Loss of reputation	External parties misusing Organix name on social media platforms / Personal comments by an employee on the social media	ALL	Management Impact	3	Likely	C	YES	Administrative control: Creating , implementing and auditing a well defined social media policy across the enterprise.	3	Unlikely	D	level 3	Level 5
Gagan - 16	Ambiguous roles and responsibility	Mismanagement of sensitive market information	Failure to release information within the required time frames of ASX	ALL	Management Impact	2	Possible	D	N/A	Administrative/ Preventative: Well defined roles and responsibilities across the organisation to ensure timely notification to ASX occurs. Administrative/ Preventative: Develop employee education package clarifying company expectations, release and profiting on market information.	3	Unlikely	D	Level 3	Level 4
Gagan - 17	Manipulation of legacy VPN infrastructure	Average VPN access methodology	Inadequate encryption of VPN connection between Organix & CMD	Logistic & Supply	Management Impact	5	Likely	A	N/A	Implementing the secure two step verification methodology using appropriate technological control	3	Rare	D	Level 4	Level 4

Organix Risk Register

Gagan - 18	Third party compliance issue	Poor RFP and vendor management	Third Party partners (CMD) have Poor or no Security operating Procedures for data parking, data access, data transfer	Logistic & Supply	Management Impact	3	Unlikely	D	N/A	Technical and Administrative control: Well established System acquisition and Design principles across the enterprise with the support of human intervention free technological platform for vendor management.	2	Unlikely	E	Level 3	Level 4
Gagan - 19	Absence of PMO	Absence of centralise control and stakeholder engagement	SAAS vendors are engaged independent of I.T function	ALL	Regulatory	3	Likely	C	N/A	Administrative control: Implementing central project management and portfolio management	2	Rare	E	Level 3	Level 4
Gagan - 20	Neglecting internal SME advice	Neglecting critical feature before outsourcing work	Data provided to SAAS is stored offsite in commercial data centres outside Organix control and verification	ALL	Regulatory	3	Likely	C	N/A	Preventive and Administrative control: Managing appropriate committees by engaging all stakeholders and SME if required.	3	Rare	D	Level 3	Level 4
Gagan - 21	Neglecting communication and project Methodology	Clueless stakeholders about the new system.	Lack of awareness/ training in use of SAAS systems, architecture	ALL	Management Impact	2	Likely	D	N/A	Preventive control: Mandatory change management and stakeholder feedback before signing off the project	3	Rare	D	Level 3	Level 4
Gagan - 22	Absence Technology control	Compromised SAAS application	Theft of data from SAAS application	ALL	Reputation & Community	3	Possible	C	N/A	Third party testing and SME expert reporting before implementing any critical off the shelf resources.	2	Unlikely	E	Level 4	Level 5
Gagan - 23	Absence of Physical control	Compromised physical access to the servers	Theft of data from commercial data centre	ALL	Management Impact	4	Possible	C	N/A	Technical / Physical control: Implementing swipe cards, cameras and other physical security guard control before entering in to main data backup systems	2	Rare	E	Level 4	Level 5
Gagan - 24	No Parallel redundancy	Data centres server failure	Technical downtime event occurs at data centre	ALL	Management Impact	3	Possible	C	YES	Technical and Recovery control: Creating a parallel redundancy policy and stress testing it before the actual event.	3	Possible	C	Level 4	Level 5
Gagan - 25	Natural disaster/ act of god event impacts data centre availability	Fire/Flood @ data server centre	Failure of data centre, loss of property, financial crisis	ALL	Management Impact	4	Unlikely	C	Yes	Technical and Compensatory control : Implementing a parallel data backup facility in different jurisdictions and location to c over such act of god.	3	Possible	C	Level 4	Level 5
Gagan - 26	Unsecure EA software	Failure of Organix enterprise system due to patch failure	Loss of confidentiality, privacy, thef of information	ALL	Management Impact	3	Likely	C	N/A	Preventive control and Administrative control: Ongoing partnership with preferred SME testing reports for any software updates	3	Possible	C	Level 3	Level 5
Srinath- 27	Inadequate governance processes and mismanagement of third party	Poor relations between Organix and the third-party vendors	Lack of transparency in third party operation of online shop and payment gateway	Retail	Reputation & Community	3	Possible	C	N/A	Deterrent/administrative- ensuring the third party contracts the governance is robust and cooperative and regular monitoring third party tools	3	Unlikely	D	Level 3	Level 3
Srinath - 28	Poor security protocols by third party vendor	Lack of developed infrastructure of the online shop	Uncontrolled Release of personal information from online shop/ payment gateway	Retail	Reputation & Community	3	Possible	C	YES	Recovery/technical - employees need to be proactive and well trained to subside these data breaches and service contract between Organix and third party vendors has to be verifying every regulation.	2	Unlikely	E	Level 5	Level 5
Srinath - 29	Poor security protocols by third party vendor	Lack of developed infrastructure of the online shop	Uncontrolled release of financial details from online shop/ payment gateway	Retail	Reputation & Community	3	Possible	C	N/A	Recovery/technical - employees need to be proactive and well trained to subside these data breaches and service contract between Organix and third party vendors has to be verifying every regulation.	2	Unlikely	E	Level 2	Level 3
Srinath - 30	Compromised inventory data flow from online shop to Organix enterprise application	Insecure back-up servers	Theft of intellectual property	Retail	Management Impact	3	Possible	C	N/A	Recovery/technical - ensuring data back up server are working efficiently and firewall security protocols are regularly updated to prevent malware and such risks	3	Unlikely	D	Level 2	Level3
Srinath - 31	Globalization of Organix in several countries	Lack of global awareness	Uncontrolled release of information provided to country regulators for accreditation purposes	Business Development & Global Expansion	Management Impact	4	Unlikely	C	N/A	Deterrent/administrative- The business report provided to department for the approval has to be well documented and reviewed.	3	Unlikely	D	Level 1	Level 1

Organix Risk Register

Srinath - 32	Intricate details of back up facility openly published on vendor website	Severe lack of privacy	Back up facility attacked	ALL	Management Impact	3	Almost Certain	B	N/A	Recovery/ Administrative – Assess exposure/extent of compromised privacy. If deemed severe, commerce selection process for new vendor immediately. Preventative/ Administrative - Establish clear operating and non-disclosure requirements with vendor.	2	Unlikely	E	Level 5	Level 5
Srinath - 33	Conflict of interest between IS/IT Management & third party suppliers (back up)	Lack of prioritisation of information	Malicious usage of Research and development designs	ALL	Management Impact	3	Almost Certain	B	N/A	Compensating/ Administrative - Competitive tender process undertaken to ensure best value add vendor selected. Preventative/ Administrative – Implementation of Code of Business conduct clarifying Organix position on engaging vendors.	2	Possible	D	Level 2	Level 4
Srinath - 34	Organix HQ targeted in physical attack harming Data Centre	Lack of Contingency protocols	Severe loss of research information and infidelity in every department	ALL	Management Impact	5	Possible	B	N/A	Detective/physical - Security of the data centre should be sophisticated as such that only people with permits allowed into data centre	1	Unlikely	E	Level 3	Level 3
Srinath - 35	Lack of Genuine trademark	Obsolete hardware	Organix enterprise applications unsupported by product manufactures	ALL	Management Impact	3	Likely	C	N/A	Detective/administration - Organix enterprise has to have a team of workers who are dedicated should auditing external party vendors.	3	Unlikely	D	Level 2	Level 3
Srinivas - 36	Absence of internal capability to maintain and develop Organix enterprise applications	People capability	Mishandling of system can lead to the catastrophe.	ALL	Management Impact	3	Almost Certain	B	N/A	Corrective/Technical - Employees should be well trained and certificated	2	likely	D	Level 2	Level 2
Srinivas - 37	Inadequate Monthly Data Backup regime	Contingency back up in case of a calamity is lacking	Redundancy of data back up	ALL	Management Impact	4	Likely	B	Yes	Recovery/ Technical - Data backup frequency must increase from once monthly to once every two days mitigating the consequence of total loss occurrence.	2	Unlikely	E	Level 5	Level 5
Srinivas - 38	Inadequate personal computing user training (lock pc's etc.)	Employee's who got recruited are in-sufficiently well trained	Mishandling of information, leakage of secured information	ALL	Management Impact	3	Likely	C	N/A	Corrective/Technical - Well trained staff	2	Unlikely	E	Level 2	Level 3
Srinivas - 39	Export of Organix data via accessible data ports on p.c's (usb, dvd)	Lack pf prioritization on security clearance.	Major loss of reputation, severe downfall in the global market	ALL	Management Impact	3	Unlikely	D	N/A	Compensating/administrative- Organix as enterprise should encourage the employees to use the company's secured devices	3	Unlikely	D	Level 5	Level 5
Srinivas - 40	Latency between collection of data from online store and knowledge creation	No real time data analysis has been implemented	Real time data from online shop unable to be utilised by Organix	Retail	Management Impact	2	Possible	D	N/A	Detective/Technical - Organix have to use latest and highly sophisticated tools to track real time data from online store.	2	Unlikely	E	Level 2	Level 2
Srinivas - 41	Breach of Privacy Act	Lack of integrity	Severe loss of company's standing in the financial market and reputation	ALL	Management Impact	2	Possible	D	N/A	Deterrent/ Administrative - Organix has to put some constraint on their Privacy and the amount of information leakage that's been happening	2	Unlikely	E	Level 2	Level 4
Srinivas - 42	Breach of therapeutic Goods Act	Lack of research on the regulations	Major loss on company's international trade and global positioning	Retail	Management Impact	3	Possible	C	N/A	Detective/administration - A well regulated information has to be collected from different organizations before entering into the market	2	Unlikely	E	Level 2	Level 4
Srinivas - 43	Loss of accreditation to therapeutic goods	A Flaw in the Formulae of the product	Tuning out their defects may cause the organization a substantial amount of financial loss	All	Management Impact	3	Unlikely	D	N/A	Deterrent/ Administrative - For the accreditation to occur they have to test their products pro-actively actively seeking threat	2	Possible	D	Level 2	Level 3
Srinivas - 44	Political Lobbying by Non Government Organisations	Product effecting major amount of people	Not meeting the requirements of government the product might effect people in a harmful way	ALL	Reputation & Community	2	Unlikely	D	N/A	Deterrent/ Administrative - The research and development has to test their products in a organized manner to avoid such risks	3	Possible	C	Level 4	Level 5
Srinivas - 45	Hostile change in tariff rates of import countries	Lack of research on inter-country financial policies	High increase of rates on products is enforced	Retail	Management Impact	3	Possible	C	N/A	Deterrent/ Administrative - Organix has to develop a well documented report on the countries they are expanding and the regulations they have to tested by	3	Possible	C	Level 3	Level 4

9.2. Team Minutes

IS/IT Group minutes

Title:	IS/IT Group Meeting 1
Date:	27/08/2016
Time:	8:00pm – 9:00pm
Held at:	Online - Skype

Chaired by:	Thomas Fulham
Minuted by:	Thomas Fulham
Distribution date:	28/08/2016

Attendees list	
Thomas Fulham (TF)	**Srinivas Jonnavithula (SJ)**
Gagan Jyoti (GJ)	**Srinath Gopathi (SG)**

Apologies list
Nil

Meeting minutes

ITEM	DESCRIPTION/ACTION	BY WHOM	BY WHEN
1	Frequency of ongoing meetings agreed to be weekly immediately after the conclusion of class on Wednesday nights. Additional Online meetings will be schedule as required	ALL	N/A
2	Create weekly online meeting place holder	TF	31/08/2016
3	Create drop box location for group documents and distribute link	SG	28/08/2016
4	Upload to dropbox foundation risk register sheet	TF	31/08/2016
5	Draft proposed report structure for review at next meeting	TF	31/08/2016
6	Draft response to point three progress review requirement (Group dynamics, proposed meeting schedule)	GJ	31/08/2016
7	Critically review case study inputting specific risk/ vulnerability items into risk register	ALL	31/08/2016
8	Submission of Week 5 progress review agreed for C.O.B Friday 2nd September	ALL	02/09/2016

NEXT MEETING

Date:	Wednesday 31st August
Time:	7:00 PM
Location:	Online Skype

IS/IT Group minutes

Title:	IS/IT Group Meeting 1
Date:	31/08/2016
Time:	8:00pm – 9:00pm
Held at:	Planned online but we had face to face @ Swinburne campus

Chaired by:	Thomas Fulham
Minuted by:	Gagan J Sharma
Distribution date:	31/08/2016

Attendees list	
Thomas Fulham (TF)	**Srinivas Jonnavithula (SJ)**
Gagan Jyoti (GJ)	**Srinath Gopathi (SG)**

Apologies list
Nil

Meeting minutes

ITEM	DESCRIPTION/ACTION	BY WHOM	BY WHEN
1	Started working on Risk register	ALL	N/A
2	Division of work among team	ALL	31/08/2016
3	Debate and discussion for work	ALL	
4	Started populating risk register	ALL	

NEXT MEETING

Date:	Wednesday 31st August
Time:	7:00 PM
Location:	Online Skype / But held @ Swinburne campus after class

IS/IT Group Minutes

Title:	IS/IT Group Meeting 1
Date:	28/09/2016
Time:	8:30-10:00
Held at:	Swinburne Library

Chaired by:	Thomas Fulham
Minuted by:	Thomas Fulham
Distribution date:	29/10/2016

Attendees list	
Thomas Fulham (TF)	**Srinivas Jonnavithula (SJ)**
Gagan Jyoti (GJ)	**Srinath Gopathi (SG)**

Apologies list
Nil

Meeting minutes

ITEM	DESCRIPTION/ACTION	BY WHOM	BY WHEN
1	Continue Risk Register Workshop	ALL	N/A
2	SP 800-30 Reviewed with relevant elements incorporated with ISO 31000 framwork as appropriate to Organix Case Study	TF	N/A
3	Obtain background news/ contextual information from industry competitors (Blackmores/ Cernovis) that could be incorporated into Organix Risk Assessment	SJ	Next meeting
4	All risk allocated to Risk Managers, draft proposed mitigating controls for group review	ALL	Next Meeting
5	Group Round Table – Personal reflection on group performance, any corrective actions required	TF	N/A

NEXT MEETING

Date:	05/10/2016
Time:	8:30pm
Location:	Swinburne

IS/IT Group minutes

Title:	IS/IT Group Meeting 3
Date:	05/10/2016
Time:	5:30pm – 8:30pm
Held at:	Swinburne Library

Chaired by:	Srinath Gopathi
Minuted by:	Srinath Gopathi
Distribution date:	05/10/2016

Attendees list	
Thomas Fulham (TF)	**Srinivas Jonnavithula (SJ)**
Gagan Jyoti (GJ)	**Srinath Gopathi (SG)**

Apologies list
Nil

Meeting minutes

ITEM	DESCRIPTION/ACTION	BY WHOM	BY WHEN
1	Review of the Report. Had a complete review of the report and decided what else should be included	ALL	N/A
2	Modifications in the risk register. Went through the risk register and decided to include the cost benefit analysis based on the cost of protection and cost of exposure. Further modifications are done based on the work done	ALL	N/A
3	Calculation of the annual loss expectancy. Included the column of annual loss expectancy expected to calculate on the estimation for the risks	ALL	N/A
4	Control requirements, Activity planning, Resource equipment and General considerations. Divided and assigned the work equally to apply the control requirements based on the threat source and threat events	ALL	N/A
5	Discussion as group to do the assigned work on time and submit it to the Dropbox and do final submission prior to the time	ALL	N/A

Next meeting

Date:	Wednesday 12th October
Time:	5:00 PM
Location:	Swinburne library

IS/IT Group minutes

Title:	IS/IT Group Meeting 4
Date:	12/10/2016
Time:	5:30pm – 8:30pm
Held at:	Swinburne Library

Chaired by:	Thomas Fulham
Minuted by:	Srinivas Bharadwaj
Distribution date:	12/10/2016

Attendees list	
Thomas Fulham (TF)	**Srinivas Jonnavithula (SJ)**
Gagan Jyoti (GJ)	**Srinath Gopathi (SG)**

Apologies list
Nil

Meeting minutes

ITEM	DESCRIPTION/ACTION	BY WHOM	BY WHEN
1	Final Update of the Report incorporating Adi's Feedback.	ALL	N/A
2	Modifications in the risk register. Split out and clarification of regulatory risks	ALL	N/A
3	Finalised ALE calculations	ALL	N/A
4	Workshop of Vulnerabilities (V)	ALL	N/A
5	Gold Review in preparation for final submission.	ALL	N/A
6	Group decision, still on track to submit by original deadline. Continue to deliver for this date.	TF	14/10/2016

Next meeting

Date:	Debrief post assignment marks release.
Time:	-
Location:	-