**Section 1:**

**BCM planning**

**BCM planning inclusive of Information Governance, Information Security Policy**

**(several paragraphs setting the context for BCM & resilience)**

**Section 2:**

**Information Security-Risk Mitigation For 10 Priorities**

**Organization Background**

Founded in 2012 by Brad Hill and Angelique Farelli, eTricity AU is a leading for-profit enterprise based in Victoria, Australia. Sustainability is integral to its identity as a provider for photovoltaic solar panel solutions. Over the course of the years, eTricity has expanded its revenue streams. Nevertheless the diversified value creations activities, its core attention is of research, development and innovation.

**Objectives**

Based on the risk assessment conducted as an initial phase of risk management (RM) process, it has been identified the 11 prioritized risks requiring formulation of the risk treatment strategies.

Risk 1. Security and Operational Efficiency of *RecShareOne*

Risk 2. Natural disaster risk

**Risk 3. Unsecured data transmission from Wi-fi and customer broadband, to eTricity data warehouse**

Risk 4. BYOD policy

**Risk 5. Cloud-Based Data Management risks (specifically referring to confidential infrastructure design**)

**Risk 6. Data leakage from phishing attacks designed to access corporate account details**

**Risk 7. Third-Party backup service (hieu)**

**Risk 8. Data transmission for government (hieu)**

**Risk 9. Human error- Accidental data deletion and leakage (spencer)**

**Risk 10. Supply chain / Internal security risks of corporate espionage and company fraud**

**(Own words but need to rephrase)** There are acceptable risk and unacceptable risk. How much of a risk is unacceptable that it puts the organization at harm? An organization certainly need to take a certain degree of risks, as they are needed as a mean to take on opportunities.

The objectives of this Business Continuity Plan are:

* Objectives 1
* Objectives 2
* Objectives 3
* Etc.

* **High availability**: Provide for the capability and processes so that a business has access to applications regardless of local failures. These failures might be in the business processes, in the physical facilities or in the IT hardware or software.
* **Continuous operations**: Safeguard the ability to keep things running during a disruption, as well as during planned outages such as scheduled backups or planned maintenance.
* **Disaster recovery**: Establish a way to recover a [data center](https://www.ibm.com/services/business-continuity/data-center) at a different site if a disaster destroys the primary site or otherwise renders it inoperable.

<https://www.ibm.com/au-en/services/business-continuity/plan>

**Reasons for Risk**

**Risk 1. Security and Operational Efficiency of *RecShareOne*  (Ragib)**

RecShareOne is a custom-made enterprise system that eTricity uses in order to maintain all of its documents. This includes all operational records like documents, contracts, suppliers, customers, orders, invoices, etc. Although keeping all of these information assets there makes it easier to centralize their management, it does lead to a single point of failure type situation. This means that if the system went down for any reason, almost all of the organizational processes would end up halting.

Furthermore, it is also a legacy system that had been developed 8 years ago, by a software company from Wonthaggi, which no longer exists. This has led to the system being incapable of properly handling the huge amount of information that the company currently processes, leading their IT team to develop patches and workarounds just to keep the system functional. This means that right now the system is extremely vulnerable even to the smallest form of DDOS attack or to any other modern malware or bot that is flowing around in the internet (as it had been created a long time ago without any proper, big update to software since)

**Risk 2. Natural disaster risk** **(ragib)**

A natural disaster is basically any natural event that causes either great damage or loss of life. This can be in any form, like fire, flood, earthquake, hurricane, etc. But no matter what, they all end up leading to the same outcome, loss or harm to personnel and loss of access to business and information assets.

In case of eTricity, it is located in Inverloch, on Bass Coast, which is a flood prone region that is constantly harassed by stormy and erratic weather events. Furthermore, currently there is also an expectation of a disastrous storm impacting it soon. Thus, there is a high likelihood of a natural disaster occurring and can lead to:

* Damage to part of all of information system or building that houses it
* Disruption of operations due to loss of access to resources
* Harm or loss of life of personnel on the site

[Reference: Whitman table 10-3, ch 10, pg 436—used the reference for the effect only and ignored the mitigation part in that table as not relevant to note that here]

**Risk 3. Unsecured data transmission from Wi-fi and customer broadband, to eTricity data warehouse (cindy)**

Customer data of electricity consumption are shared and exchanged over the Wi-Fi and customer broadband to eTricity data warehouse and vice versa. Large amounts of data are generated and processed over the last 10 years.  Confidentiality, integrity, availability is at risk from unauthorised access.

**Risk 4. BYOD policy (cindy)**

BYOD or Bring Your Own Device is a practice in a shifting working culture where employees are allowed to use personal devices for work. The benefits that BYOD provides also comes with consequences of heightened security risks associated with, but not limited to  hacking, malware, and data leakage. The concern with eTricity BYOD is the missing procedural guide, in specific the  BYOD Code Of Conduct to protect against BYOD vulnerabilities.

**Risk 5. Cloud-Based Data Management risks (specifically referring to confidential infrastructure design) (ted)**

The CBDM is one of the important areas for the company to secure as this area has lots of information that are crucial to the business. The risk within this area is that they share with their subbies the confidential designs. If the subbies get compromised, the data would be leaked. Another thing about this area is that the lowering costs would lead to insufficient security measures for the CBDM and the monitor system is decided by people who may not be experts at understanding the digital enviroment.

**Risk 6. Data leakage from phishing attacks designed to access corporate account details (ted)**

This type of attack is common and is used to target lots of the employees in the corporate. By using emails to bait the users to click on the links in the email, lots of people keep getting attacked by this type of phishing and the data related to the company would be leaked.

**Risk 7. Third-Party backup service (hieu)**

**Risk 8. Data transmission for government (hieu)**

**Risk 9. Human error- Accidental data deletion and leakage (spencer)**

The risk of data deletion and/or leaks within eTricity is due to the large disparity in user access groups. From an outside perspective, it is unclear what groups have access to what internal data, who can edit/remove information, and the hierarchy involved in the management of those groups (especially the 3rd party contractors).

Data deletion is an issue of backups and data redundancy, whereas leaks are an issue that can affect external stakeholders and will need to be dealt with in accordance with the Notification of Data Breach Ammendment.

**Risk 10. Supply chain / Internal security risks of corporate espionage and company fraud**

The largest aspect of the organisation that lacks credibility and accountability is the supply line communication. According to the case, only the Chief Engineer was charged with selecting suppliers, which has had little documentation or justification for the choices. This poses a risk of corporate corruption and there can be no support for these decisions because they have been made by an individual.

In addition, communication with suppliers in Guangdong, China, are made exclusively through email, which does not interface with RecShareOne. This prevents access to the paper-trail outside of the engineering department (potentially just the Chief Engineer).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk** | | | **Risk Analysis** | | | **Risk treatment (Accept, share, reduce, avoid)** |
| **Category** | **Description** | **Key Controls** | **Impact** | **Likelihood** | **Score** |
| Operational | Security and Operational Efficiency of *RecShareOne* |  | 5 | 5 | 25 | Avoid |
| Reason for rating:   * The heart of the company * Contain all the data connected to all other parts of the business * Impact all the business goals and objectives * Critical organizational asset | | | | | | |
| Operational | Natural disaster risk |  | 5 | 2 | 10 | Reduce |
| Reason for rating:  Natural disasters are difficult to mitigate and result may  be devastating  Waterproofing and stabilisation measures | | | | | | |
| Operational | Unsecured data transmission from Wi-fi and customer broadband, to eTricity data warehouse |  | 4 | 3 | 12 | Share |
| Reason for rating:   * Various ways to fix the issue * lost of confidentiality of transferred data * eTricity hv extranet vpn as a form of control | | | | | | |
| Operational | BYOD policy risks |  | 5 | 3 | 15 | Reduce |
| Reason for rating:   * Everyone has BYOD * May not updated OS * Connect unsecure networks * Prone to social engineering attack | | | | | | |
| Strategic | Cloud-Based Data Management risks (specifically referring to confidential infrastructure design) |  | 4 | 2 | 8 | Share |
| Reason for rating:   * Cloud-based risk * Risk can transfer to cloud server company * International storage laws not strict | | | | | | |
| Strategic | Data leakage from phishing attacks designed to access corporate account details |  | 5 | 5 | 25 | Avoid |
| Reason for rating:   * Ignore the advice of the IT department * Lack of trust and respect * High use of emails | | | | | | |
| Strategic | Internal security risks of corporate espionage and company fraud |  | 4 | 5 | 20 | Avoid |
| Reason for ratings:   * People keep stuff in their PC * No internal auditing system | | | | | | |
| Strategic | Third-Party backup service risks |  | 4 | 3 | 12 | Share |
| Reason for ratings:   * The responsibility of the third-party company * Backup company not tested | | | | | | |
| Strategic | Data transmission for government – Governance risk |  | 2 | 2 | 4 | Accept |
| Reason for ratings:   * eLargely a PR risk * Relies on clear communication to the client-base * Potential risk | | | | | | |



**Internal Controls**

|  |  |
| --- | --- |
| Access Controls | Regulate the admission of users into trusted areas of the organisation, logical & physical encompassing, identification, authentication authorisation, accountability including network access control |
| Firewall |  |
| Backup files |  |
| Documented processes |  |
| Anti-virus systems |  |
| Training process |  |
| Certification |  |
| Emails |  |
| Computers |  |

**JACOBSON WINDOW (Avoid, transfer, etc)**

**Section 3: Business Impact Analysis**

**Critical Business Functions** **(CBF)**

Vital business functions without which an [organization](https://www.bcmpedia.org/wiki/Organization) cannot long operate. If a critical business function is non-operational, the [organization](https://www.bcmpedia.org/wiki/Organization) could suffer serious legal, financial, goodwill or other serious losses or penalties.

(**Source:** Australia. A Practitioner's Guide to Business Continuity Management HB292 - 2006 )

|  |  |  |  |
| --- | --- | --- | --- |
| **Critical Business Functions** | | | |
| **Process Area** | **Critical Function** | **Detailed Processes** | **Reason For Criticality** |
| **Production** | Supply chain management (supplier to eTricity to consumers) | * Delivering innovative solutions for customers through product research and innovation * Quality management * Distribution and logistics * Finding reliable suppliers and negotiations | * Delivering solutions to customers needs * Reason for competitive advantage |
| Design, manufacture and assemble |
| **Sales** | Sales management (customer handling, distribution,  installation) | * Marketing of products/services to potential customers * Customer service | * eTricity revenue is highly dependant upon sales performance |
| **Finance and Accounting** | Company finance management, transactions, budget approval | * Determine company’s  financial health * Aiding decision making * Point of contact for budget approval | * Fulfill legal and financial obligations * Ensure smooth running of business operation without financial disruptions |
| **IT** | Securing network and system infrastructure, protecting proprietary data | * Ensure compliance to NPP and Australian Privacy Legacy, and Notification of Data Breach * Data management, utilisation and governance * Establishment, maintenance and update to IT infrastructure * IT security * Implementation of supplemental programs and services | * Failure to adhere to regulations is not limited to exposure of risks like   fines, but also to loss of goodwill   * Ensure CIA of data protected * Critical for establishing efficient system infrastructure to support operational processes * Extracting full potential of data to improve business processes and efficiencies |
| Live report generation referring to eTricity products |
| **Human Resource** | Employee lifecycle management | * Management of employee lifecycle * Training for regulation compliances and best practices * Development of good company culture | * Supporting the needs of business to meet mandates, goals and objectives * Good company culture increases productivity and employee satisfaction. e.g., data driven culture, security culture |

**Assumptions**   
Throughout the development of this business continuity plan, key assumptions were made to be able to provide accurate prevention and recovery plans:

examples of assumptions:

* Staff are denied access to the office building for a sustained period of seven calendar days
* Extend planning to commence on day two or three if a disaster is projected to exceed seven calendar days
* Address only critical business functions and not daily operational contingencies
* Only critical business functions will be accorded priority during the seven calendar day period
* No more than one country will be affected concurrently by the same disaster
* Disaster occurs at the most vulnerable time for each business function
* Disaster recovery (DR) plan for an IT functional unit is already in place and tested
* Alternate staff and replacement equipment are available within planned timeframes

**Assessment of Capability Maturity**

**Business Impact Analysis (BIA) On Disruption Scenarios**

|  |
| --- |
| **BUSINESS IMPACT ANALYSIS:** The process of analysing business functions (i.e. the activities, and processes of an organisation to deliver product and services) and the effect that a disruption might have upon them.    **1. Critical Business function**    A function or activity to which priority must be given following an incident, in order to mitigate impacts on an entity’s key products and services which support the achievement of key business objectives.    **2. Information assets or critical IT System  at risk**    **3. IMPACT LEVELS**    Assess , consequence, likelihood and risk prioritisation  and assign a business impact level to that    **Level 1** Business functions is mission critical and must be available during all business hours. Online systems must be available 24 hours a day, seven days a week.  **Level 2** Business processes can survive without the business function for a short amount of time.  **Level 3** Business processes can survive without the business functions for a longer period of time.  **Level 4** Business processes can survive without the business functions for extended periods without collapse of business.    **4. MTD/MAO**  Maximum Tolerable Downtime (MTD) represents the amount of time that management can accept for business processes to be unavailable or disrupted.  **5. RTO**  Recovery Time Objective (RTO) defines the target restoration of a disrupted service within a period of time. Exceeding RTO would cause unacceptable impact to system resources.    **Essentially the RTO must ensure that the MTD and MAO are not exceeded** |

**Example scenario of this occurring for etricity:**

**Loss of data**

–source ransomware

|  |  |  |  |
| --- | --- | --- | --- |
| **Disruption Scenario: Loss of data** | | | |
| **Disruption Source** | **Risk of disruption source** (including detailed description of the risk) | **Existing controls or strategies** | **Vulnerabilities/**  **Potential Threat Vectors** |
| Ransomware | denied access to system or software | IT department performs patch management | Technological obsolescence  Staff negligence |
| Malware Infections |  | IT department performs patch management | Technological obsolescence  Staff negligence |
| DoS and DDoS attacks | downtime, loss of sensitive data | extranet VPN | Network Configurations |
| Software Corruption | loss of active data, potential corruption of stored data | Software updates | Technological Obsolescence |
| Human Error | - |  |  |
| Natural disaster risk | -Power loss  -damage to intellectual property  -loss of human resources | Insurance  Back-up data locations | Climate Change  Disaster Prone Areas (Inverloch - Flooding) |
|  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Disruption Scenario: Loss of data** | | | | | | |
| **Process Area** | **Critical Business Function (include business objective)** | **Information assets or critical IT System at risk** | **Business Impact (brief description)** | **Overall Impact level** | **MTD/MAO** | **RTO** |
| **Production** | Supply chain management (supplier to eTricity to consumers) |  | **-** | **Consequence:**  **Likelihood:**  **Risk rating:**  **Impact level:** |  |  |
| Design, manufacture and assemble | - product design  -manufacturing software  -machinery equipments  -RecShareOne enterprise system | -leakage to product design causing loss of product competitive edge  - machinery downtime snowballing to machinery error would result to repairment expense | **Consequence:**  **Likelihood:**  **Risk rating:**  **Impact level:** |  |  |
| **Sales** | Sales management (customer handling, distribution,  installation) | -RecShareOne  -Customer data  -Customer facing web server | -lost of sales opportunities  **-**customer data breach could result in fines and penalties, and loss of goodwill. | **Consequence:**  **Likelihood:**  **Risk rating:**  **Impact level:** |  |  |
| **Finance and Accounting** | Company finance management, transactions, budget approval | -Financial data  - Confidential banking details  - RecShareOne  - Accounts Reconciliation Officer Personal device  - Customer transaction records | **-**Delay in operational transactions, decision making, and overall productivity  - data transmission leakage of customer transaction records, from data warehouse to RecShareOne may result in fines and penalties, and loss of goodwill. | **Consequence:**  **Likelihood:**  **Risk rating:**  **Impact level:** |  |  |
| **IT** | Securing network and system infrastructure, protecting proprietary data |  | -data leakage may result in fines and penalties, and loss of goodwill. | **Consequence:**  **Likelihood:**  **Risk rating:**  **Impact level:** |  |  |
| Live report generation referring to eTricity products | -Jock’s Baby customer data warehouse | **-**downtime to live report results to customers dissatisfaction | **Consequence:**  **Likelihood:**  **Risk rating:**  **Impact level:** |  |  |
| **Human Resource** | Employee lifecycle management | -RecShareOne  -Employees personal information | **-**Employees are entitled to make claim if data breach causes mental or financial impact | **Consequence:**  **Likelihood:**  **Risk rating:**  **Impact level:** |  |  |

**Identify resource requirement**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area:: HR** | | | | |
| **Critical Business Function : Employee lifecycle management** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| RecShareOne |  |  |  |  |
| Human resource - HR manager |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: IT** | | | | |
| **Critical Business Function : Live report generation** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| Customer data management servers - Jock’s baby |  |  |  |  |
| eTric App |  |  |  |  |
| Home wall monitor |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: IT** | | | | |
| **Critical Business Function : Securing network and system infrastructure, protecting proprietary data** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| Human resource - IT, cybersecurity, data management team |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: Sales** | | | | |
| **Critical Business Function : Sales management (customer handling, distribution,  installation)** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| Enterprise system - RecShareOne |  |  |  |  |
| customer facing web server | Providing real-time analysis of electrical usage for customers |  |  |  |
| Human resource - Sub contractors | Onboarding new customers and installing hardware | Will be unable to enter new customers into the system | 100% |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: Finance and Accounting** | | | | |
| **Critical Business Function : Company finance management, transactions, budget approval** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| Enterprise system - RecShareOne |  |  |  |  |
| Computer Devices |  |  |  |  |
| Human resource - CFO, Accounts reconciliation officer |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: Production** | | | | |
| **Critical Business Function: Supply chain management (supplier to eTricity to consumers)** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| Enterprise resource - RecShareOne (records associated with exchange of purchasing orders and delivery) |  |  |  |  |
| customer facing web server |  |  |  |  |
| Email (maintaining supply chain for manufacturing and assembly in China) |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: Production** | | | | |
| **Critical Business Function: design, manufacture and assemble** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| eTric original designs (in filing cabinet) | original product design may be needed as a reference point for product enhancement | available. not impacted. | 20% | Original design may not be needed at all times. because:  1.it is outdated  2.newer products have been launched. more improved designs should be used as a reference point for further improvement. |
| Computer devices | - needed to enter production order, and other manufacturing data.  - to access software for prototyping, testing and command manufacturing process to machineries | computer encrypted, access denied |  |  |
| RecShareOne | all operational records associated with supplier-eTricity exchange are maintained in RecShareOne | system encrypted, access denied |  |  |
| Manufacturing devices | Equipments needed to assemble and manufacture products | operation may be paralysed for manufacturing equipments  operated by software |  |  |
| Human resource-  data entry clerks | required to maintain the information trail of important documents,subcontractors, contracts, suppliers, customers, orders, invoices, receipts, etc. | human resources availability are not impacted, however the associated operational function will be halted. Thus, affecting operational productivity |  |  |
| Human resource- solar engineers | required to  conduct design, manufacturing, assembling. commanding the machines what functions to perform | human resources availability are not impacted, however the associated operational function will be halted. Thus, affecting operational productivity |  |  |

* **network file sharing allows managers and other staff to store information such as invoices, purchase orders, or other information related to their suppliers and vendors.**

Since Ted had not been able to go through this part after wednesday, I am just finishing it up following the tables provided by cindy. Need her to do a final check on this part just to ensure all necessary information are presented here via the tables

**(Ragib START)-**

**Disruption Scenario Two: Loss of access to physical assets**

**Example scenario of this occurring for etricity:**

This can occur in various ways in etricity. Among them, the most likely way will be through a disaster like Storm or flood. That’s because Etricity is located in Inverloch on Bass Coast which is a place well known for wild winds, storms, floods and erratic weather events. Thus, if any such event occurs and damages any buildings hosting the company’s local server, workstations, etc. the employees will lose access to those devices and in turn lose access to the information assets stored locally in the devices. Although the company will be able to continue their operations by relying on previous backups, they will have to spend time and effort to not only gathers that information once more, but also on fixing the damaged devices. Thus the operational efficiency of the organization will be impacted.

|  |  |  |  |
| --- | --- | --- | --- |
| **Disruption Scenario: Loss of access to physical assets** | | | |
| **Disruption Source** | **Risk of disruption source** (including detailed description of the risk) | **Existing controls or strategies** | **Vulnerabilities/**  **Potential Threat Vectors** |
| Natural disaster risk | Loss of power  Damage to physical assets  Harm or loss of human life | Insurance  Back-up or redundant assets  First aid treatment and hospital | Climate Change causing unpredictable weather  Company is in Inverloch which is a disaster prone area known for flooding and storms |
| Network attacks (like malware, DDOS, etc.) | Denied access to use of physical assets (like servers, workstations, etc.)  loss of power  Damage to physical assets  Overload/ downtime of resources and services | IT department performs detective and preventive measures of threats by using suitable tools | It staff lack the necessary tools and also lack the proper network configuration  IT Staff negligence regarding tools and softwares used to defend against such threats  IT Staff not having proper knowledge regarding the attacks and preventive measures |
| Software Corruption | loss of access to physical assets due to fault in software | IT department performing regular software updates and applying patches | IT Staff lack the necessary tools and also lack the proper network configuration  IT Staff doesn’t know how the software functions in depth |
| Human Error | Damage to devices (like local servers,workstations, etc.) that hold information assets  Download of untrusted/ third party software | Proper training and awareness regarding use of organizational resources (both hardware and software) | Target of Phishing and pharming  Disgruntles employee  Lack of knowledge regarding use of certain tool |
| New technology or infrastructure | Loss of access to physical assets,  Damage to physical assets,  Error in linking or using new technology or infrastructure with old, proprietary assets | Insurance  IT department performing necessary modifications to allow seamless linkage | Staff negligence regarding new technology or infrastructure  Staff not knowing how the new technology or infrastructure  Staff being negligent regarding how the new technology or infrastructure is being setup and used |
| Financing, budgeting issue or theft | Loss of access to physical assets | Proper financing and budgeting plans,  Proper monitoring and punishing process  Insurance | Disgruntled employee  Employee in heavy debt  Budget and finance team not considering all assets in their profit and expense calculation |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Disruption Scenario: Loss of access to physical assets** | | | | | | |
| **Process Area** | **Critical Business Function (include business objective)** | **Information assets or critical IT System at risk** | **Business Impact (brief description)** | **Overall Impact level**  [following impact table for risk where High 7-10, Medium 4-6, Low 0-3] | **MTD/MAO** | **RTO** |
| **Production** | Supply chain management  (supplier 🡪 eTricity 🡪consumers) | Physical assets and resources (including BYODs, RecShareOne) related to supply chain | **Disruption of supply chain led to pausing the business activities as resources and information assets stored in the resources are in accessible** | Consequence:  Medium (5)  Likelihood:  Low (2)  Risk rating:  10  Impact level:  Low | Don’t let any disruption of supply chain assets (no matter how small) last more than 1 week | At least 75% of the most critical supply line assets should be functional within 48hrs |
| Design, manufacture and assemble | Assets and resources used to make prototype (like RecShareOne, Servers, etc) | **Halting the business due to lack of resources and assets to build the prototype**  **Loss of trust from customers who are waiting for the product** | **Consequence:**  High(7)  **Likelihood:**  Low (2)  **Risk rating:**  14  **Impact level:**  Low | Don’t let any disruption assets and resources(no matter how small) used to make prototype and products  last more than 48hrs | At least 80% of the most critical assets and resources should be functional within 24hrs |
| **Sales** | Sales management (customer handling, distribution,  installation) | Assets and resources that are:  a)sold to customers (the solar panels),  b)used distribute and install products at customer’s home (tools used by subbies, BYODs, etc.), c)communicate with customers, store sales data (sales database server, workstations, RecShareOne), etc. | **Loss of trust from customers**  **Decrease in company value in terms of money and reputation** | **Consequence:**  High(7)  **Likelihood:**  Medium(6)  **Risk rating:**  42  **Impact level:**  Medium | Don’t let any disruption assets and resources(no matter how small) last more than 48hrs | At least 90% of the most critical assets and resources should be functional within 24hrs |
| **Finance and Accounting** | Company finance management, transactions, budget approval | All Physical assets and resources themselves (like servers, workstations, money, etc). Also Assets used to maintain and process the financial and accounting data (RecShareOne) | **Halts business function as the assets and resources are effectively frozen and thus not usable either in transaction or to perform any form or transaction** | **Consequence:**  High(9)  **Likelihood:**  High(8)  **Risk rating:**  72  **Impact level:**  High | Don’t let any disruption assets and resources(no matter how small)  last more than 18hrs | At least 90% of the most critical assets and resources should be functional within 10hrs |
| **IT** | Securing network and system infrastructure, protecting proprietary data | Assets and resources (like network, servers, electrical lines, etc.) themselves which are used for these purposes | **Halts business function as these assets and resources make up the backbone of the company and without it company cannot function effectively** | **Consequence:**  High(9)  **Likelihood:**  High(9)  **Risk rating:**  81  **Impact level:**  High | Don’t let any disruption assets and resources(no matter how small)  last more than 12hrs | At least 90% of the most critical assets and resources should be functional within 6hrs |
| Live report generation referring to eTricity products | Assets and resources used to the generate report (ie solar panel sold to customers) and also devices that generate the report can be impacted (ie the new eTricStorage) | **Loss of customer trust**  **Also value of company in terms of money and reputation falls** | **Consequence:**  High(8)  **Likelihood:**  Low(2)  **Risk rating:**  16  **Impact level:**  **Low** | Don’t let any disruption assets and resources(no matter how small)  last more than 12hrs | At least 90% of the most critical assets and resources should be functional within 6hrs |
| **Human Resource** | Employee lifecycle management | Assets and Resources themselves (like workstation, equipment, etc. provided to employees), alongside assets used to process and store them (RecShareOne) | Loss of trust from employees, reducing their work efficiency and effectiveness  Value of company in terms of reputation and money falls | **Consequence:**  Medium(7)  **Likelihood:**  Medium(7)  **Risk rating:**  49  **Impact level:**  **Medium** | Don’t let any disruption assets and resources(no matter how small)  last more than 24hrs | At least 75% of the most critical assets and resources should be functional within 12hrs |

**Identify resource requirement**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area:: HR** | | | | |
| **Critical Business Function : Employee lifecycle management** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| RecShareOne |  |  |  |  |
| Human resource - HR manager |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: IT** | | | | |
| **Critical Business Function : Live report generation** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| Customer data management servers - Jock’s baby |  |  |  |  |
| eTric App |  |  |  |  |
| Home wall monitor |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: IT** | | | | |
| **Critical Business Function : Securing network and system infrastructure, protecting proprietary data** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| Human resource - IT, cybersecurity, data management team |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: Sales** | | | | |
| **Critical Business Function : Sales management (customer handling, distribution,  installation)** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| Enterprise system - RecShareOne |  |  |  |  |
| customer facing web server | Providing real-time analysis of electrical usage for customers |  |  |  |
| Human resource - Sub contractors | Onboarding new customers and installing hardware | Will be unable to enter new customers into the system | 100% |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: Finance and Accounting** | | | | |
| **Critical Business Function : Company finance management, transactions, budget approval** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| Enterprise system - RecShareOne |  |  |  |  |
| Computer Devices |  |  |  |  |
| Human resource - CFO, Accounts reconciliation officer |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: Production** | | | | |
| **Critical Business Function: Supply chain management (supplier to eTricity to consumers)** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| Enterprise resource - RecShareOne (records associated with exchange of purchasing orders and delivery) |  |  |  |  |
| customer facing web server |  |  |  |  |
| Email (maintaining supply chain for manufacturing and assembly in China) |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: Production** | | | | |
| **Critical Business Function: design, manufacture and assemble** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| eTric original designs (in filing cabinet) | original product design may be needed as a reference point for product enhancement | available. not impacted. | 20% | Original design may not be needed at all times. because:  1.it is outdated  2.newer products have been launched. more improved designs should be used as a reference point for further improvement. |
| Computer devices | - needed to enter production order, and other manufacturing data.  - to access software for prototyping, testing and command manufacturing process to machineries | computer encrypted, access denied |  |  |
| RecShareOne | all operational records associated with supplier-eTricity exchange are maintained in RecShareOne | system encrypted, access denied |  |  |
| Manufacturing devices | Equipments needed to assemble and manufacture products | operation may be paralysed for manufacturing equipments  operated by software |  |  |
| Human resource-  data entry clerks | required to maintain the information trail of important documents,subcontractors, contracts, suppliers, customers, orders, invoices, receipts, etc. | human resources availability are not impacted, however the associated operational function will be halted. Thus, affecting operational productivity |  |  |
| Human resource- solar engineers | required to  conduct design, manufacturing, assembling. commanding the machines what functions to perform | human resources availability are not impacted, however the associated operational function will be halted. Thus, affecting operational productivity |  |  |

* **network file sharing allows managers and other staff to store information such as invoices, purchase orders, or other information related to their suppliers and vendors.**

1. **Determine the disruption impact**

**[Ref:**HB 262-2006 **table 10 pg 63** ]

|  |  |
| --- | --- |
| **Class of Impact** | **Area of impact** |
| **Financial** | **Loss of potential revenue**  **Increased operational cost for the company (due to employment of any external recovery team, recollection of information, etc.)**  **Decrease in stock value**  **Causing inflexible budget** |
| **Non-Financial** | **Loss of corporate reputation and brand**  **Loss of stakeholder confidence and goodwill**  **Decrease in staff morale**  **Decrease in faith on management control and capability** |

**Step 2: Confirm critical business function–(name all “directly impacted” business areas)**

|  |  |
| --- | --- |
| **Critical Business Function** | **Description /Rationale** |
| Sales Function | **Sales areas of a company focus primarily on connecting with potential investors, clients, customers or sponsors with the goal of building brand awareness and generating revenue. For instance, in case of eTricity, they will focus on determining prices of the PV solar panel solutions, push out relevant advertisement and marketing regarding their products, etc…..**  **In case of this disruption scenario, the company will lose data that had been stored in their backup which would include sales and marketing data, statistical information regarding customers use of eTric system,etc. These are all crucial parts of the sales area of the company** |
| Finance and Accounting | The disruption scenario will also cause the company to lose information on employee salaries which have been paid, income and expense details, financial statements (like balance and loss statements),etc, which fall under finance and accounting area of the company |
| IT | This is one of the main areas that will be impacted as backup is mainly one of the functions that falls under the IT area of the company |
| Production and Purchasing | The disruption scenarios would affect backup files which would include product prototypes, designs specifications, subbies details, contracts,etc, all of which are related to this area of the company |

Step 3: Identify resource requirement

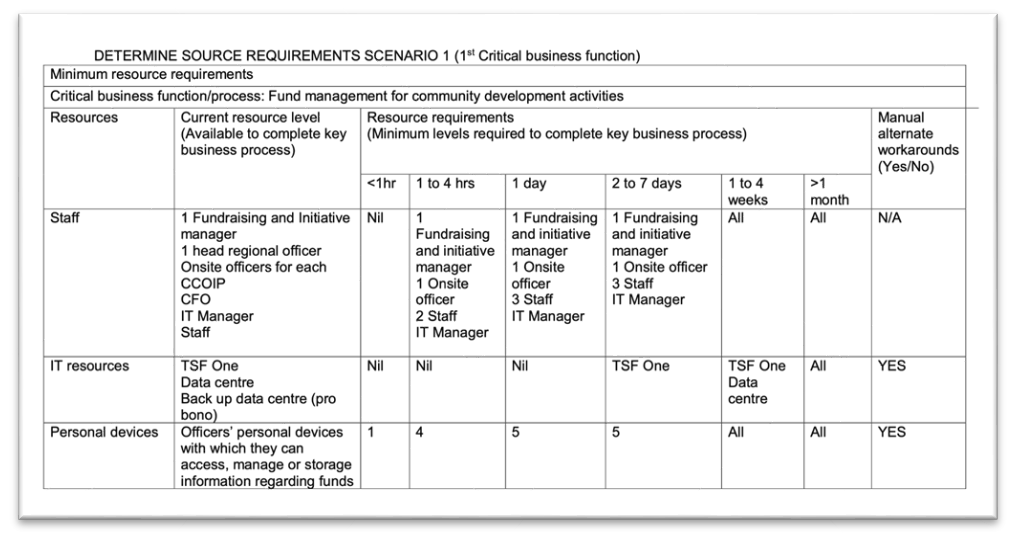
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: Production** | | | | |
| **Critical Business Function : Supply chain management; Design, Manufacture and Assemble** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| RecShareOne | Store the information of all company records |  |  |  |
| BYOD |  |  |  |  |
| Web server |  |  |  |  |
| Email server |  |  |  |  |
| eTric solar panel inverters, wall monitor and kit |  |  |  |  |
| eTricStorage |  |  |  |  |
| Manufacturing devices |  |  |  |  |
| Workstation, |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: Sales** | | | | |
| **Critical Business Function : Sales Management** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| RecShareOne |  |  |  |  |
| web server |  |  |  |  |
| smartphones, pcs and tablets |  |  |  |  |
| eTricStorage |  |  |  |  |
| BYOD |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: Finance and Accounting** | | | | |
| **Critical Business Function : Company finance management, transactions, budget approval** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| RecShareOne | Store the information of all company records |  |  |  |
| Workstation |  |  |  |  |
| etricity AU data warehouse |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: IT** | | | | |
| **Critical Business Function : Secure Infrastructure data, Live report generation** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| Customer data management servers |  |  |  |  |
| eTric App |  |  |  |  |
| Home wall monitor |  |  |  |  |
| Networking devices used to set up extranet and VPN infrastructure devices |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minimum Resource Requirements** | | | | |
| **Process Area: HR** | | | | |
| **Critical Business Function : Employee lifecycle management** | | | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** | **Resource requirements**  **(Minimum levels required to complete key business process)** | **Rationale** |
|
| RecShareOne |  |  |  |  |
| workstation |  |  |  |  |



…….

|  |  |  |
| --- | --- | --- |
| **Minimum Resource Requirements** | | |
| **Process Area: Production** | | |
| **Critical Business Function : Supply chain management** | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** |
|
| RecShareOne | All operational records  related to supply exchange are stored in RecShareOne | Partner portal and remote network access |
| Human resource management | Select suppliers and communicate with the related parties | Not affected |

|  |  |  |
| --- | --- | --- |
| **Minimum Resource Requirements** | | |
| **Process Area: Production** | | |
| **Critical Business Function : Design, manufacture and assemble** | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** |
|
| RecShareOne | Store, protect, manage and transmit patented designs | Partner portal and remote network access |
| Human resource management | Select suppliers and communicate with the related parties | Not affected |
| Guangdong assembler | Receive and assemble the selected components |  |

|  |  |  |
| --- | --- | --- |
| **Minimum Resource Requirements** | | |
| **Process Area: Sales** | | |
| **Critical Business Function : Sales management** | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** |
|
| RecShareOne | The heart of  the company, holding the data of various information of the company |  |
| Licensed subcontractors | Responsible for distribution and installations of eTric units to households |  |
| Web server | Means of information between the company and the customers |  |

|  |  |  |
| --- | --- | --- |
| **Minimum Resource Requirements** | | |
| **Process Area: Finance and accounting** | | |
| **Critical Business Function : Company finance management, transactions and budget approval** | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** |
|
| RecShareOne | All operational records  related to supply exchange are stored in RecShareOne |  |
| eTricity AU Data Warehouse |  |  |

|  |  |  |
| --- | --- | --- |
| **Minimum Resource Requirements** | | |
| **Process Area: IT** | | |
| **Critical Business Function : Securing network and system infrastructure, protecting proprietary data** | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** |
|
| RecShareOne | The heart of  the company, holding the data of various information of the company |  |
| Human resource - HR manager |  |  |

|  |  |  |
| --- | --- | --- |
| **Minimum Resource Requirements** | | |
| **Process Area: IT** | | |
| **Critical Business Function : Live report generation** | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** |
|
| RecShareOne | The heart of  the company, holding the data of various information of the company |  |
| Human resource - HR manager |  |  |

|  |  |  |
| --- | --- | --- |
| **Minimum Resource Requirements** | | |
| **Process Area: Human resources** | | |
| **Critical Business Function : Employee lifecycle management** | | |
| **Resource required to perform function** | **How resource is associated to perform function** | **Resource availability /impact  in case of scenario** |
|
| RecShareOne | The heart of  the company, holding the data of various information of the company |  |
| Human resource - HR manager |  |  |

Step 3: Identify resource requirement

……….

**Step 4: Establish Interdependencies (Mapping)**

**Although all the directly impacted business areas had been mentioned in the very first step, this is not the only area of impact for this disruption. That's because all the areas of a business are interconnected, just like a spiderweb!**

**Hence, it is not too surprising to realise that the Human resource area is also impacted by this disruption. After all, this area focuses on eTricity’s employees side including their performance, benefits provided to them, claims or allegations, laws regarding them, etc in order to maintain the organizational culture. Thus, the impacts on Sales, and Finance and Accounting areas, would end up impacting employees which in turn would end up impacting the HR area as well!**

**Section 4**:

**Incident Response Plan**

**2 Incident Handling Procedures**

**Scenario 1 : Ransomware**

* **Before the incident**
* **Incident Detection and analysis**
* **During**
* **After**

**Incident Detection and Analysis**

* incident detection

Detection of Ransomware often  involves:

* precursors
* indicators
* security monitoring

|  |  |
| --- | --- |
| **Indicators** | **Example** |
| SAMPLE.  Reports of unusual or suspicious activity by staff or external stakeholders. | A staff member receives an email asking them to confirm their network credentials or to provide other personal or sensitive information. |
| Multiple staff report being ‘locked out’ of their network accounts. |
| An external stakeholder reports receiving spam or phishing emails from your organisation. |
| A member of the public approaches your organisation to report the discovery (or exploitation) of a security vulnerability. |

* Incident Analysis

analysis to confirming presence of  incident

|  |  |
| --- | --- |
| **Actions** | **Description** |
| SAMPLE. Reviewing log entries and security alerts | Are there any unusual entries or signs of suspicious behavior on the network or applications? |

Ragib Start

**########################################################################**

**I am just finishing this part up following the table shown in f2f class. Need Cindy to go through and check it to ensure all necessary information are presented here via the tables.**

**++ Need her to explain what she meant by incident detection and analysis, whether it’s a part of before or standalone type module? + whether we really need it or not**

**Currently doing it without it. So need her help to fix that part on sunday**

**##########################################################################**

**Scenario 2 : Loss of access to Physical Asset**

* Before the incident

Users

Don’t download, open or forward suspicious files, software or attachments from any website or email on company device (like on company server),

Don’t damage the assets and resources being utilized by the company any way. This includes (but are not limited to) servers, workstation, wirings, network devices, etc.

Follow any predefined policy regarding the usability of any physical asset

Report any potential of damage that can occur or has occurred on company asset or resources

Follow the protocols and timings noted in maintenance policies and perform timely maintenance to organizational assets, alongside notifying others about the matter on a timely basis

Technology services

Perform proper usability, maintenance and performance testing on the all organizational assets

Set up timers and threshold in the assets to automate the maintenance and repair process, before loss of access to asset occurs

Set up proper database to monitor number, names, location, last maintenance date and use of all assets and resources, alongside names of groups who should and shouldn’t have access to them

* During

Users

Note down the time when loss of access had been detected

Note down access to which asset have been lost alongside whether any alternative access methods is working or not (like if access to RecShareOne though BYOD has been lost, try checking whether it is the same case on company workstations)

Determine whether access has been lost due to personal device issue (like not being connected to company network while trying to access) or due to company asset or resource issue

Contact IT Staff immediately regarding the matter detailing the case within the best of your ability

Technology services

If reports of issue have been noted, determine the scope of loss of access to the asset by asking the following questions:

What type of asset was it?

How many assets have been impacted by it?

Are the affected assets linked or independent?

How many users have lost access?

Was it a business critical asset or resource?

Was it business critical?

Was there any loss or lack of maintenance (like software update) on the asset?

Is the asset affected by time durations (ie permanent or temporary asset)?

Begin troubleshooting of the issue by using relevant technical tools, softwares and techniques via the deployment of the response team to inspect the asset in question

* After

Users

Continuously monitor assets and resources being used and review their last maintenance date, performance level, damage level, etc.

Note down details about the incident, the reason behind it and the solution proposed by the IT Staff and follow it diligently

Share the information regarding the problem and solution with your colleagues so as to raise awareness regarding the issue and its solutions

Technology services

Conduct proper response plan regarding the issue and note down the specific method or technique used to resolve it in a detailed, yet simple to understand format

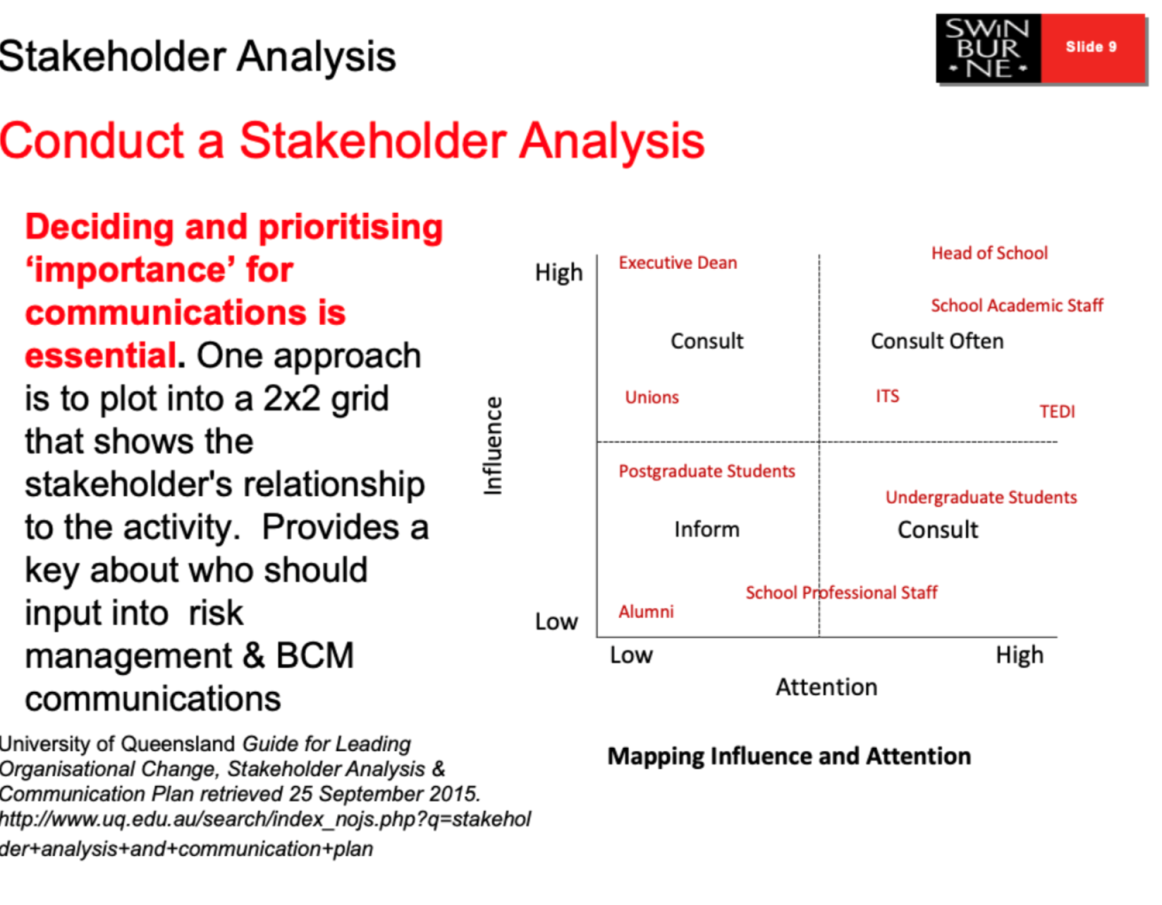
Discuss about the issue that lead to the loss of access and its solution with not only currently impacted users but also ones who may be impacted by the similar issue in the future via interview

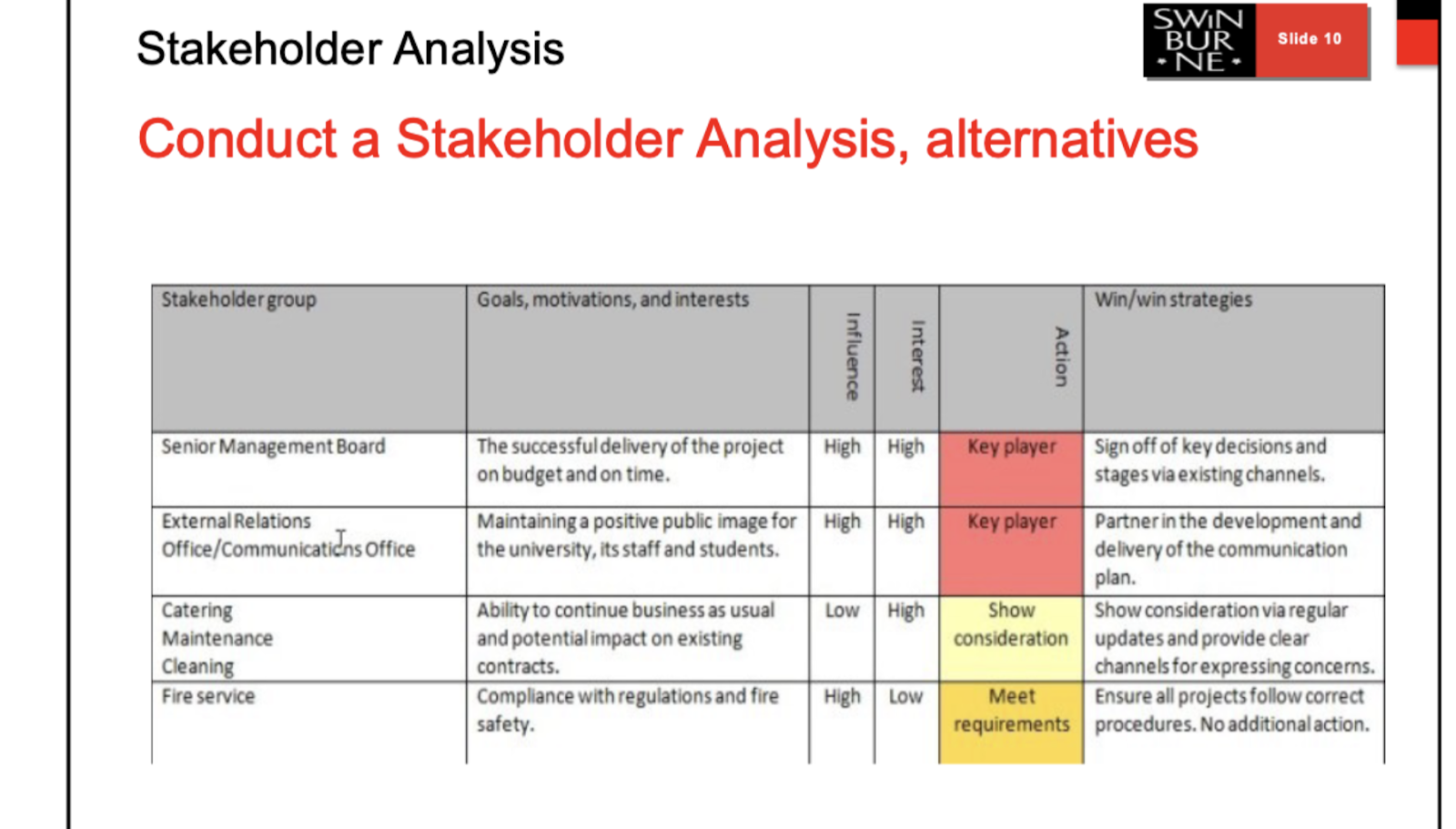
Ensure that the issue has been completely resolved by performing necessary verifications, testing, etc. of the asset

Notify everyone that the issue has been resolved, alongside letting them know where details regarding the source of issue and solution have been noted

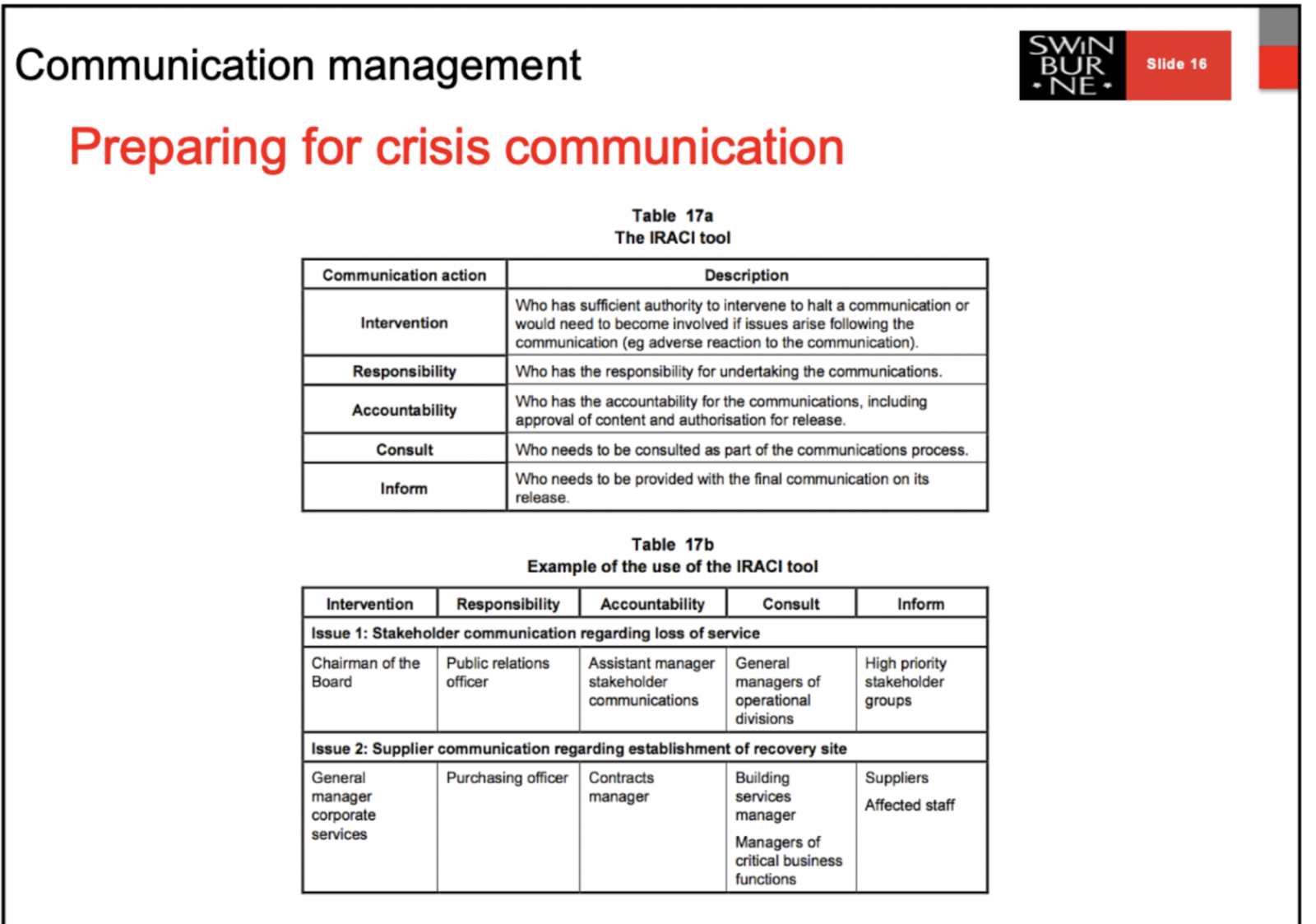
Ragib End

**Stakeholder analysis**

****

****

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Stakeholder group** | **Goals, motivation, and interests** | **Influence** | **Interest** | **Action** | **Win/win strategies** |
| Board of Directors | Ensure return to investments |  |  |  |  |
| Customers | Consume products/services best to fulfill needs/desires without compromising |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

****

|  |  |
| --- | --- |
| **Communication action** | **Description** |
| **Intervention** |  |
| **Responsibility** |  |
| **Accountability** |  |
| **Consult** |  |
| **Inform** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Intervention** | **Responsibility** | **Accountability** | **Consult** | **Inform** |
| **Issue 1:** | | | | |
|  |  |  |  |  |
| **Issue 2:** | | | | |
|  |  |  |  |  |