THE UNIVERSITY OF AUCKLAND RESILIENCE MANAGEMENT PLAN

29 July 2013
vP1.1

LIST OF CONTENTS

1. EMERGENCY PROCEDURES SUMMARY

A range of emergency fire / evacuation notices are posted throughout Campus sites. In addition, there are numerous safety & emergency response plans and procedures that apply to specific Faculty & Service Division operations. This page summarises some generic procedures. Further details can be found in the various emergency procedures guides, manuals and contingency plans.

IN CASE OF FIRE:

1. **Sound alarm and warn other people.**
2. **Dial (1) 111 and give details.**
3. **Evacuate to nominated assembly areas and remain there until all clear.**

IN CASE OF EARTHQUAKE:

1. **If indoors stay there and move clear of obvious hazards.**
2. **If out doors move clear of obvious hazards.**

When shaking stops:

3. **Check other people and treat injuries etc.**
4. **Deal with other hazards created by earthquake, e.g. Fires, electrical hazards, etc.**

IN CASE OF ACCIDENT:

1. **Arrange or render First Aid.**
2. **Call ambulance (1) 111 if needed.**
3. **Notify Security at UNISAFE ph x85000 or (1) 923 5000.**
4. **Ensure accident scene is safe.**
5. **DO NOT DISTURB THE SCENE.**

If serious harm has occurred:

6. **Notify Security at UNISAFE ph x85000 or (1) 923 5000.**
7. **Notify Health & Safety Manager.**
8. **Responsible Manager to make Mandatory Notifications and reporting to OSH (refer Health & Safety Manager).**

IN CASE OF POWER CUT

1. **Evacuate the building if instructed to do so.**
2. **In the event the power is out for more than 30 mins, and there have been no instructions, make your way out of the building.**

IN CASE OF HAZARDOUS SUBSTANCE EMERGENCY / CHEMICAL SPILL

1. **Withdraw from the area and raise the alarm.**
2. **In the event of an emergency or major spill call (1) 111 and give details.**
3. **Render first aid if it is safe to do so.**
4. **Isolate and contain the spill if it is safe to do so, if you are a trained & equipped responder.**
5. **Notify Security at UNISAFE ph x85000 or (1) 923 5000.**
6. **Notify Lab Manager or Hazards & Containment Manager.**

EMERGENCY SIGNAL

Continuous ringing of Alarm Bell or an audible evacuation instruction (this signal varies from site to site).

ALL CLEAR SIGNAL

Verbal message to Fire Wardens to notify staff it is safe to return.

2. INTRODUCTION

2.1 Context

The purpose of The University of Auckland (UoA) Resilience Management Plan is to set out the key elements that comprise the University approach to responding to an emergency or business interruption.

UoA Resilience Management Plan sets out the overall resilience framework and principles applying to the University's people, places and systems. It fits within the University's Risk Management Framework. As set out in that framework, all Faculty/ SD Managers are responsible for managing their own risk in their activities and operations (i.e. are the Risk Owners).

Resilience management is a type of risk management and is a generic term. Other terms used to describe aspects of resilience management include:

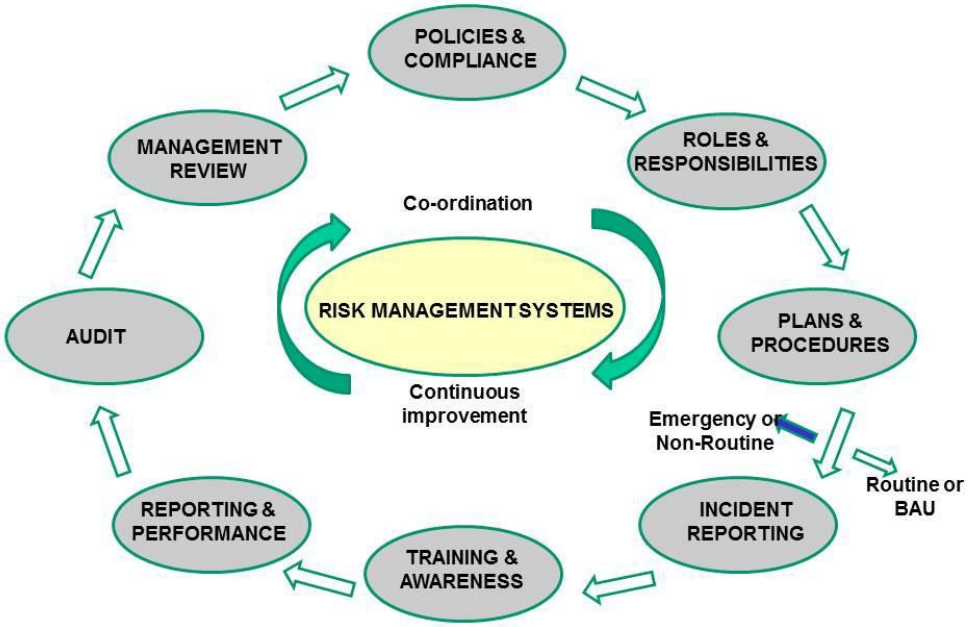
- Emergency management
- Crisis management
- Disaster management
- Business continuity management
- Contingency planning
- And many more.

Recapping the Risk Management Framework

The University of Auckland (UoA) Risk Framework is our overall system for the management of risk, resilience & security. It follows a quality system model, and is consistent with standards for risk, hazard, resilience and security risk management.

Figure 1 shows the elements of a typical risk framework which include: policies; compliance; roles & responsibilities; plans & procedures; incident reporting & investigation; training & awareness; measuring & reporting performance; audit and management review.

FIGURE 1: HOW TO MANAGE RISK



High Level Objective

All material risks to UoA staff, students, facilities, and interests are identified and appropriately managed, using best practice. To achieve this objective UoA shall meet the following strategic risk outcomes.

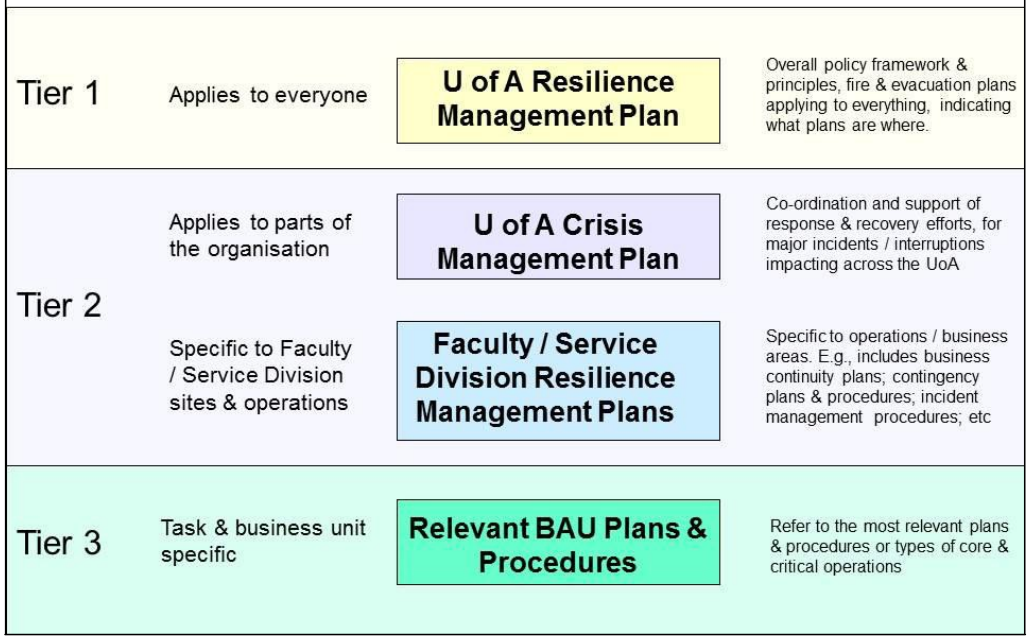
Risk Outcomes

1. To provide a duty of care to students, staff and the public
2. To provide a safe, secure and hazard free environment and facilities
3. To maintain, protect and promote the interests and reputation of UoA as it conducts teaching, learning and research
4. To operate in a financially responsible manner that ensures the efficient use of resources and maintains UoA's long term viability
5. To preserve the University's autonomy and role as critic and conscience of society

6. To meet compliance requirements (legal, civil, commercial and core business)
7. To provide and maintain resilient systems, facilities and people
8. To maintain and protect funding streams / revenue
9. To protect intellectual property and intellectual capital
10. To be a good corporate citizen – social, corporate, ethical and environmental responsibility.

Figure 2 shows the relationship between this University Resilience Management Plan and other resilience management & response plans in place across the University.

FIGURE 2: RESILIENCE MANAGEMENT PLAN RELATIONSHIPS



Definitions
For the purposes of this Plan, the following definitions apply:

Resilience
Resilience is the ability of the University's people, places and systems to return to business as usual after an emergency and or interruption.

Emergency
An emergency is any unplanned event that can cause deaths or significant injuries to employees, students or the public; or that can shutdown University systems, sites, disrupt operations, or cause physical or environmental damage.

Business Interruption
A business interruption is any unplanned event that can cause more than minor disruption to business as usual (BAU) operations.

Business Continuity Management
Business Continuity Management is an ongoing process that is supported by senior management, comprising all Business Continuity Planning, practices and processes. This includes the development, implementation and maintenance of strategies, plans, resources and actions to secure a managed response to an unexpected incident that impacts the operation of the University's critical processes.

Crisis
A crisis is an emergency or business interruption that has significant organisational implications, and requires whole of organisation resources and or coordination.

In such circumstances, the UoA Crisis Management Plan is activated. In the context of the UoA Emergency Management Statute 2007 (set out below), a crisis is an "emergency" as defined in that Statute.

The University of Auckland Emergency Management Statute 2007
The Statute sets out the delegations to support the governance and management of the University for the duration of an emergency and any recovery period.

In the Statute, "emergency" is defined as follows, in section 1.1 of the Statute:

"Emergency means an event, occurrence or circumstance beyond the control of the Council that:

a) Adversely affects the premises, buildings or facilities of the University; or its supporting infrastructure; or its staff of students; such that a substantial part or parts of the University are required to close, be quarantined or restricted (at the behest of any local or national authority or voluntarily) for a period of more than five days; and / or

b) Prevents the delivery or undertaking of normal day to day management functions; and

c) Is declared such by the Council or (where for any reason the Council cannot pass a resolution, whether or not in a meeting) by the Emergency Cabinet.

An Emergency includes such reasonable recovery periods following any closure, quarantine or restriction as may be necessary to ensure the University is capable of resuming its normal day to day management and governance functions, in whole or part."

In the event an Emergency was declared under the Statute, the UoA Crisis Management Plan would support the Emergency Cabinet in the conduct of their duties and decision-making.

2.2 University Resilience Management Policy

1. The University will ensure that it is able to function to the fullest possible extent, even though this may be at a reduced level, during and after an emergency and / or business interruption event.

2. The University will achieve this by:
   - Maintaining effective resilience management systems to mitigate the adverse effects of interruption events and to enable timely and effective return to business as usual conditions; and
   - Maintaining resilience response plans that enable timely and effective response to emergency and / or business interruptions.

3. The University will regularly assess resilience risk across its organisation and operations to identify the critical functions and priorities for response and recovery efforts.

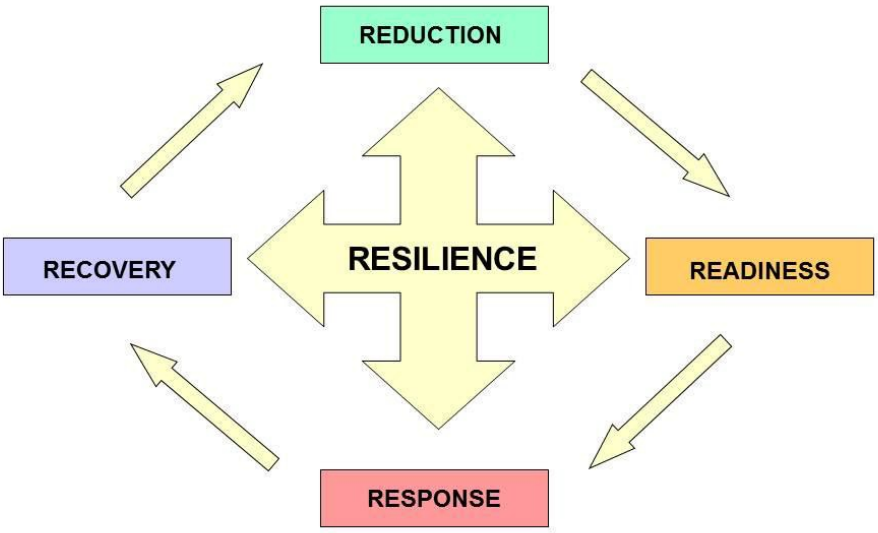
4. The University's response priorities are:
   1. Safety & security of people;
   2. Protecting critical infrastructure and services;
   3. Maintaining the Universities core business functions of research; and teaching and learning; and
   4. Protecting the environment.

2.3 Resilience Management Systems

Figure 3 shows the "4R's" of resilience, which underpin New Zealand's approach to resilience management:

- **Reduction** – those measures to prevent or reduce resilience risk, which are captured in the University risk management programme
- **Readiness** – pre-planning risk based scenarios, and formulation of plans and procedures
- **Response** – the organization, processes, equipment, systems and procedures to respond to an interruption event and or an emergency
- **Recovery** – those measures required to move out of the emergency phase of an event, and to return to business as usual, and to re-establish readiness. Learnings from the response then feed into corrective action required, to better manage the resilience risk and to prepare for and respond more effectively in the future.

FIGURE 3 - 4 R'S OF RESILIENCE

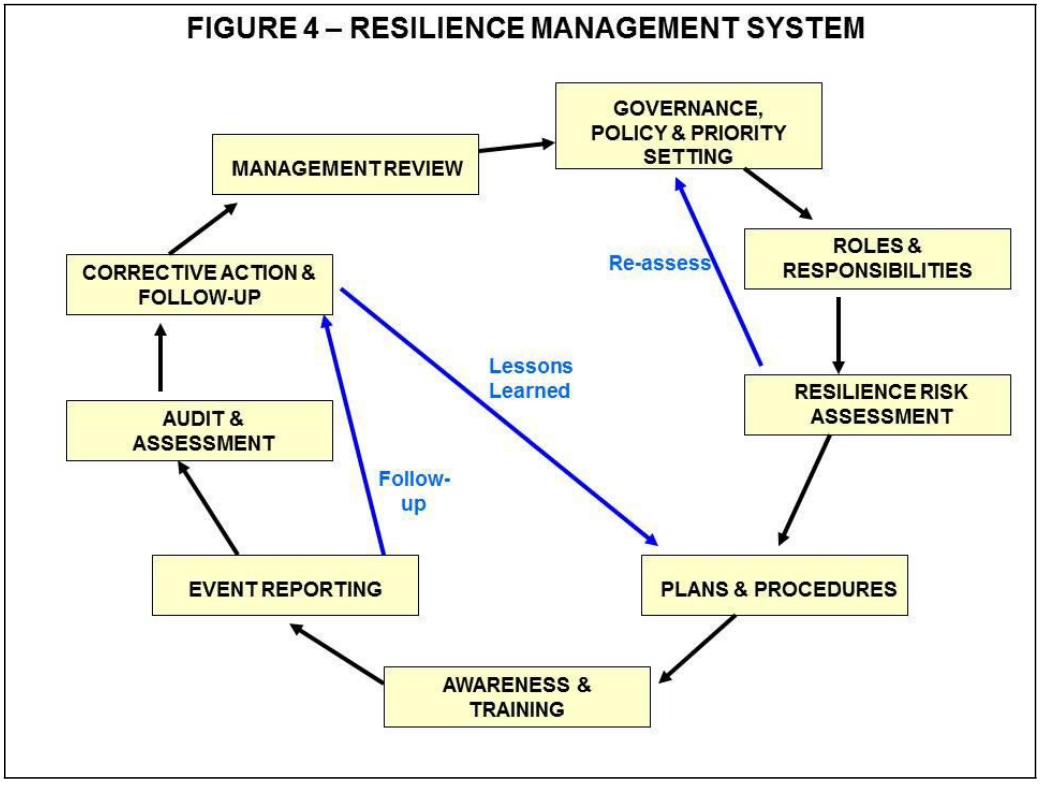


The Resilience Management programme is part of UoA's risk management framework. Resilience risks are captured by the risk framework processes and practices.

The UoA Resilience Management System is the tool UoA uses to ensure it is able to continue functioning during and after an interruption to business or an emergency.

Figure 4 shows the elements of the system. It comprises a suite of policies, processes, plans and procedures that are kept updated, tested and continuously improved.

FIGURE 4 – RESILIENCE MANAGEMENT SYSTEM



Elements include:

- Governance, policy & priority setting (part of the University risk management framework process)
- Roles and responsibilities
- Resilience risk assessment (part of the University risk management framework process)

- Plans and procedures
- Awareness and training
- Event reporting
- Audit & assessment
- Corrective action and follow-up, including lessons learned
- Management review.

These themes are discussed in this Plan.

2.4 Applicable Plans

It is the role of the Risk Office, under the leadership of the Director of Organisational Performance & Chief Information Officer – DOPCIO (and also Director of the Risk Office), to determine, alongside the F/SD Manager where Resilience Response Plans are required. Plans are prepared by the F/SD with input and guidance from the Risk Office.

This Plan (The University of Auckland Resilience Management Plan) sets out guidance for F/SD Managers to prepare their own Resilience Response Plans and/ or to ensure their relevant emergency, response, contingency and business continuity plans and procedures harmonise with it.

Key resilience response, contingency plans and procedures held at critical parts of UoA are described below.

The University of Auckland – whole of organisation:

- The University of Auckland Resilience Management Plan [this plan]
- The University of Auckland Crisis Management Plan
- The University of Auckland emergency, fire & evacuation plans & procedures.

F/SD's that hold relevant resilience response & contingency plans include:

- Business continuity plans – all F/SD's
- Hazardous facility response plans & procedures (chemical, bio-containment, biosecurity, radiological) – applying to the Faculties of Science, Engineering and Health & Medical Sciences.
- Information Technology Services incident management, contingency & disaster recovery plans & procedures - ITS

- Security response & contingency plans & procedures – Property Services
- Student Critical Incident Response Plan – Campus Life & International Office
- Teaching & Learning Recovery – DVC (Academic)

3. ABOUT RESILIENCE RESPONSE

3.1 Resilience Response Process

Faculty/ Service Division & site resilience response plans set out the way UoA responds to emergencies and interruption events, using a "4R's" approach (reduction, readiness, response and recovery), shown on Figure 3.

These plans refer to other BAU plans and procedures as appropriate, and focus on how UoA BAU critical services can be delivered during an emergency and or business interruption event.

Figure 5 shows the resilience response process. This process goes through a familiar series of phases to resolve the event, consistent with standard incident & emergency management disciplines. These phases include:

- **Raising the alarm / observation**. Knowing the event has occurred; and making emergency notifications as soon as possible, e.g., to emergency services if there is a need for fire, ambulance and or police response;

- **Activate / notify**. The observer (e.g. site worker, auditor or even a member of the public) notifies the F/SD Manager. The F/SD Manager makes the decision about the event level (i.e., its potential consequences), and if necessary activates the Resilience Response Plan. As shown in Section 4, the F/SD Manager lets UoA Management / Risk Office know in a timely manner;

- **Emergency phase**. Where there is imminent danger to staff, fire wardens facilitate evacuation, and first-aider's render first aid. This is the "fire & evacuation" phase, set out in notices posted around the campus, as part of the mandated health & safety management system;

- **Stabilise**. The F/SD response team carry out the pre-planned actions to stabilise the situation, under the control of the nominated Incident Co-ordinator (IC) (the F/SD Manager delegatee or alternate);

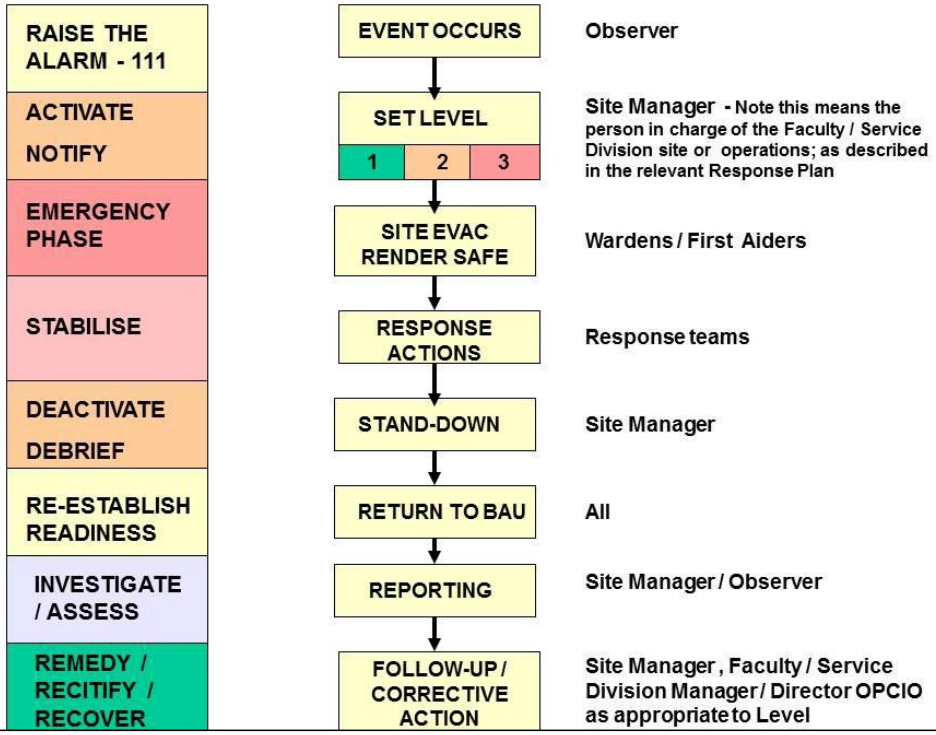
- **Deactivate**. The IC formally stands down the response, so everyone knows the response is over; and conducts a hot debrief; the initial debrief immediately after deactivation to poll impressions and learnings from the response team.

- **Re-establish readiness**. Things return to a BAU footing. Measures are taken to re-establish readiness; e.g., equipment and resources are replenished, and if necessary, undergo inspection and maintenance;

- **Investigate / assess**. The F/SD Manager, IC, incident observer and response staff contribute to the formal event report and investigation, and an evaluation of the response. Reports are kept on file, and available on request to the Director OPCIO.

- **Remedy / rectify / recover**. The F/SD Manager initiates any corrective action, or follow-up actions, in order to improve resilience. If appropriate the F/SD Manager formulates a lessons learned communication in association with the Risk Office.

FIGURE 5 – RESILIENCE RESPONSE PROCESS



3.2 Resilience Response Plan Elements

Resilience Response Plans are prepared by Faculties/ Service Divisions for their key processes and systems. These response plans can be in any form the F/SD's determine appropriate to what they do, and the arrangements they have in place for managing their resilience.

The Risk Office advises that effective resilience response arrangements include the following elements:

- A clearly defined purpose and scope of the plan
- Description of the types of scenarios and events the F/SD are preparing to respond to, which arise out of the resilience risk assessment
- Defined levels of emergency or interruption event, and points at which the plan is activated, and when and who are notified
- A clearly defined response organisation
- Linkages and arrangements with other parts of UoA or beyond UoA (e.g., Memoranda of Understanding)
- Contact details of those with key roles in the response (including nominated alternates)
- Articulated responsibilities and authorities of all involved in the response
- Critical equipment and systems required for the response
- Means of communicating with the staff, students and public regarding the status of the emergency – at activation, during the event, and when the event is over (stand-down)
- Measures for re-establishing readiness, testing and maintenance of response and communications equipment
- Measures required for life safety
- Training and awareness arrangements for those involved in the response
- A testing and exercise programme, that aims to test all elements in the plan within a 3 year cycle
- Arrangements for assessing the effectiveness of the response, and lessons learned
- Arrangements for event follow-up and corrective action
- Regular reviews and updating of the plans.

The Risk Office provides advice and support for F/SD in the preparation and updating of plans. As part of the risk management framework processes, the Risk Office also assists / advises as required with resilience risk assessments, testing, and corrective action / follow-up programmes.

4. ACTIVATION & NOTIFICATIONS

4.1 Determining Activation Levels

Each Faculty / Service Division determines the appropriate level of emergency and notification for the scenarios relating to their operations, as part of the planning and resilience risk assessment process. The levels are described below.

Figure 6 shows the event level, with indicative potential interrupt durations and notifications timeframes. Event levels at minor, moderate and major are calibrated by F/SD's in their plans, and determined by the scenarios the plan cover, and the types of critical function that can be potentially impacted.

FIGURE 6: EVENT LEVEL & RISK OFFICE / MANAGEMENT NOTIFICATION

STATUS	EVENT / EMERGENCY	INDICATIVE POTENTIAL INTERRUPT DURATION*	NOTIFY MGMT / DIR. OPCIO
LEVEL 3	MAJOR	> 5 DAYS	< 60 mins
LEVEL 2	MODERATE	< 5 DAYS	< 4 hours
LEVEL 1	MINOR	< 4 HOURS	< 5 working days
BUSINESS AS USUAL (BAU)			

*- As specified in response plans – this will vary between critical functions; and Faculty / Service Divisions

MGMT – management ; DIR OPCIO – Director Organisational Performance & Chief Information Officer (who is the Director of the Risk Office)

The work done by F/SD's as part of their business continuity planning process identifies critical business functions across UoA and the significant interruption

periods for key scenarios that constitute a minor, moderate or major interruption duration.

The objective of this pre-planned and staged notification process is to ensure that the Risk Office and the Faculty/Service Division Management learn about emergency and or interruption events in a timely manner. UoA Management, facilitated by the Risk Office, can then determine the implications for UoA and also be available to offer the assistance and resources the Faculty / Service Division will need to return to business as usual in the most timely and effective manner.

In addition, the Risk Office and Management are required to follow UoA risk disclosure framework, and notify management and governance depending on the risk and implications of the particular emergency and or interruption.

Level 1 events are minor, and are dealt with by the F/SD, and do not require additional resources for managing the event, and have a minor impact on UoA. Reporting / notification to management happens in the usual way as part of the BAU arrangements, and via the weekly UoA Situational Awareness reporting process that is coordinated by the Risk Office.

Level 2 events are moderate, and include those that require any type of mandatory notification to a government or law enforcement agency (for example Occupational Safety & Health, Ministry of Business, Innovation and Employment, or the Ministry for Primary Industries). The events effects may extent into or adversely affect other parts of the University operations and services. For these types of events the Risk Office is notified, and maintains a watching brief in case the event escalates to Level 3. Formal reporting is required to the Risk Office during and following the event.

Level 3 events are major. Impacts of the emergency or the interruption to critical services are likely to be significant. It will require external resources such as the emergency services and / or specialist response services. It also includes an emergency and or an interruption that happens outside of UoA, but significantly affects UoA (such as a natural disaster or major infrastructure failure). The Risk Office is notified as soon as possible, and the Director OPCIO or the Vice Chancellor determines whether the University Crisis Management Plan needs to be activated, and convenes the Crisis Management Team, as described in that Plan.

4.2 Mandatory Notifications

Pre-planned procedures and protocols specify the mandatory notifications that are required, depending on the circumstances; to whom; how soon; who will make the call; and reporting / documentation that is required. Some of the more common ones are set out below. These will vary from operation to operation.

TABLE 1: MANDATORY NOTIFICATIONS

Type of Incident	Caller	Who to Call	Situation	Timeframe
Fire / Ambulance / Police Emergency	Observer	(1) 111 Operator Security UNISAFE ph. x85000 or (1) 923 5000	Any emergency	As soon as possible after incident
Serious harm injury	Business unit supervisor / manager	(1) 111 Operator Security UNISAFE ph x85000 or (1) 923 5000 Health & Safety Manager Faculty / Business Unit Manager OSH - MBIE	Serious harm injury – any loss of consciousness; incident involving chemicals; where emergency services attend; where attendance at emergency room or hospital is required	As soon as possible after incident
Hazardous substance / chemical incident	Observer Business unit / lab manager / supervisor	(1) 111 Operator Security UNISAFE ph x85000 or (1) 923 5000 Hazards & Containment Manager	Any spill; suspicious fumes / smells, theft of chemicals or equipment	As soon as possible after incident
Radiological or radioactive source incident	Observer Business unit / lab manager / supervisor	(1) 111 Operator Security UNISAFE ph x85000 or (1) 923 5000 Hazards & Containment Manager Office of Radiation Safety (formerly National Radiation Laboratory)	Any incident: lost source, spill, loss of containment, contaminated or exposed personnel	As soon as possible after incident
Biosecurity breach	Business unit supervisor / manager	Hazards & Containment Manager Ministry of Primary Industries	Biosecurity or quarantine breach incident	As soon as possible after incident

Occupational Safety & Health, Ministry of Business, Innovation & Employment, Formerly Dept. of Labour

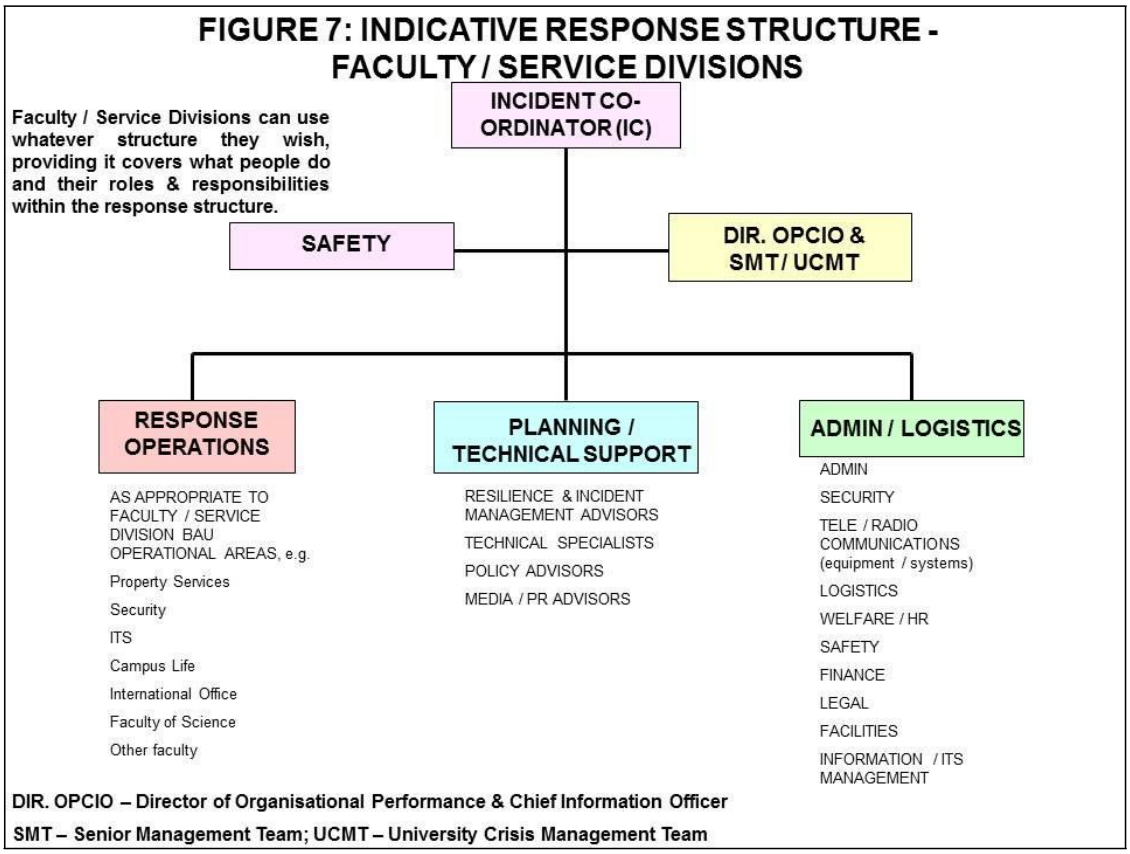
5. RESPONSE ORGANISATION

5.1 Response Structures & Actions

Indicative Response Structure

Figure 7 sets out an indicative response structure. The type of response structure will depend on the specific operations and scenarios, and is up to whatever works for the Faculty / Service Division. Actual arrangements are set out in plans and procedures. Generic guidance is provided below.

FIGURE 7: INDICATIVE RESPONSE STRUCTURE - FACULTY / SERVICE DIVISIONS



Someone needs to be in charge. This person is nominated by the F/SD Manager, and is usually referred to as the Incident Co-ordinator. Section 5.2 provides further guidance regarding roles, responsibilities and authorities.

The types of tasks that need to be carried out are:

- **Duty of care** - advice to the person in charge re: safety & security matters, to ensure the duty of care to all those involved in the response, and the public who could be affected;
- **A linkage** into the University resources and support, and for major events, the Crisis Management Team – this is coordinated by the Director OPCIO;
- **Operations** (i. e., those carrying out the actual response);
- **Planning / technical support** (those advising the people in charge and the responders; and
- **Administration / logistics** (those enabling the response to happen, with money, resources, logistics, telecommunications, technical support and things).

Faculty / Service Division Response Team Key Actions

Key actions to be taken in emergency and business interruption events are set out in F/SD plans and procedures. The following steps are generic, and identify activation, notification, and de-activation decision points.

All Events

1. Person in charge of the site / operation (the "Responsible Person") is notified of the event.
2. The Responsible Person determines the Level of the Event, and notifies the F/SD Manager.
3. If Level 1, the F/SD Manager resolves the event under BAU.

Level 2

4. F/SD Manager determines what additional resources are required from the University and contacts the Director OPCIO.
5. The F/SD Manager manages the event, as described in their Resilience Response plans & procedures.
6. The Director OPCIO puts the University Crisis Management Team (UCMT) on alert.
7. The Director OPCIO or the Vice Chancellor decides whether to activate the University Crisis Management Team, and whether to escalate response to Level 3.

Level 3

8. The F/SD Manager manages the event, as described in their Resilience Response plans & procedures

9. The Director OPCIO or the Vice Chancellor activates the University Crisis Management Team, sets priorities and provides resources, coordination and advice to the F/SD Manager who is coordinating their response.

Stand-down & review

10. The F/SD Manager determines when the event is over and to return to BAU. The F/SD Manager formally stands down the event.
11. The F/SD Manager conducts debrief, re-establishes preparedness and reports on F/SD response activities and effectiveness.
12. The F/SD liaises with the Director OPCIO for Level 2 and 3 events, with regards to follow-up and lessons learned; and reviews plans and procedures.

5.2 Responsibilities & Authorities

Roles are assigned by the F/SD Manager for F/SD operations; and by the Director OPCIO / Vice Chancellor for the University Crisis Management Team.

TABLE 2: GENERIC RESILIENCE RESPONSE RESPONSIBILITES & AUTHORITIES

Position	Responsibility	Authority
Responsible Person – Faculty/ Service Division Manager or Delegate	All site operations Decides to activate the relevant F/SD Resilience Response Plan Sets the event level Notifies F/SD Manager For Level 2 and 3 events, notifies the Director OPCIO Event reporting & follow-up	Activates the relevant F/SD Resilience Response Plan Appoints the Incident Co-ordinator Authorises resources and contractor assistance as recommended by the Incident Co-ordinator
Incident Co-ordinator (at smaller sites, the Incident Co-ordinator may also be the Faculty / Service Division Manager or Site Manager)	Manages response team and response operations Safety & security of Response Team Maintains F/SD incident log Notifies neighbours Liaises / co-operates with Emergency Services; and hands over incident control to them if directed to Debrief and event review	Evaluates event level Decides when event is over ("stand down") To discontinue response operations if safety or security is compromised Requests additional resources from Director OPCIO is required
Site Response Team	Respond safely as per the response procedures	To discontinue response operations if safety or security is compromised
University Crisis Management Team ♦ Director OPCIO ♦ SMT Key Leaders ♦ SMT Advisors ♦ Faculty / Service Division Manager (refer University Crisis Management Plan)	Support the F/SD Incident Co-ordinator and provide resources required to respond to and effectively recover from the event Make / co-ordinate mandatory notifications and liaison as appropriate Handle legal and public affairs matters Event review, Lessons Learned and policy review if required	Make policy decisions Set priorities Advise Council Advise Ministers / Government as appropriate Media statements Customer liaison Financial support for response / recovery operations

Plans should contain up-to-date contact lists of key response personnel. Those plans that are publically available should withhold these details to ensure the privacy of the people concerned.

5.3 Designating Emergency Operations Management Locations

All resilience response management operations are managed from a F/SD Management Emergency Operations Centre (EOC) at a pre-planned designated location. In the event the designated EOC location has been evacuated or is unavailable, then operations are managed from designed alternative locations. Planning for a mobile EOC capability is also a good idea. E.g. a vehicle with radio, communications equipment including material and equipment pre-staged in plastic containers.

Resources are generally pre-staged at the EOC, with up-to-date copies of plans and procedures, ICT support and telecommunications / radio communications equipment, and basic Civil Defence supplies. It is advisable to have low technology alternatives such as hard copies of plans, whiteboards and so on in the event that infrastructure services are compromised (e.g., power, heating, lighting, IT services).

Many operational responses at the University will be coordinated or hosted by Property Services at their purpose built control room and facilities at 24 Symonds Street.

6. TRAINING & AWARENESS

It is important that all those participating in resilience response activities are adequately trained and competent to carry out the necessary tasks. Faculty / Service Divisions need to provide training, within the framework of their professional development / human resources programmes.

Three tiers of resilience response training are required;

- **Tier 1** – what everyone needs to know, i.e., induction level
- **Tier 2** – what people working in a particular environment or specialized operation need to know, about initial response actions to take to ensure their personal safety and that of others
- **Tier 3** - what responders and those with specific designated roles as set out in the resilience response plans need to know.

Training records need to be maintained, setting out which staff have undergone which training and when. Refresher training is required for those carrying out specialized response roles.

The Risk Office can provide guidance on training resources, methods, providers and programmes, as appropriate.

7. TESTING & EXERCISES

Regular testing & exercising of response arrangements and equipment is essential. Examples include:

- Notification exercises
- Equipment deployment exercises of scenarios
- Testing of alarms and specialised equipment
- Table top exercises.

The Risk Office can provide guidance and advice on testing & exercising. F/SD should aim to exercise all elements of their response arrangements within a 3 year cycle. There should be an independently conducted and evaluated exercise every 3 years.

Formal arrangements for the maintenance and testing of critical response equipment are also required, for example personal protective clothing, spill control equipment, radio communications equipment and so on. Note that some equipment has mandated requirements, for example fire detection and control, and this is covered by Property Services and Health & Safety.

8. FOLLOW-UP, REPORTING & PERFORMANCE

Debriefing after an event is an important part of the resilience response process. These should focus on what went right, what went wrong, and what would be changed next time.

Event performance reporting is essential to enable assessment of the effectiveness of responses and learnings for continuous improvement, not only for the F/SD but for the wider resilience management community at the University. Such assessments can be carried out internally, in conjunction with the Risk Office or externally as appropriate.

Incident follow-up, identification of corrective actions, and closure (i.e., assurance that these actions are completed) is essential. The Risk Office has a coordination role with regard to the follow-up of major events. In the event there are enduring issues, or those with broad implications, they may initiate a Risk Case, an assessment or investigation, a project, a programme of work, or (for enduring issues) a Task Force, to manage the risk around the issues identified. This process is described in the University of Auckland Risk Framework (refer Figure 1).

9. MANAGEMENT REVIEW

Resilience response plans need to be regularly reviewed, as part of the annual business planning and reporting cycle.

Particular events and the identified corrective actions may require an immediate change to policies, plans and procedures.

Resilience risk management plans, processes and procedures are subject to the internal audit programme as required. This is co-ordinated by the Risk Office.

The Risk Office can advise F/SD's on all aspects of managing resilience risk, and work alongside F/SD specialists as required.