WELLCOME GENOME CAMPUS

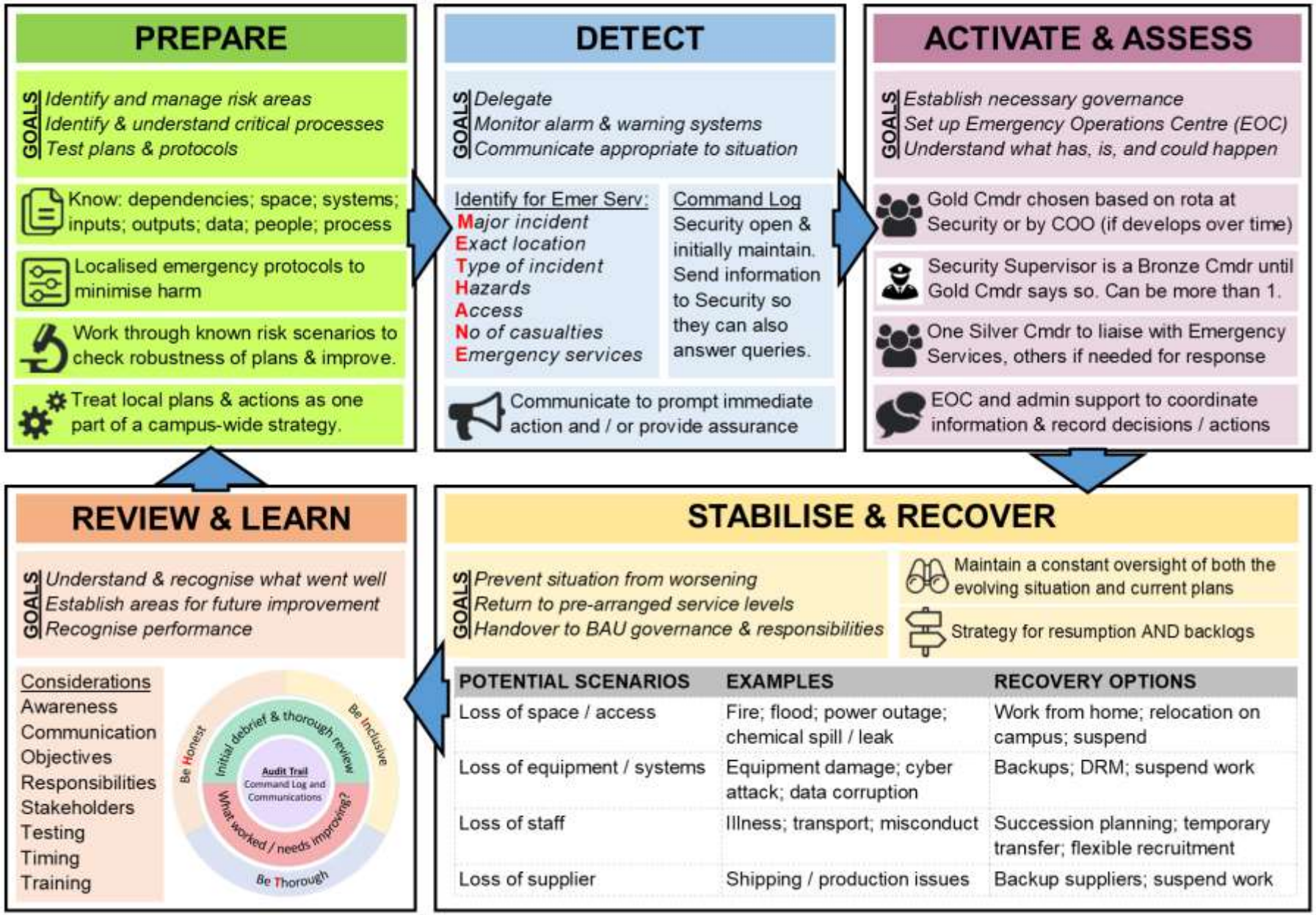
Wellcome Genome Campus &

Wellcome Sanger Institute

Business Continuity Plan

Version 9.1 (Mar 2022)

Plan on a Page



Contents

01. Business Continuity Policy

Purpose

The GRL Business Continuity Management System (BCMS):

- works with the Risk Management Framework to identify proactive action to improve GRL's resilience in the event of a major disruption;
- acts as a framework to coordinate teams across campus (including partners) in responding to, and recovering from, major disruption by recovering services to pre-defined levels;
- provides a focussed, distinct decision-making process to ensure wider campus implications of a disruption are managed and resolved to support a return to BAU levels of activity;
- sets out management and review arrangements for live disruptions and test exercises to further improve resilience;
- details stakeholders' roles and responsibilities in the event of a major incident;
- sets out means by which all stakeholders are kept informed;

The BCMS is focussed around a Business Continuity Plan (BCP). The BCP is NOT a rigid structure, but a scalable set of options that can be flexed to suit the wide range of scenarios to which it could be applied. GRL's recovery priorities will encompass the safeguarding and/or restoration of one or more of the following, depending on the incident:

Safeguarding:

- staff and visitors to campus;
- biological resources;
- financial investment in scientific equipment;
- critical data;

Restoration of:

- scientific and sequencing activities;
- internal and external IT resources, data and informatics storage and systems;
- domestic and support facilities for staff;
- premises which are safe and secure to work in;

Major disruptions arise in different ways, are identified through different routes, and can be limited in their impact or affect the whole campus. They include:

Sudden Physical Impact Incidents – little or no warning, often with high impact. For example: flood or fire affecting access to, and use of, campus buildings; industrial accident (e.g. serious chemical spillage); fatal accident.

Slowly Developing Incidents – can start in one department, then spread over a prolonged period, causing serious disruption to multiple stakeholders (e.g. academic misconduct). Alternatively starting elsewhere and spreading to the campus over time (e.g. pandemic).

ICT Incident – can happen with little or no warning, or can build in severity over time depending on the nature of the incident or any malicious agent involved. Includes malware, ransomware or other malignant agent, or the loss of storage space or high capacity computing capability through equipment failure.

Scope

The activities within this document only apply to the management and recovery of GRL assets, including those used by other entities but for which GRL is responsible.

The purpose of the BCP is to manage a coordinated response across multiple teams. Individual departments are no longer required to maintain separate business continuity plans replicating this one. However, this plan does not replace any emergency protocols departments may currently have in place to detect, track and respond to incidents. Owners of such protocols, and any underpinning information, are required to review them to ensure that appropriate escalation to the campus BCP is incorporated, and to notify the GRL Risk Manager where protocols need referencing in the BCP.

Definition of Major Incident

A major incident is an incident that meets two or more of the following criteria:

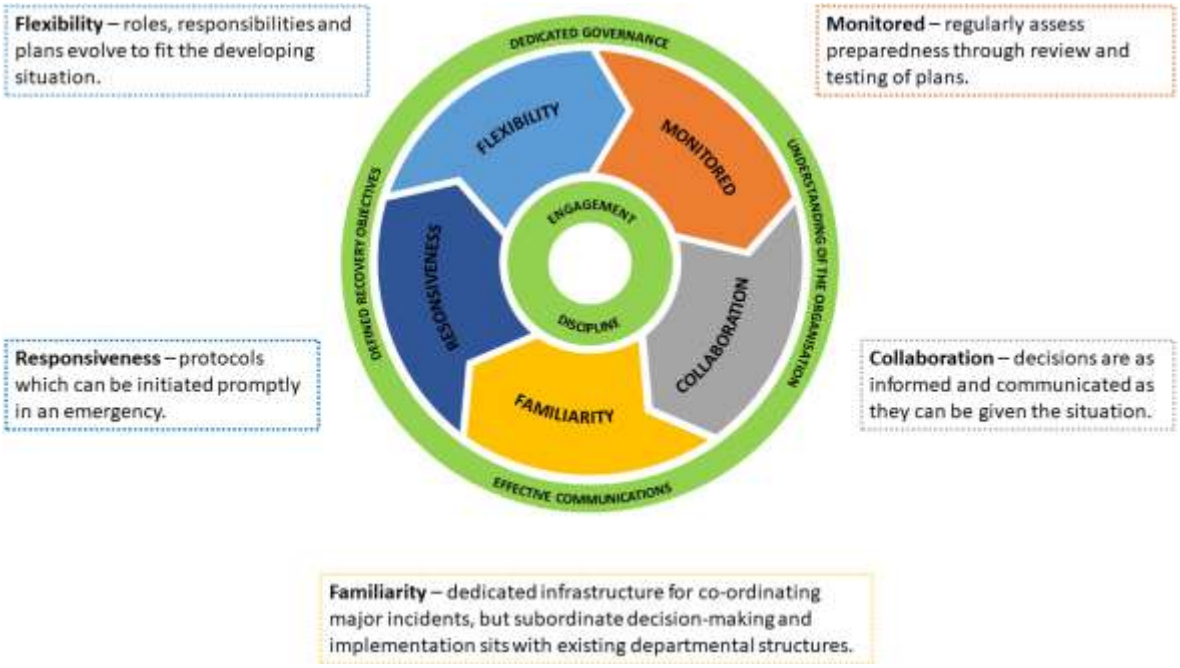
Personal Safety: There is a clear and current threat to human life or serious injury, especially where the repercussions could extend beyond the initial impact to reputational damage and/or service disruption.

Service Disruption: Interrupts or degrades business-critical services or underpinning infrastructure in a manner which either prevents, or has the potential to prevent, resumption to acceptable levels within 48 hours. This could result from a disruption to the availability of space (especially laboratories), people, supplies, technology and/or capital. Examples include: prolonged power grid failure; failure of high compute facility; significant fire or flood; widespread illness or supply issues.

Co-ordinated Response: Requires a prolonged and/or co-ordinated response that involves more than one department, and existing governance is not well suited to respond. It is important to note that many incidents can be managed without needing to initiate the BCP if they can be managed through normal governance.

Business Continuity Principles

Five principles underpin the management of major disruptions affecting campus activities:



Management Commitment

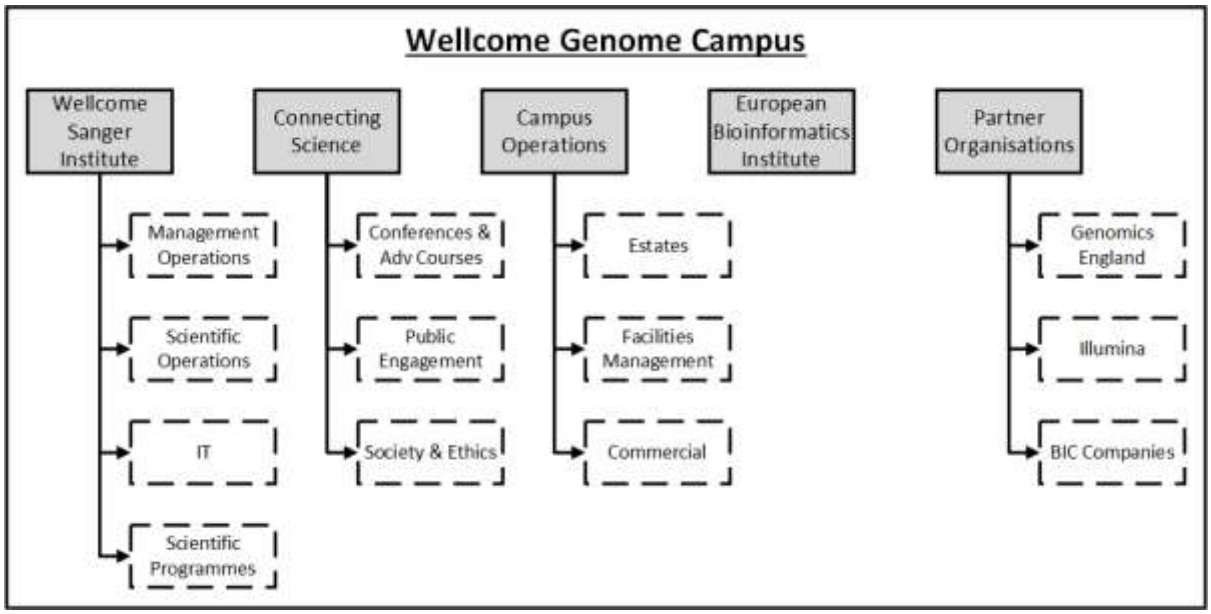
Each manager within the organisation has responsibility to ensure reasonable steps are taken to maintain the resilience of their departmental business processes by ensuring that:

- risks are identified and mitigated as far as is reasonably possible to minimise disruption;
- where necessary, emergency protocols are put in place to ensure action is taken to stabilise and recover from major disruptions, and that those protocols are referenced in the campus BCP;
- plans are in place to enable contact with staff who may be critical to support recovery in the immediate aftermath of a disruption;
- business impact assessments have been undertaken of priority activities to understand required timescales and prioritise for recovery, including Maximum Tolerable Period of Disruption (MTPD) and Recovery Point Objectives (RPO)

The Sanger Board of Management (BoM) has delegated Executive Responsibility for the campus Business Continuity Management System and Business Continuity Plan to the Chief Operating Officer and the Chief Financial Officer. Management responsibility is delegated to the GRL Risk Manager.

The roles and responsibilities are maintained within the BCP documents, with out-of-office contact details securely stored separately, to ensure that in the event of a major incident, escalation and communication can be rapidly effected.

02. Campus Overview



The Wellcome Genome Campus (WGC) is located at Hinxton, South Cambridgeshire and is the home of some of the world's leading genomics research programmes including:

The Sanger Institute which is a world-leading centre for genome-based biological research. This research is based upon high-throughput sequencing and bioinformatics technologies, and the use of natural and experimental-induced variation (genetics) as tools to understand the function of the genome.

Connecting Science, operating the Wellcome Genome Campus Conference Centre, Advanced Courses and Conferences and Public Engagement

The European Bioinformatics Institute, part of the European Molecular Biology Laboratory which is a major Informatics faculty carrying out basic research in computational biology providing Genomics data to partner researchers and industries throughout the world

Biodata Innovation Centre. A centre for Biodata startups and spinouts linked to genomic science. BIC contacts include Illumina and Genomics England Limited (GEL).

Each of these organisations plays a critical role in advancing the frontiers of human knowledge in Genomics, and this Business Continuity Plan is set in place in order to ensure that the campus that supports them is run at the highest level of reliability and availability, and that all assets, physical and intellectual property is protected from loss or degradation.

The Sanger Institute's scientific research programmes include Human Genetics, Cancer, Ageing and Somatic Mutation, Parasites & Microbes, Tree of Life and Cellular Genetics. The Scientific Operations team develop and provide sequencing, data, scientific resources, and biological resources that support the needs of these scientific research programmes.

Management Operations provide many of the Campus-Level activities that support all programmes, including IT, informatics and the Corporate Data Centre, Facilities Management (including Customer Services and Capital Projects), Health and Safety, HR and Finance.

03. Potential Hazards

The following potential hazards need to be addressed through departmental or organisation risk assessment and management, to ensure the best possible preparedness for a disruption.

Failure of utilities	Campus sits within a rural setting with many of the electrical services supplied via overhead lines vulnerable to weather damage. Buried services are vulnerable to damage from excavation activities arising from building and development in the area. Growth in demand for utilities means there is little capacity in the local networks. BCP responses to these issues lie within the resilience of backup and storage facilities on site.
Flood damage	Campus is located within the flood plain of the River Cam. Many areas of the site are regularly flooded. Site development reflects this by: • Construction of buildings with basement areas used for ancillary or car parking, but these often house excess assets and systems • Flood protocols protect exposed areas e.g. West Pavilion
Access to work	Many staff commute to the site, and so their attendance is subject to weather effects. Most departments provide facilities for home working. Residential facilities exist on site that can be exploited if staff need to stay on site.
Fire damage	There is a high concentration of equipment assets, and the presence of flammable chemicals and materials. This is managed with two approaches: • Baseline: good fire compartmentalisation, this is monitored and maintained by regular inspection and remedial protection. There is also a networked fire detection system providing addressable point identification both locally (in the building) and remotely (to security control) to promote rapid response. • Special facilities that have added levels of detection such as VESDA systems and enhanced suppression systems such as sprinkler or inert gas as in the Data Centre. Each department is responsible for good housekeeping to minimise stocks of solvents or gasses in the working area to reduce fire loads.
Environmental risk	Emissions to the environment through air, water or land form part of a separate management system accredited to ISO 14001 for environmental standards. There are response plans to deal with pollution incidents.
Security risk	Campus is a semi-open site with a large perimeter, public access and water courses running through the site. The security risk is managed via: • Extensive perimeter monitoring • Camera systems on main access ways • Card access control on the building entrances • Manned patrolling of the site out of hours • Visitor escort protocols • A 24/7 security control room
Critical building environments	Many building environments, for research, data processing and special assets are vulnerable to interruption and damage through the failure of

	heating, cooling and air quality systems. The WGC is equipped with a sophisticated control and monitoring system which reports technical and performance issues to the site maintenance team and instigates callout (out of hours) via security if needed.
Loss of Laboratory and Office Space	Potential alternative laboratory space (on or off-site) for critical activities needs to be identified with sufficient resources and space. This should be quantified and communicated before a disruption so recovery time is not wasted. In the event of loss of office space there are potentially many rooms that individuals can work from, the restaurant and coffee shops are viable short-term alternatives. Wi-Fi is available across the site and if required many employees can work from home.
Loss of Equipment	Many campus automation platforms are highly technical, expensive and specific to each supplier, and not all platforms can be supplied by alternative suppliers. Laboratory managers need to ensure that critical spares for essential automation platforms are available if a machine fails, and that alternative suppliers are identified and recorded for use where possible. Lab managers should ensure that service contracts from critical automation platforms are proactively reviewed to ensure that they provide the necessary cover, including the ability to receive loan equipment at short notice if that is required.
Loss of People	Cross training features heavily in many of the resilience plans, and needs to be proactive so that resilience is maintained during a period of decreased personnel levels. Teams should set targets for their cross-training and minimum capability levels, and ensure that these levels are periodically reviewed to ensure resilience.
Loss of Critical Supplies	Teams, especially laboratory based teams or those using specialist supplies or services, need to work with Procurement and Supply Chain Management to identify alternative suppliers in case of disruption. They also need to understand local stock levels of each, and how it affects recovery over time (where appropriate via the Sanger Logistical Services) so that they are able to plan effective recovery.

04. Stages of Incident Management & Recovery

Preparedness

Resilience and preparedness aid quick and efficient response and recovery. Elements include:

- Identify and manage areas of risk;
- Identify and understand critical processes and the impact of disruption;
- Test plans and protocols by thinking through specific scenarios;
- Talk to the GRL Risk Manager for support in resilience planning and testing.

A Business Impact Analysis (see Appendix A2) aims to capture critical elements that could support immediate decision-making at the highest level in the event of a disruption.

Incident Detection & Stabilisation

Early warning that a disruption has happened is vital. GRL identifies incidents through:

- Building Management System (BMS) detecting physical incidents;
- IT alerts warning of cyber and other system-related disruptions;
- All other departments monitoring issues in their areas (e.g. staff disputes) that could escalate into larger scale disruptions.

GRL's BCP supports a swift response to any major disruption, with a framework for:

- Delegation of responsibility from BAU governance to a dedicated command structure;
- Monitoring alarm & warning systems to keep track of the major disruption;
- Communicating quickly & widely to enable stakeholders to make informed decisions.

Recovery Activation

The decision by the Gold Commander to activate the BCP triggers the creation of an infrastructure (appropriate to the scale of incident), including the establishment of:

- Necessary governance to make and support decisions;
- An Emergency Operations Centre to collate and communicate information;
- A clear understanding of what happened, is happening and could happen.

Recovery Planning & Implementation

The infrastructure in place develops strategic, tactical and operational response plans that mitigate the impact of the incident. This impact can be physical, emotional and/or reputational:

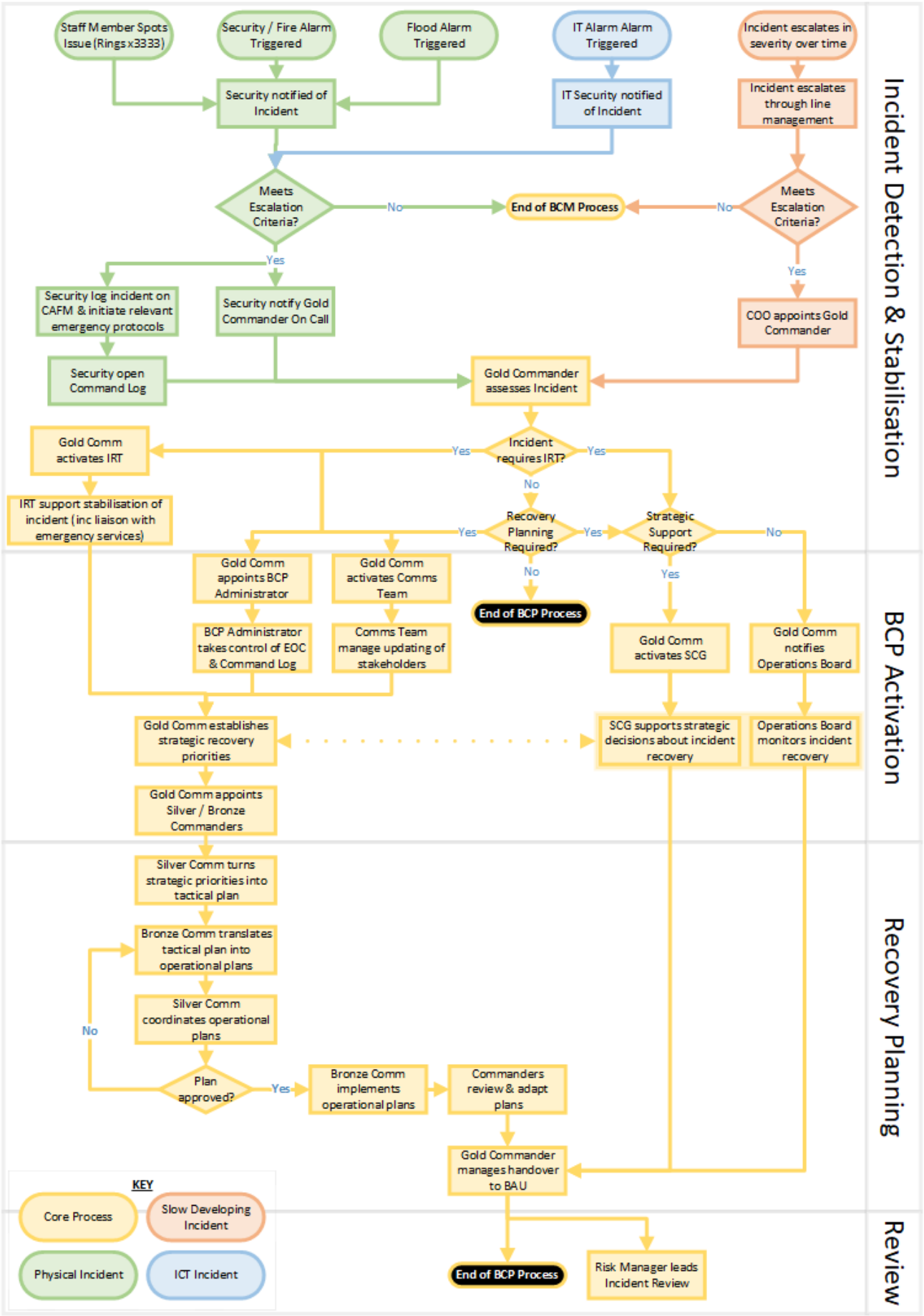
- Stabilise the situation by preventing it from worsening;
- Return to pre-defined service levels within required timescales;
- Hand responsibility back to BAU governance & responsibilities

Review & Learn

An initial debrief for immediate thoughts should be followed by a considered analysis to:

- Understand & recognise what went well, and why;
- Establish areas for future improvement, and who will monitor actions;
- Recognise performance

Incident Response & Recovery Management Summary Process Flow



Notifying Gold Commander

Security holds a 24 hour rota of On Call directors (with contact details) in the event of a major incident. If the On Call director cannot be reached, directors should be contacted in the following order until a director agrees to assume the role of Gold Commander for the incident:

1. Chief Operating Officer (Martin Dougherty x4937)
2. Associate Chief Operating Officer (Sian Nash)
3. Human Resources Director (Charlie Weatherhogg x5319)
4. Director of Scientific Operations (Cordelia Langford x4808)
5. Chief Information Officer (James McCafferty x9922)
6. Chief Finance Officer (Maggie Payne x4786)
7. General Counsel (Nadia Meliti x6846)
8. Director of Communications (Steve Palmer x6928)

Until such time as a Gold Commander has accepted the role, the on site Security Supervisor has limited authority to restrict access to the campus, and communicate closure (see below) as a precautionary measure (for example, if emergency services are fighting a fire), based on their own assessment of the situation and advice from the emergency services. As long as such a decision can be justified it should be supported, even if subsequently countermanded by the Gold Commander.

If, after accepting the role, the Gold Commander is at any point unavailable (e.g. while on route to campus) the limited authority above reverts to, in the following order as available:

- Estates & Facilities Representative
- Health & Safety Representative
- On site Security Supervisor

Once a Gold Commander is in place the on site Security Supervisor becomes a member of any Incident Response Team, and then a Bronze Commander, by default until such time as the Gold Commander relieves them of this role.

Supporting the Gold Commander

The immediate support required for the Gold Commander will vary by incident. In some instances the support of the on-site Security Team may be sufficient. At other times, for example where personal safety or physical property is, or has been, compromised, it may be necessary to initiate a short term Major Incident Response Team, comprising staff from Estates & Facilities Management, Health and Safety, Security and/or, if the ICT infrastructure is compromised, Information and Digital Solutions. This would be subsumed by Silver Command as stabilisation become recovery. The use of such a team will be at the discretion of the Gold Commander and dependant on what is needed to stabilise the immediate incident.

Security retain a list of senior or critical campus staff who can be contacted in the event of an emergency, listed as “Gold Commanders”, “Incident Response” and “Subject Experts”. However, with the exception of the Gold Commanders, such individuals are not “On Call” and cannot be assumed to be available immediately.

Initiating Activation and Assessment

The activation checklist (Appendix A1) provides a starting point for immediate considerations. There are also templates for the Command Log (Appendix A4) and for a completion form (Appendix A5) that follows the M/ETHANE methodology for collecting information for the emergency services. Other information of value may be found in Appendix A6.

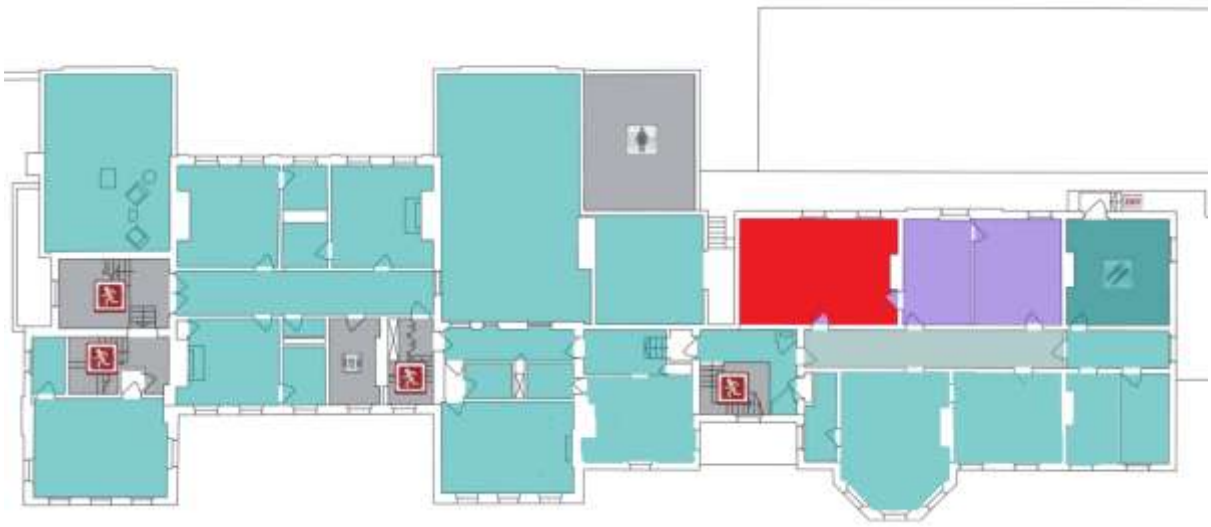
05. Emergency Operations Centre

An Emergency Operations Centre (EOC) is a physical location from where incident management can be coordinated. It needs to support:

- **Information Gathering & Sharing:** to establish current situation and potential impacts.
- **Ease of Engagement:** somewhere where Gold and Silver Commander(s) can be found.
- **Incident Briefings:** for the incident response team(s) so everyone is on the same page.
- **Visibility of Response Plans:** to enable review, challenge and agreement.

The following locations are default locations for EOCs depending on the location of the incident:

- C302 & C303 (Sulston Building, floating room above DiNA)
- K310 (Hinxton Hall 3rd floor, in Red below)



The EOC should be equipped with:

- sufficient furniture to work in comfort for a prolonged period;
- communications accessibility;
  - access to networking capability and/or wifi (as well as printers & copiers if required);
  - sufficient landlines for incoming AND outgoing calls;
  - good mobile signal;
  - access to videoconferencing kit;
  - access to 2 way radios (default = Channel 3) (available at Security Reception);
- information gathering and display tools
  - whiteboard, flipchart, post-it notes or other vertical planning tools (inc pens / pencils);
  - projection units to display shared information
  - access to broadcast radio and television (preferably with recording capability);
- hard copies of:
  - emergency response protocols; business continuity and crisis communications plans;
  - contact/telephone lists;
  - diagrams of facilities and systems; (available at Security Reception)
- stationery, business and incident management forms, pens, pencils, markers and supplies
- drinking water for EOC staff

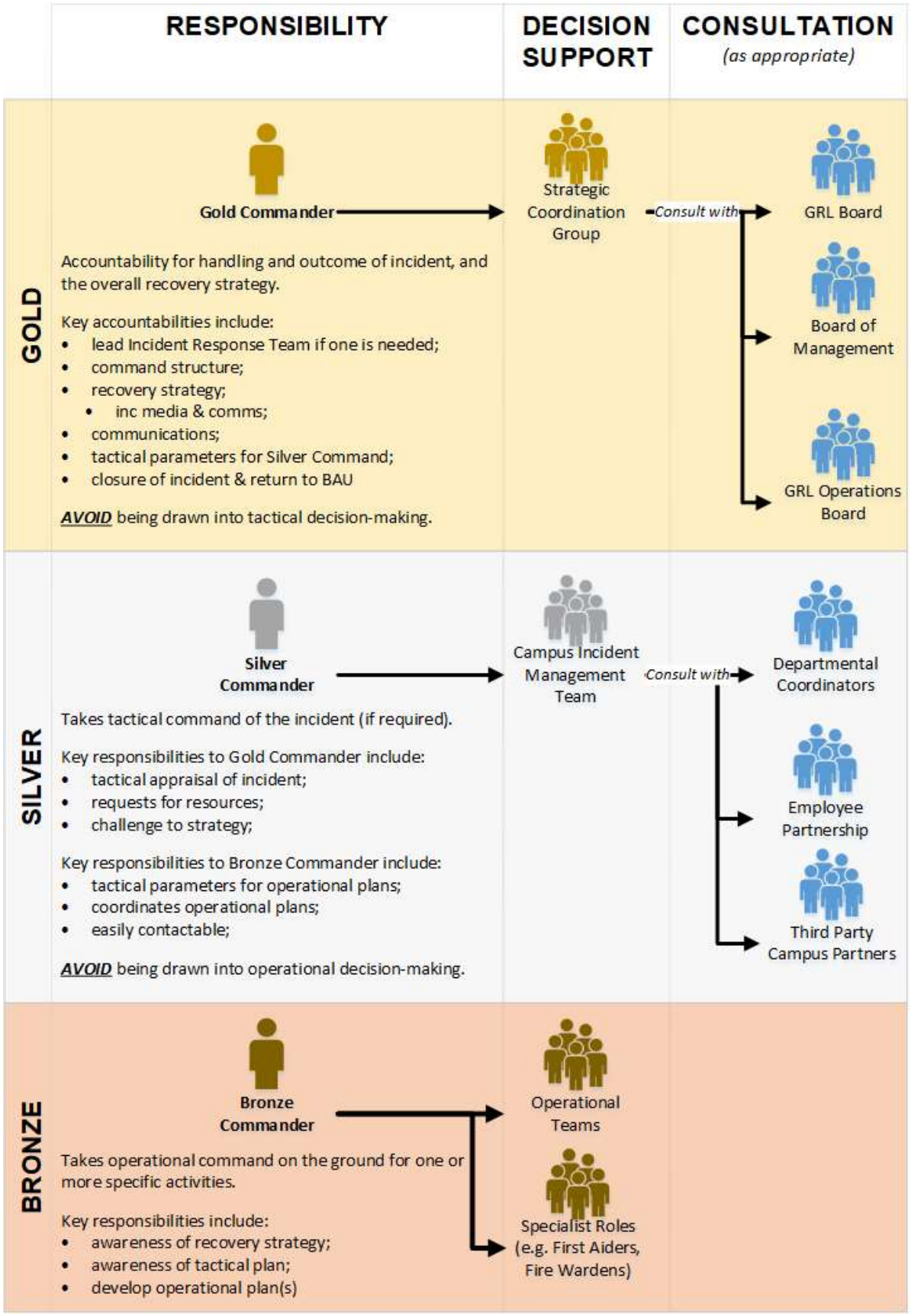
Many of these functions can be undertaken remotely but as yet there is no template for a wholly virtual EOC that would replace all of the functions above. This will be looked at for the future.

In the event that the internal telephones are compromised, there is a network of copper phone lines across Campus enabling outgoing or incoming calls. They are located in the following places:

Location	Building	Location	External Line
LA2-03	Conference Centre	Reception	01799 531592 / 01223 837260
M2-21		Ancillary Building	01223 830658
L2-06	Reception Building	Security Control Room	01799 531591
N2-14	Morgan Building	IT Service Desk	01223 837825
D3-28	Sulston Building	Comms Room 4	01223 835916
D2-68	Sulston Building	Central Comms	01223 832914
R1-05	RSF	Comms	01223 837458
T2-11	East Lodge	Directors Office	01223 833956

06. Business Continuity Management Governance Structure

Governance over a major incident (and subsequent recovery) functions at three levels:



Detailed Roles and Responsibilities

Any major incident should have:

- a designated Gold Commander taking overall responsibility for responding to the incident;
- a designated Silver Commander to liaise with emergency services if they have been called;
- at least one Silver Commander overseeing the tactical response to the incident (if needed);
- at least one Bronze Commander overseeing implementation of any operational responses.

The operational control of the incident remains in the hands of the Commanders although the appropriate support groups provide advice and challenge. Flex these responsibilities as the incident requires to ensure that the necessary action is taken.

Gold Commander

At any given point in time there will only ever be a single Gold Commander, with ultimate accountability for the handling and outcome of the incident. Principal responsibilities include:

- assume overall command of the incident until the incident is closed or they are replaced;
- set up a resilient command structure to stabilise the incident and manage recovery;
- set, review, update and communicate recovery strategy (inc. communication & media strategy);
- lead a small Incident Response Team if one is needed to immediately stabilise an incident;
- turn strategy into tactical parameters for Silver Commander;
    - *considerations should include health & safety of staff (both generally and those managing the incident); legal / compliance; partners; suppliers; local community*
- maintain objectivity and avoid being drawn into tactical decision making.
- ensure they are located to be easily contactable so as to manage the incident effectively;
- declare and communicate closure of incident, and disbanding of response team(s).

Responsibilities to the Silver Commander

- approves request for additional resources to support incident management & recovery;
- be readily available to Silver Commander, either by location or means of communication;
- ensures the resilience and effectiveness of the Silver Commander;
- approves the tactical plan, ensuring it delivers the strategic objectives.

Strategic Coordination Group (SCG)

Supports the Gold Commander, who ultimately makes the decisions. In the early stages of incident management, when time is short, members may act more as individual sounding boards. As the situation stabilises and more time is available a more collegiate decision-making model may be appropriate:

- chaired by Gold Commander (or delegated alternate depending on circumstances);
- membership is Ops SLT and Directors Office. Additions at discretion of Gold Commander;
- reviews the resources available and advises on any increase and/ or reduction;
- makes specialist skills available to the Silver Command as requested;
- advise on legal & regulatory issues;
- reviews, challenges and advises on the recovery strategy as it evolves;
- approving changes to policies for the purposes of recovery only;
- monitors effectiveness of the decision-making structure and approves BCP closure.

Silver Commander

The key function of a Silver Commander is as a dedicated resource to manage the operational delivery, leaving the Gold Commander free to focus on strategic factors and communications – especially externally facing communications. Key considerations in appointing a Silver Commander are the scope of the incident response or the timescale of the recovery.

Important responsibilities of the Silver Commander:

- assumes tactical command of the incident;
- appoints any further Bronze Commander(s) as appropriate to support operational delivery;
- set, review, update and communicate the tactical plan based on Gold Command strategy with the same considerations incorporated (e.g. legal, Health & Safety, community etc).
- if the incident is prolonged, oversee changeover of staff and commanders, including themselves;
- be located appropriately to exert their tactical command over the incident

There must always be a separate Silver Commander dedicated solely to liaising with the emergency services in incidents where they are called, and if the incident involves hazardous materials on campus that Silver Commander should be drawn from the Health & Safety Team.

Responsibilities to the Gold Commander

- makes requests to Gold Commander for additional resources;
- coordinating an ongoing situation assessment and response plan with Bronze Commander(s) & Service Managers to brief Gold Commander;
- challenges the Gold Commander's strategy to ensure that it can be delivered;

Responsibilities to the Bronze Commander(s)

- tasks and coordinates the Bronze Commander(s) plans in accordance with the tactical plan;
- ensures that any changes to the tactical plan are communicated upwards and downwards;
- ensures that Bronze Commander(s) work within the parameters set in the response plan or communicate any necessary deviation;
- maintains objectivity so as not to become drawn into bronze decision making.
- ensure they are located to be easily contactable so as to manage the incident effectively;

Campus Incident Management Team (CIMT)

The team supports the Silver Commander, advising on and challenging decisions:

- chaired by Silver Commander (or delegated alternate depending on circumstances);
- challenging and approving the tactical plan submitted by the Silver Commander;
- ensuring that tactical plan is linked, and not run in silos;
- recommends new policies or changes needed to support incident management and recovery;
- ensures tactical plans are delivered to schedule by Bronze Commander(s) / operational teams, or reasons provided and solutions found;
- resolving conflicts in operational priorities;

Incident Response Team

A short term operational group led by the Gold Commander, with members drawn from Health & Safety, Estates & Facilities Management, Security, the Engineering Contractor, and Information and Digital Solutions. The focus is immediate stabilisation of the incident. Replaced by Silver Command.

Bronze Commander

The Bronze Commander takes the operational decisions necessary to accomplish the Silver Commander's tactical plan. There can be more than one Bronze Commander as long as each has a clearly defined and logged remit. For example, an incident may require:

- a Bronze Commander (Evacuations) ensuring people are safely contained;
- a Bronze Commander (Operational Response) ensuring operational responses such as flood defences are implemented; and
- a Bronze Communications (Media) to liaise with the Media at an operational level.

Important responsibilities of the Bronze Commander:

- assume operational command of the incident or specified supporting activity
- have a clear understanding of the Gold Commander's strategy, the Silver Commander's tactical plan and their role within it
- be suitably located to maintain effective operational command of their area of responsibility
- review, update and communicate any changes that may affect the tactical plan

Bronze Commanders are responsible for the command of a group of resources, and carrying out functional or geographical responsibilities related to the tactical plan. The number of Bronze Commanders and their roles/specialisms is determined by the scale and nature of the incident.

Tasks for Bronze Commanders may be stated in existing emergency protocols, or may be delegated by the Silver Commander in accordance with an agreed response plan. Some Bronze Commander roles require specialist knowledge, skills and expertise and, therefore, should be allocated to individuals or post-holders who are appropriately trained and competent.

BCP Administrator

The BCP Administrator is an administrative role responsible for the following activities:

- ensures that the management and recovery is documented, including any changes;
- establishing and managing the Emergency Operations Centre and coordinating meetings;
- ensuring SCG and CIMT members are contacted;
- act as go between where necessary between Gold Commander and Silver Commander(s);
- produce management reporting as and when required;
- working with Communications Team on internal and external communications;
- maintaining the Command Log throughout the incident for review, as well as a clear audit trail

Communications Team

The Communications Team:

- recommend a communications strategy as part of the Gold Commander's recovery strategy;
- keep staff regularly and appropriately informed on incident management and recovery based on information provided by Gold and Silver Command;
- manage media relations as appropriate;
- add communications-related updates to the Command Log;

07. Command Handover Protocol

Responsibility for the closure of the incident, and the standing down of the various management roles and teams, sits with the Gold Commander. The Gold Commander will make this decision in consultation with the Silver Commander(s), the Strategic Co-ordination Group and other key stakeholders once the Gold Commander considers the incident to reached a point where business as usual governance can resume responsibility for the disrupted activities. Responsibility will then be handed back to the organisation on the formal agreement between the Gold Commander and the GRL Chief Operating Officer.

This will be recorded in the Command Log and the Log will be signed and closed. The Command Log, and any associated documentation on the incident, will then be retained for a period of 6 years.

08. Testing the Plan

This plan, either as a whole or individual aspects of it (including any emergency protocols or arrangements that support it), should be tested annually. Testing fulfils two important functions:

- *Fitness for Purpose:* to reflect changes in organisation, procedures, systems or people. Testing the plan highlights whether it will work when needed.
- *Familiarisation:* The more familiar key staff are with how they and others should respond to an incident, the more calmly and efficiently they will respond in a real situation.

Testing can be done at different scales and with different types of activity. All tests should be notified to, and shared with, the GRL Risk Manager, who will follow up on any actions and learning points. Types of test include:

- *Facilitated Discussion:* test a localised activity in detail with a small number of participants. For example, rising flood waters require a building to be evacuated. A facilitator leads participants through the necessary actions, including activation of the plan and initial responses (e.g. SOP implementation, building evacuation & recovery, use of the METHANE methodology to communicate information to the Emergency Services).
- *Plan Audit:* a paper exercise, which can be done solo or with a small team. It works better with individual elements of the plan rather than protracted exercises covering the whole plan. Examples include conducting the first coordination meeting, who is communicated to about what, why and when, disaster recovery of IT systems.
- *Speed Exercising:* an exercise in concise communication, where participants practice explaining, in two minutes or less, their role in a scenario. The goal is to practise the concise sharing of critical information, and develop tools and techniques for doing so.
- *Walkthrough:* a physical walkthrough of actions in situ to understand the locations of items and places of note. More suited to specific activities pertaining to an incident, these walkthroughs can identify elements that may seem logical on paper but become more problematic in practice, for example casualty management, alternative escape routes in the event of a blockage
- *Tabletop Exercise:* these can be single team, focussing on the activities of one part of the response (e.g. Communications, Stores), or multi-team, wide-ranging in nature, including the response from top level management. The aim is to see how teams respond to problem solving, engagement, decision-making, recording activities and working together as a team, as well as identifying any gaps in support that improvement to the plan could offer.

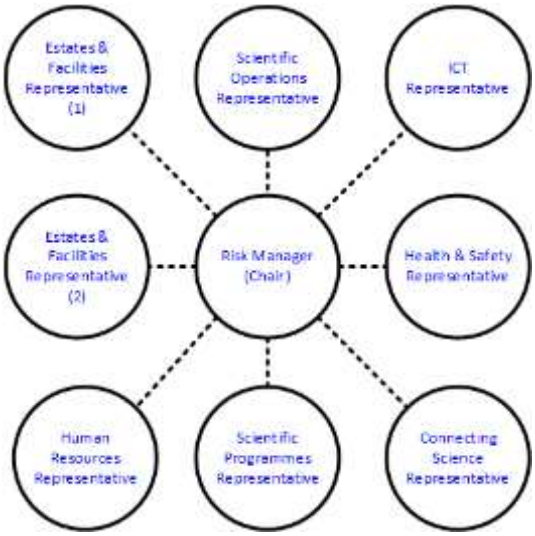
The Business Continuity Working Group (Section 9) will monitor and review tests, discuss improvements to the plan or related documents, to provide assurance to Operations Board that the plan will effectively support management during a major disruption.

09. Communication & Management of this Plan

Copies of the Business Continuity Plan will be accessible as follows:

Hard / Soft	Location
Soft copy	Fred (minus confidential contact information – stored separately), accessible to GRL staff, EBI and BIC companies
Soft copy	USB drives provided to: All members of Management Operations SLT Estates Director and all direct reports Security Management team Health & Safety Management team USB to USB-C adapters for use with USB drives.
Hard copy	Safe at Security Control (along with Flash Drive to USB-C adapters)
Hard copy	Securely in COO's office (filing cabinet, outer office)
Hard copy	Securely in Estates Director's Office

The plan will be reviewed every six months by a Business Continuity Working Group, comprising:



The purpose of this working group will be to:

- Review the BCP and ensure that it is still fit for purpose;
    - Identify any corrections or amendments that have been identified;
- Review what testing has taken place in the previous six months, and lessons learned;
- Review what testing is planned for the next six months and recommend and changes;
- Provide assurance to GRL Operations Board that the plan will support the response to a disruption.

WELLCOME GENOME CAMPUS

Appendices: Tools

Appendix A1: Major Incident Management / BCP Activation Checklist

The following is a checklist of critical actions to be considered in the management of an incident, even before the BCP is initiated. The letter indicates ideal responsibility between Bronze, Silver and Gold command, Administrator and the Communications Team, but ultimately if a different role is better placed to fulfil the task, the most important thing is that the Gold Commander has visibility that it is done.

For the purposes of the BCP the Security Supervisor should consider themselves responsible for the site until such time as a Gold Commander is appointed, and thereafter a Bronze Commander until such time as the Gold or Silver Commander relieves them.

ACTION	INITIALS	TIME
DETECTION & SCENE / SITE MANAGEMENT (Immediate)		
Notify emergency services if appropriate *(B)*		
The emergency services collect and exchange information using a METHANE model so it is helpful to use this when gathering information which can then be passed on to them ***(See Appendix D)***: **M**ajor Incident – this is for the emergency services to declare. **E**xact Location – what is the exact location of the incident. Local emergency services use or accept addresses using http://www.what3words.com/, a website that divides the world into 3m x 3m squares, each denoted by combinations of three words. For example, the front gate is "serenade.horn.streamers". Either give that location or, if time allows, identify as closely as possible the location on campus where the incident happened. **T**ype of Incident – fire, flood etc **H**azards – hazards or potential hazards at the incident site – toxic chemicals, flammable materials, explosives etc. **A**ccess – best routes for access to and from the incident **N**o. of Casualties – how many and what condition are they in **E**mergency Services – number of emergency responders (vehicles & people) are required / already on site		
Evacuate scene / site as far as is practicable *(B)*		
consider implications for accommodation / transportation in due course		
Secure scene / site to prevent unnecessary access or situation worsening *(B)*		
Support casualties with first aid / other support *(B)*		
FIRST CONTACT (Within 10 mins)		
Contact Gold Commander *(see next page)* *(B)*		
Ask Gold Commander if Incident Response Team should be contacted – Yes / No *(B*		
Contact Incident Response Team (if advised by Gold Commander) *(B*		
Implement any necessary emergency response protocols (see Appendix 5) *(B)*		
Identify witnesses to refer to investigating authorities *(B)*		
ACTIVATION (Within 15 mins if required)		
Record incident on CAFM if a physical incident *(B)*		
Open Command Log *(see Appendix A3)* *(B)*		
Confirm and communicate activation of the Business Continuity Plan *(G)*		
existing Silver / Bronze Commanders on site, Comms Team		
Make contact with any Silver and Bronze Commanders on scene / site already *(G)*		

ACTION	INITIALS	TIME
Make initial assessment of incident, likely disruptions and current response status		
including what, if any, action has already been taken (G)		
Check for any potential secondary incidents that could result from the first *(G)*		
Appoint specific Silver Commander to liaise with emergency services *(G)*		
Appoint Silver and Bronze Commander(s) as required *(G)*		
Appoint Administrator(s) to maintain records & support command *(A)*		
Take responsibility for Command Log *(A)*		
Set up as Emergency Operations Centre *(see page 9)* *(A)*		
ONGOING		
Maintain rolling assessment of situation & adapt strategy and plans accordingly *(G)*		
Notify the Administrator of important decisions / actions	***ALL***	
Document all decisions & actions in the Command Log *(A)*		
COMMUNICATION		
Send initial notification on incident to all staff and stakeholders *(C)*		
Remind staff not to share certain material on social media		
Establish a communications plan to keep all stakeholders suitably informed *(C)*		
Provide information to, and coordinate with, Communications Team on messages *(G)*		
Set any automated responses to incoming calls / emails *(B)*		
Assign an appropriate media spokesperson for 'on-camera' interviews *(C)*		
Set up media / social media monitoring *(C)*		
INITIAL ASSESSMENT & ENGAGEMENT		
Establish means of updating Strategic Coordination Group and CIMT members *(G)*		
Convene first meeting of Strategic Coordination Group as required *(G)*		
Convene first meeting of Campus Incident Management Team as required *(S)*		
Backfill to undertake business as usual during incident & response management *(G)*		
Develop & communicate recovery priorities, strategy & objectives *(G)*		

Appendix A2: M/ETHANE Completion Form (for use by Security)

Time	Date
Name of Caller	
Number(s) Called	

M	Major incident	Has a Major Incident been declared? **YES/NO** *(If no, then complete ETHANE message)*	*This relates to what the emergency services deem a Major Incident, so will be determined by them.*

E	Exact Location	What is the exact location or geographical area of incident	
T	Type of Incident	What kind of incident is it? Fire? Flood? Physical or Cyber Breach?	
H	Hazards	What hazards or potential hazards can be identified? Are they active threats?	
A	Access	What are the best routes for access and egress?	
N	Number of casualties	How many casualties are there and what condition are they in? Where are they?	
E	Emergency Services	Which and how many emergency responder assets/personnel are required or are already on-scene?	

Restricted once complete

Appendix A3: Critical Information

The following information is of value in the assessment of current and potential risks in the event of a major incident:

A. Existing Emergency Protocols

- Fire Code of Practice (on Fred – owned by Campus Health & Safety)
- Standard Operating Procedure: Flooding (owned by Estates & Facilities Management)
- IT Major Incident Management Process (on Fred – owned by Information and Digital Solutions)
- Security Emergency Protocols (owned by Security)
  - EP04 – Security Escalation Plan – *escalation of a Security matter within Security / FM*
  - EP06 – Fire Alarms – *action in response to fire alarm*
  - EP07 – First Aid – *requesting a First Aider or attending a First Aid incident*
  - EP09 – Emergency Telephone Message – *how & when to change message; template*
  - EP10 – Power Blips and Power Failure – *checks to make; who to call; what to record*
  - EP11 – Chemical Spill or Suspicious Liquid – *who to call; secure area; spill kit deployment*
  - EP12 – Water Leaks and Flooding – *response to finding a leak; flooding alarm checks*
  - EP13 – Travellers – *who to contact; actions in response to traveller presence*
  - EP14 – Emergency IT Escalation Checks and Call Out Procedure – *who to contact*
  - EP15 – Telephone Threat – *checklist of details to take if one is made*
  - EP16 - Combination Codes & Passwords – *to various locations on campus*
  - EP18 – Emergency or Remote Access – *granting access to restricted areas*
  - EP19 – High Voltage Systems Failure – *who to call; key access*
  - EP26 – Suspicious Items – *action in response to a call*

B. Campus Information

- Site plans indicating the following are in a Red folder in the Security Control Room:
  - Fire hydrants and emergency equipment
  - Isolating points for utility services
  - Hazard materials, chemicals etc.
  - Building configuration and layout
  - Action plans for closing down / isolating / protecting critical plant, machinery & other equipment
- Call out lists of essential personnel and contact details, including:
  - Gold Commander prioritisation & out of hours callout;
  - Specialist individuals who can act as Silver / Bronze Commander(s);
  - Communications Team contacts;
  - Insurance contacts;
  - Regulatory Authorities;
  - Emergency agency contacts (e.g. Environment Agency, Emergency Services, Wellcome)

Appendix A4: Business Impact Analysis Template

Resilience and preparedness are key to quick and efficient response and recovery. It is important that GRL understands and mitigates, as much as possible, its critical risks, but also that it is aware of the personnel, dependencies and functions without which essential work could not proceed and recovery would be more difficult. This information is captured in a Business Impact Analysis (BIA).

BIAs give a starting point for recovery planning, although commanders should augment the BIAs with any additional detail available at the time of disruption. The information they contain will be translated into a graphical map of dependencies.

There should be one BIA for each of the following:

- All 5 scientific programmes;
- Scientific Operations;
- Finance, Procurement, Grants & Stores;
- Human Resources;
- Legal, Governance & Policy;
- Communications Team;
- Director's Office;
- Information Technology;
- Estates & Facilities Management;
- Advanced Courses & Conferences;
- Public Engagement / Society & Ethics;
- Conference Centre

Each BIA identifies critical decision-makers and operational staff who could support the Gold and Silver Commanders, and key operational personnel (potential Bronze Commanders). It also sets out, for each critical departmental function:

- **Maximum Tolerable Period of Disruption (MTPD):** the time it would take for the loss of the particular function to become unacceptable. This may be driven by contractual or regulatory deadlines, or impact on other operations.
- **Recovery Time Objective (RTO):** the period of time following an incident within which a service / operation must be resumed or resources must be recovered
- **Recovery Point Objective (RPO):** the point to which information used by an activity must be restored to enable the activity to function on resumption
- **Dependencies** that must be available to support the particular function;
- **Core / Alternate Locations:** the building(s) which, if access was lost, would most disrupt the function, and any known alternative building(s) activity could definitely be moved to.

For some critical operations a distinct recovery protocol or plan may be required. Where such plans exist they should be brought to the attention of the Risk Manager for reference in the campus BCP.

To reduce administration and reduce the possibility of working from out of date information, BIAs will not include the detail of critical systems, equipment, space etc. That information is available in other sources, and can be drawn upon at the point of disruption.

Service	Source	Access
Equipment	Science Support Services Laboratory Equipment database	Bryony Warman; Cat Dockree; Emily Pigg
Consumables	SLS Spreadsheets	Thomas Thron; HoOps
Space	OfficeSpace Desk Booking System	Bryony Warman; Tina Smith; Emily Pigg
IT Systems	IDS Tiered System Recovery Plan	

BUSINESS IMPACT ANALYSIS TEMPLATE

DEPARTMENT					
CRITICAL STAFF *For all critical staff positions a primary and an alternate contact is required, to allow for holidays, illness etc. Add as many extra rows to each set of names as required.*					
Critical Staff (Strategic) *The person or persons who should be involved in Gold Command cross-campus strategic decision-making should departmental representation be required.*					
Primary Contact (Role)	**Name**	**Contact Details**	**Alternate Contact (Role)**	**Name**	**Contact Details**
Critical Staff (Tactical) *The person or persons who should be involved in Silver Command cross-campus tactical decision-making should departmental representation be required, or to manage critical departmental operations*					
Primary Contact (Role)	**Name**	**Contact Details**	**Alternate Contact (Role)**	**Name**	**Contact Details**
Critical Staff (Operational) *The person or persons who should be involved in Bronze Command management activities, or critical to departmental operations*					
Primary Contact (Role)	**Name**	**Contact Details**	**Alternate Contact (Role)**	**Name**	**Contact Details**

Assumptions Underpinning Responses	[Note any points such as time of year if there are variances at different times of year]

CRITICAL OPERATIONS					
Operation *(including minimum critical level of activity)*			**MTPD**	**RTO**	**RPO**
Dependent Functions (i.e. need to be operating so this function can)					
Outsourcing possible?	Yes / No	Core Locations:		Alternate Locations:	

BUSINESS IMPACT ANALYSIS TEMPLATE

DEPARTMENT	

OTHER OPERATIONS *List here other operations that are non-critical, but whose resumption does need to be factored into plans at some point*			
Operation	**MTPD**	**RTO**	**RPO**

OTHER INFORMATION		
Existing Emergency Protocols (Existing SOPs etc that will be invoked in the event of a disruption)		
Critical Information (What other plans, drawings, data etc. does the dept hold that could inform or support decision-making following a disruption?)		
Information	*Location*	*Who Has Access (Please include names)?*

Appendix A5: Command Log

The Command Log is a record of decisions and actions taken to respond to a major incident. It is important that this is maintained as it will perform a number of functions:

During the incident:

- Supporting an assessment of the current situation by providing details of action taken and decisions outstanding or taken.

After the incident:

- Providing a focus for any review and assessment of the incident and how it was managed;
- Providing a formal record in the event of any regulatory, legal or other investigations following the incident.

The Command Log should be opened as soon as a Major Incident is declared, by Security, Estates, IT or whoever declares the Major Incident. Once an Administrator has been appointed by the Gold Commander they should take ownership of the Command Log and retain that ownership until the Incident is declared closed by the Gold Commander, or in a long incident the Administrator is relieved.

There is a template for a Command Log on the following page.

Command Log Template

Incident:	*[Short title]*		**Location:**	*[insert building / area affected]*	
Description:	*Short description of incident you can use for communicating with stakeholders*				
Commander (Gold):	*[insert name]*		**Commander (Silver):**	*[insert name]*	
Incident Opened:	*[insert date / time]*		**Incident Closed:**	*[insert date / time]*	
Date	**Time**	**Information / Request**	**From Whom**	**Action / Decision Taken**	**By Whom**
After the incident is closed this log should be signed by the Gold Commander as a record of the incident.					
Signed:				**Date:**	

Appendices: Communications

Appendix B1: Initial Notification to All Staff

GRL does not have an active communications system that enables text messages to be sent widely. The Communications Team should be amongst the first wave of contacts, but in the event that a simple initial message needs to be sent, for example, to announce a closure of campus in the event of a fire, the following means of communication are available without recourse to the Communications Team:

- **Answerphone Message** – 0800 093 4818 *(Security Emergency Protocol EP 09)*
  plays an emergency message to anyone dialling in on the campus emergency number;
- **Hinx E-mail** – hinx@sanger.ac.uk (see below for draft template)
  Security can send a message without it being held for moderation;
- **BIC Contacts** – please use to enable BIC companies to manage their own communications
  - bic-hr-leads@wellcomegenomecampus.org
  - bic-bcp-leads@wellcomegenomecampus.org
- **EBI Contact** – Andrew Cornell (cornell@ebi.ac.uk) / Rachel Curran (curran@ebi.ac.uk)
  - Contact phone numbers held at Security Reception

Security will develop a contingency plan for handling people who arrive on campus during an emergency as it cannot be assumed anyone will check these sources before coming to site.

First Notification E-mail Template [Title: IMPORTANT – CAMPUS ACCESS RESTRICTED]

Dear xxxx,

An incident has occurred on campus that requires GRL to restrict access to the Wellcome Genome Campus, in accordance with the Wellcome Genome Campus Business Continuity Plan. This is due to [include brief details of disruption].

Please do not come to the campus under any conditions you receive an e-mail informing you that it is safe to do so. Further updates will be posted at: *[add location / method of updates]*.

Thank you for your patience at this time.

Kind Regards,

[Insert Name & Job Title of Gold Commander]

Appendix B2: Initial Agenda Items for First Meetings

Strategic Coordination Group

1. Apologies
2. Introductions
3. Confirming Roles and Responsibilities
4. Response Checklist Progress
5. Current Assessment of Disruption
6. Response / Recovery Strategy & Priorities
7. Any Other Business
8. Date and time of Next Meeting

Campus Incident Management Team

1. Apologies
2. Introductions
3. Confirming Roles and Responsibilities
4. Response Checklist Progress
5. Current Assessment of Disruption
6. Immediate Priorities and Tactical Parameters
7. Resource Requirements & Availability
8. Any Other Business
9. Date and time of Next Meeting

Appendices: Incident Review

Appendix C1: Post Incident Review

Post Incident Reviews aid future planning.

Once the incident has been completed, the Gold Commander will arrange a 'hot debrief' session with all the stakeholders to capture vital information about the incident and verify the sequence of events have been captured appropriately. Timescales for a 'full debrief' shall be determined by the appointed inquiry leader, but must be within 15-25 days of the initial incident.

Debriefing Guidelines

The debriefing must be led by a senior manager who was not involved in the management of the incident. The group should adhere to the following ground rules when debriefing:

- conduct the debriefing openly and honestly
- be consistent with professional responsibilities
- respect the rights of individuals
- not attribute blame, but focus on improvements
- should be in-line with WGC organisation and HR policies

Key Aspects of Debriefing

The key aspects of debriefing are as follows:

- gather initial information from those involved individually rather than in a group;
- include external parties such as suppliers, partners and external authorities;
- identify the nature and root cause of the incident;
- look for both strengths and weaknesses of how the incident was handled;
- assess the adequacy of management response;
- look for elements that could be integrated into BAU to improve efficiency or effectiveness;
- assess the effectiveness of the BCP and recovery plans, and recommend improvements

Output from debriefing

Output from debriefing is as follows:

- Complete BCM Incident Report (summarise the sequence of events, identify individuals involved, describe actions of staff involved, provide an accurate timeline);
- Likely cause of the incident;
- Approximate cost of response & recovery;
- Lessons identified from the incident, and dissemination of these;
- Agreed service improvement plan, with all actions given an assigned owner. The campus Risk Manager, as operational owner of the BCP, will ensure actions are followed up, escalating concerns to GRL Operations Board.

The output should be circulated amongst those involved in the response prior to being released. It is the responsibility of the review leader to track any actions through to closure, or to delegate that role to somebody who will report progress to the GRL Operations Board.

Document Change Control

Version #	Date of Issue	Author(s)	Brief Description
6.0	03/12/2014	Jim Hood	BCP recreated
7.0	27/01/2016	Jim Hood	BCP Issued
7.1	21/04/2016	Lucy Jobson	Amending phone numbers
7.2	28/11/2017	Jim Hood	Amending names and telephone numbers
7.3	01/06/2018	Jim Hood	Amending names and telephone numbers
8.0	01/03/2019	Martina Palmer	Amending names and phone numbers. Amended appendix B. Removed Appendices R,S,U & X
8.1	01/10/2019	Robert Bush	Amending names
9.0	25/10/2021	Robert Bush	Merging v8.3 of Business Continuity Plan with v1.1 of the Major Incident Management Process. Version provided to DHSC.
9.1		Robert Bush	Minor amends to BAI template