WHAT IS THE RIGHT CCMER FOR YOUR CLIENT?
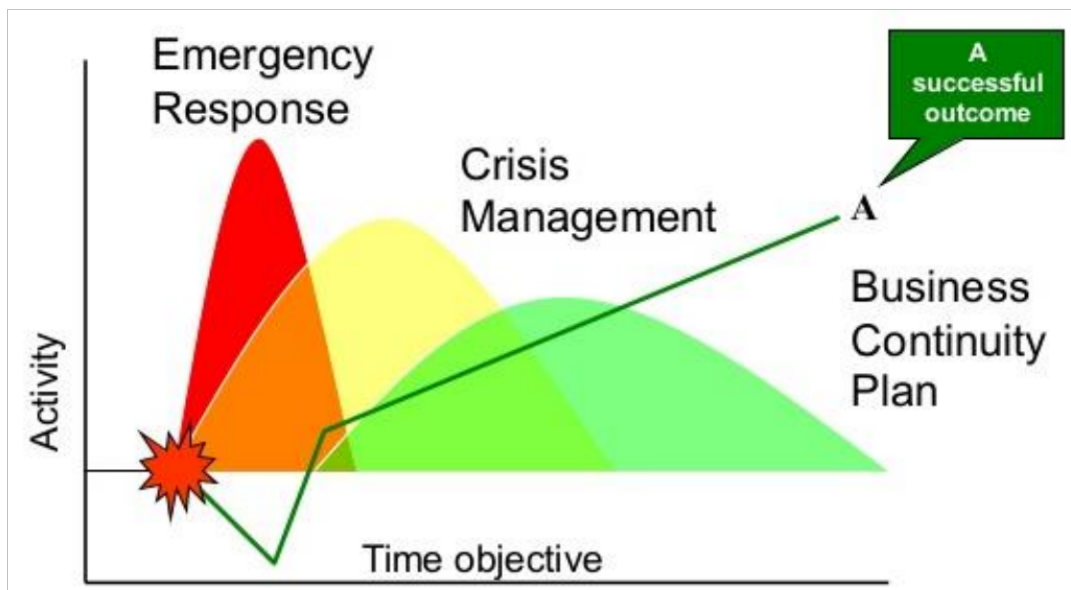
This document has been elaborated in response to the ad 928687 from M de Souza transferred to James Twomey james.twomey@orioneng.com
The objective of this document is demonstrating that I have a clear idea and concept about the JD which is very short

A. INTRODUCTION
3 periods in the time space in case of Emergency

A.1. Clarification
People often use the terms **"incident/emergency management"** and **"crisis management"** interchangeably. Yet, as understood by myself, Michel Louis Friedman, both are part of a comprehensive business continuity management solution.
Understanding the nuanced differences between the two concepts helps organizations to plan effectively, developing robust strategies and processes that can be deployed when faced with either a crisis or an incident/emergency.
What is the difference between incident/emergency management and crisis management? It comes down to a difference in scope.

A.2. What Crisis Management Is
- Crisis management is a strategic approach to issues, focused largely but not exclusively on communication. Crisis management is usually handled at the C-suite level and has an emphasis on brand and reputation management.
- A crisis is a situation that poses a threat to the organization's very existence. If the situation is not resolved, the results could be catastrophic to the enterprise. In today's dynamic media space, crises can arise fast and snowball even faster, driven by a 24/7 media cycle, the presence of social media, and access to information and opinion that may not be accurate or relevant.
- Managing a crisis means being proactive and fast, focusing on rapid resolution and recovery that is effective. It also means clear, effective communication that is sent to stakeholders, shareholders, regulators, the general public, and employees via multiple media and messengers.

- Planning for a crisis means preparing the organization for potential crises and developing the processes that will be used when or if a crisis is declared. Once in a crisis, it is time to put those processes and capabilities into play, providing for responses that can be delivered consistently and accurately. Consider that communication in a response needs to involve traditional print and broadcast media, text and voice, multiple social media channels, and your employees themselves, from customer relations to front-line salespeople and executives.
- Incident/emergency management involves a specific response to an event that is categorized, assessed, and addressed.

A.3. What Incident/emergency or emergency Management Is

Incident/emergency management is much more specific, with a particular event occurring that could lead to a loss of operations, services, or functionality. An incident/emergency, if not handled well, can lead to a crisis.

Incident/emergency management comprises the processes of identifying and categorizing incident/emergency s, investigating those incident/emergency s, and remedying any losses of services, access, or capability that result. Once an incident/emergency has been identified and reported, it involves deploying plans to respond appropriately to the incident/emergency and reporting on the outcomes of that response implementation.

Incident/emergency s often vary in scope and impact, meaning it is critical that organizations have solutions in place that will determine the type or category of the incident/emergency and the scope of that incident/emergency 's impact on systems, operations, or users. This assessment is essential for determining how incident/emergency s are addressed.

1. Definition of a good Crisis, Continuity and Emergency Response Advisor

*This job as Crisis, Continuity & Emergency Response Advisor is based on a personality able to understand priorities and understand the relativity of the time **WITH** the action to be put in place , able to work with priorities with tiers or stages realtives to the situation (asset, country, project , escalation……..*

A Good incident / emergency advisor (I have been the formal emergency manager of Sonangol Pesquisa e Producao, SARL (Sonangol P&P sarl), Iraq during war and after for ENI in the ZFod JV and various projects in drilling or seismic) have 2 missions or two personalities with develop specific skills not especially following a scale of time but considering projection to a close to far future for the company . it's easy to understand that one key system is in mind , the Pear system

1.1.   Emergency manager or advisor:

apply the **PEAR** Program with the program of prevention of near misses, incident/emergency accident disaster and "Fait du Prince" in states decision. The pear program classifies the elements to be protected

2. **P**eople
3. **E**nvironment
4. **A**sset
5. **R**eputation

For sustain the pear program you have the key **HSE program** and **ERP preparation**,

1. Develop proactivity with training or HSE tools
2. Develops drills at each level (vessels, unit, regional, national) for evaluate the problems and the solutions in case of emergency
3. Verify the equipment like PPE, firefighting, BA and alarms in case of H2S
4. For offshore aerial, supply vessels are prepared
5. For onshore escape road are prepared
6. Insurrectional or war situation are trained with specific (examples enclosed)
7. The bridging documents must be done and verified with all the actors of the project or area

When all these stages are completed the Emergency manager can write the **ERP's (Emergency Response Procedure)** for each asset, the headquarter and draft the **Emergency Response Plan** for the unit of production or subsidiary in country.

Definition.

Emergency a serious, unexpected, and often dangerous situation requiring immediate action. *"your quick response in an emergency could be a lifesaver"*
An emergency starts when an alarm is activated and finishes when the situation is at 100 % controlled considering the Pear program
1. **P**eople are safe or under treatment in a medical facility
2. **E**nvironment risk are controlled or pollution is contained
3. **A**sset is in security without risk of escalation in own destruction
4. **R**eputation of the company is not compromised or at the minimum
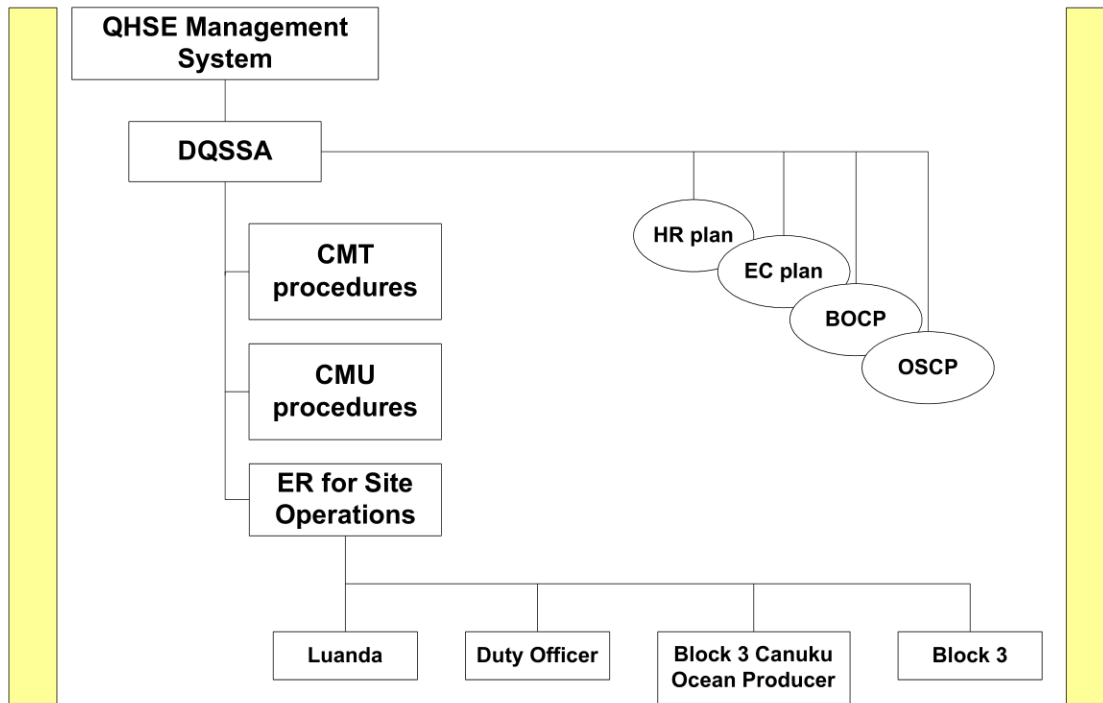
Emergency Response Plan — a set of written procedures for dealing with **emergencies** that minimize the impact of the event and facilitate recovery from the event. That's the time of writing the Emergency Response

At this moment the E&P have this own emergency response plan considering each asset, each project and the head quarter
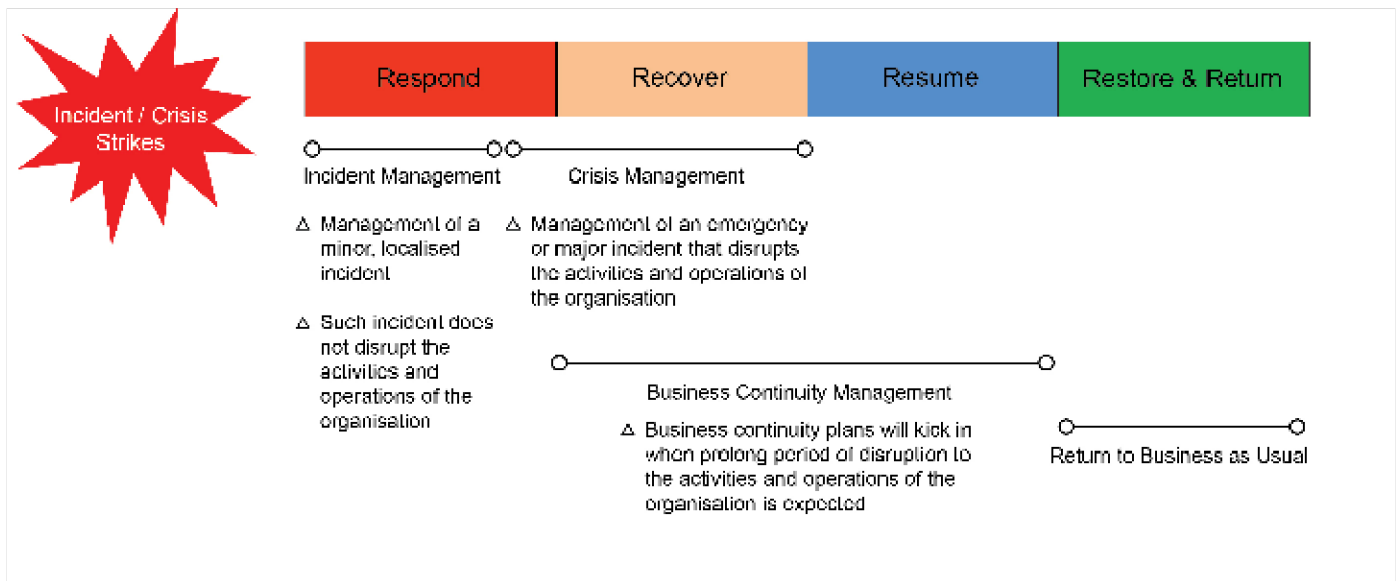
1.2.   Document Interfaces

The Emergency Response Plan   defines the requirements to ensure the document remains fit for purpose. The ERP defines this process in more detail. This emergency response plan fits within the system as a level 3 document, but is integrated with other level two documents such as company contingency plans as illustrated in the document hierarchy below given as example:

```
                    ┌──────────────────┐
                    │ QHSE Management  │
                    │     System       │
                    └──────────────────┘
                            │
                    ┌──────────┐
                    │  DQSSA   │─────────────────────┬──────────────┐
                    └──────────┘                     │              │
                         │                                     ⬭ HR plan
                    ┌──────────┐                          ⬭ EC plan
                    │   CMT    │                              ⬭ BOCP
                    │procedures│                                 ⬭ OSCP
                    └──────────┘
                         │
                    ┌──────────┐
                    │   CMU    │
                    │procedures│
                    └──────────┘
                         │
                    ┌──────────┐
                    │ ER for Site│
                    │ Operations │
                    └──────────┘
                         │
        ┌────────────┬───────────────┬──────────────────┬─────────────┐
   ┌────────┐  ┌──────────────┐ ┌──────────────┐  ┌──────────┐
   │ Luanda │  │ Duty Officer │ │Block 3 Canuku│  │ Block 3  │
   └────────┘  └──────────────┘ │Ocean Producer│  └──────────┘
                                 └──────────────┘
```

<p style="text-align:center; color:red">This illustration is an example of an ERP developed by Michel Friedman</p>

1.3.   Local organization

In each asset, project in a country or subsidiary /country you must have
- A trained-On Scene Commander and delegate will be nominated at all times, both able to reach the field command facilities in a reasonable time-frame (several minutes) to ensure suitable arrangements are put in place rapidly to mitigate the effects of an incident/emergency and coordinate emergency response activities.
- Suitable personnel will be nominated to assume command on any manned facility to ensure decisions can be made locally and immediately, and the emergency procedures described within are followed.
- Facilities will be maintained across the field allowing personnel in command positions to fulfill their role using an appropriate team response.
- Emergency arrangements will be sufficient to ensure that the asset emergency organization can be activated rapidly and personnel can be transferred to a place of safety at the earliest opportunity.
- The procedures within this plan remain appropriate for the operations.
- All personnel who work within the asset will be provided the necessary information to respond appropriately in the event of an emergency.

Drills and training are mandatory for all the personnel

1.4.   Organization

This field ERP covers all the fixed installations within the field, including the establishment and set-up of the Advanced Command Post (ACP), and the arrangements and procedures on all manned and unmanned installations:

- Field ERP Overview
- Normally Manned Installation specific information
- Normally Unmanned Installations specific information

1.5.   philosophy

Emergency Response Plans of contractor operated facilities must be designed to integrate within the Field ERP philosophy to ensure the functional response system is maintained. This can either be by design or by bridging documentation provided for the duration of the facility project life.

In-line with the ERP, Mission Cards, called MPR, are provided for key personnel. These should be used for induction, training and during emergencies where considered beneficial.
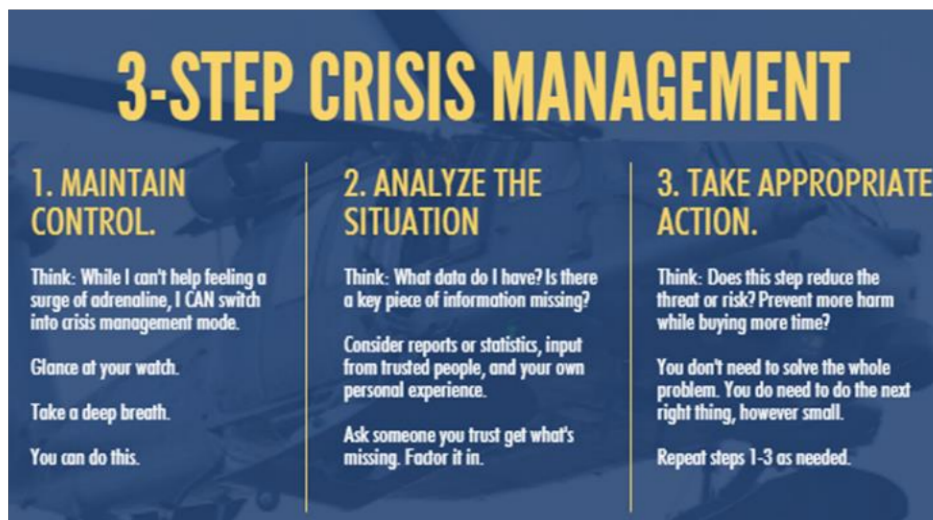
Mission Cards are defined and established to provide a description of Roles and Responsibilities of key personnel. Action aide memoirs are also provided for key personnel, to act as more specific guidance to carrying out their role.

Scenario checklists have been provided for use by the relevant PIC or any member of the OSC Team to ensure all aspects of the incident/emergency are considered and pre-planned guidance to incorporate company and local policy and philosophy.

1.6. The Maintenance of Information

The Field RSES is responsible for ensuring this document is maintained in-line with the ERP and also adequately to ensure key information that may be used during an emergency is accurate and up-to-date as soon as possible after any change.

Any person in the Asset emergency organization who may have a key role during an emergency (including those personnel onshore such as the Asset Duty Officers) are required to familiarize themselves with this plan. These personnel are required to bring to the attention of the Field RSES, any amendments that they consider appropriate.

3-STEP CRISIS MANAGEMENT

1. MAINTAIN CONTROL.

Think: While I can't help feeling a surge of adrenaline, I CAN switch into crisis management mode.

Glance at your watch.

Take a deep breath.

You can do this.

2. ANALYZE THE SITUATION

Think: What data do I have? Is there a key piece of information missing?

Consider reports or statistics, input from trusted people, and your own personal experience.

Ask someone you trust get what's missing. Factor it in.

3. TAKE APPROPRIATE ACTION.

Think: Does this step reduce the threat or risk? Prevent more harm while buying more time?

You don't need to solve the whole problem. You do need to do the next right thing, however small.

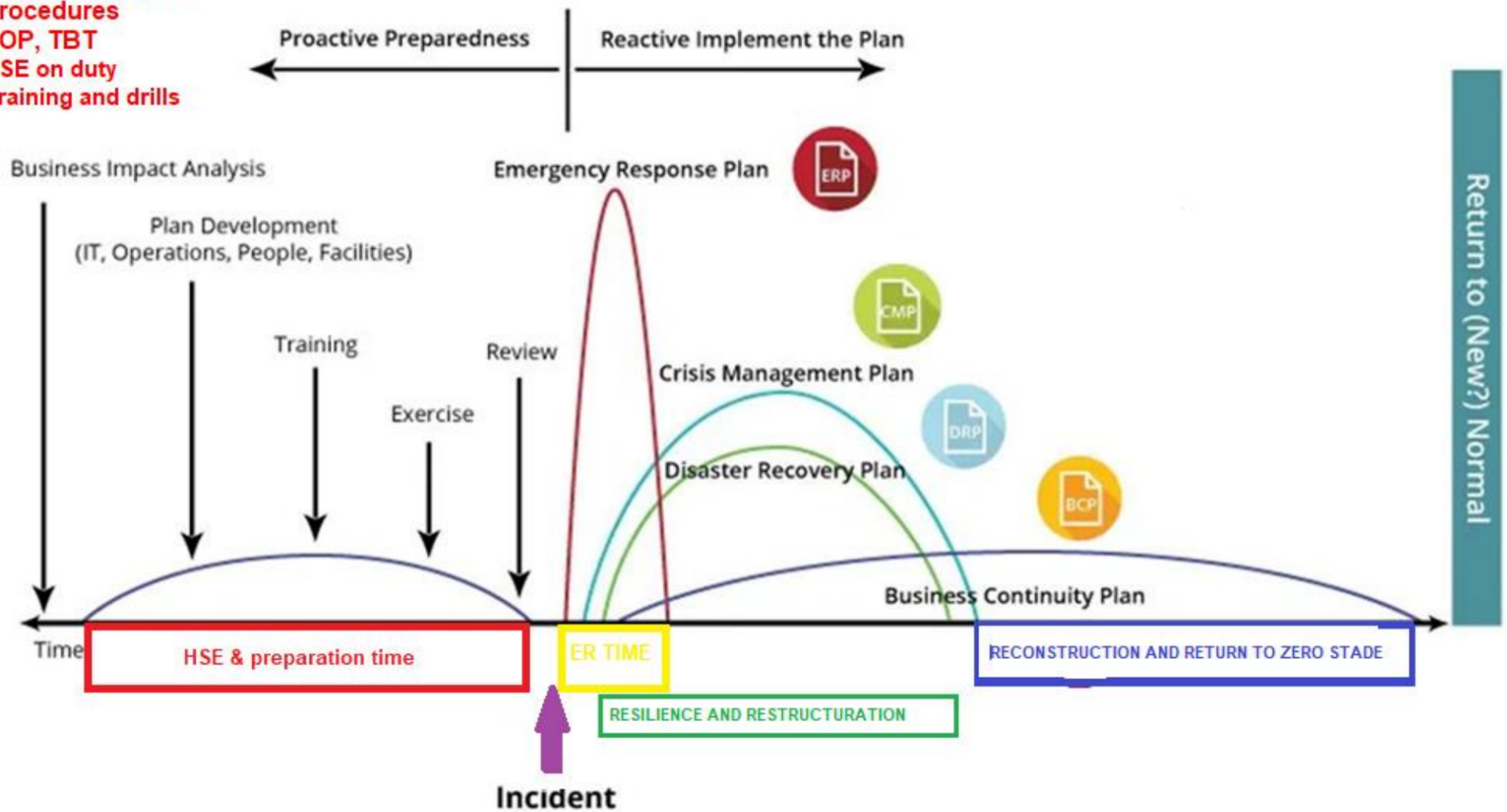Repeat steps 1-3 as needed.

1.7. Training

The training of personnel within the Asset and field rests with the Asset or field. This includes emergency training and suitable induction for all personnel, ranging from induction of all personnel on their required action in the event of an emergency, through to specific training for On-scene Commanders. However, specialist Major Emergency Management (MEM) training will be coordinated by the DQSSA in coordination with other emergency training and exercise needs of the company.

- The ER is Responsible for driving improvements in the regions ER arrangements which helps minimize the risks for personal and process safety in accordance with the Upstream Safety Leadership

- Principles to achieve the goal of **PEAR** program "no accidents, no harm to people and no damage to the environment" based on the two roots HSE training, developing proactivity and involve the personnel in the HSE philosophy of the company.

- Supports the development and implementation of consistent ER plans and initiatives for continuous improvement of site safety culture and HSE performance, and develops and conducts CC&ER and Business Support Team (BST) training programs for the Region.

- Develops a tactical ER work programme in conjunction with Incident/emergency Management Team's (IMT), BST and ER Manager in support of all aspects of the operations from Subsurface to Operations HSE plan deliverables.

- Delivers ER promotional activities and training to the site workforce and associated consulting/coaching on ER procedures/programmes and hazard identification to deliver strategic improvements.

- Plans the provision and documentation of training and exercises to maintain the capability of response personnel for the region. Coordinates the provision and documentation of training and exercises to maintain the capability of response personnel

- Maintains ER facilities in a state of readiness

- Actively participates and conducts ER audits, self-verification, equipment inspections identifying gaps, creating gap closure plans and implementing solutions, and assists with incident/emergency investigations and risk assessments.

- Develops and maintains the Region CCM management system in accordance with the Quality and Safety Management systems.

- Implements lessons learned process within ER to capture improvements identified during exercises and actual incident/emergency s.

- Develops insights from ER metrics analysis, contractor self-verification and other findings to advise on emerging risks and improvement opportunities for ER and provides direction to improve the region's management of incident/emergency s.

- Provides professional advice and support during ER responses, manages record-keeping for incident/emergency mobilizations and is part of the regions' On-call Rota.

HSE training AS:
Procedures
SOP, TBT
HSE on duty
Training and drills

Proactive Preparedness ← | → Reactive Implement the Plan

Business Impact Analysis

Plan Development
(IT, Operations, People, Facilities)

Emergency Response Plan — ERP

Training

Review

Crisis Management Plan — CMP

Exercise

Disaster Recovery Plan — DRP

Business Continuity Plan — BCP

Return to (New?) Normal

Time

HSE & preparation time

ER TIME

RECONSTRUCTION AND RETURN TO ZERO STADE

RESILIENCE AND RESTRUCTURATION

Incident

Incident and ER define the time for resilience and reconstruction for return zero time

1.8. Testing

The testing of the procedures will be regularly carried out to ensure the suitability of the emergency arrangements, facilities and personnel competencies within Asset. The following tests may be carried out to achieve this:

- Inspection of emergency equipment, facilities and procedures
- Emergency drills to ensure specific elements of the response arrangements are periodically checked
- Simulation exercises to validate the integration of arrangements across the field
- Full Scale Exercises (FSE) to demonstrate the robustness of the field emergency organization

The affiliate testing procedure identifies the requirements for the field to ensure adequate tests, as identified above, are carried out on a suitable basis. The Asset Emergency Drill and Exercise schedule specifies the frequency and scale of each of the testing methods for each facility.

2. Crisis, Continuity Response Advisor

We have seen in the first part of this document that HSE and emergency preparation are key for intent to avoid a incident, accident, disaster. It is easier to do the same type of preparation for managing the crisis and go back to activities so far it's possible. The most important is establishing clear concepts and instructions inside a document like the ERP document.

2.1. Purpose and application

This Directive defines the Orion Client requirements to effectively respond to crisis and emergency situations in a way that minimizes adverse impacts following the PEAR RULES:

DURING THE EMERGENCY YOU ONLY CONSIDER THE FOLLOWING POINTS

1. **P**eople
2. **E**nvironment
3. **A**sset
4. **R**eputation

This PEAR rule applies to all operating sites and activities where we are considered the operating company having prevailing influence. To efficiently and effectively implement this Directive we require commitment from all our people, at every level. Everyone in the asset, project must meet the requirements explained in this Directive and participate in any necessary training; and familiarize themselves with relevant site emergency response and evacuation requirements.

1. **Supervisors and Managers must:**
   ensure that everyone they supervise is made aware of, and understands, the requirements of this Directive and that they are adequately trained and competent to carry out their assigned tasks; and observe the activities they control and regularly check that they conform to this Directive.
2. **General Managers must:**
   demonstrate commitment to emergency and crisis preparedness by understanding and implementing this Directive; establish and implement a group emergency management plan for the business unit; reinforce their people's expectations about being prepared for emergencies and crises to ensure they conform with this Directive; communicate our expectations of business continuity and disaster recovery plan requirements, development and implementation.
3. **The Chief Risk Officer or CCMER leader must:**
 establish and implement our emergency response framework; implement an audit process to review, update and test emergency response, crisis management, business continuity and disaster recovery; provide training to ensure our people are able to follow the crisis and emergency management Directive.
4. **The Emergency Team Leader must:**
 follow the responsibilities as defined in the site emergency response and group emergency management plan templates
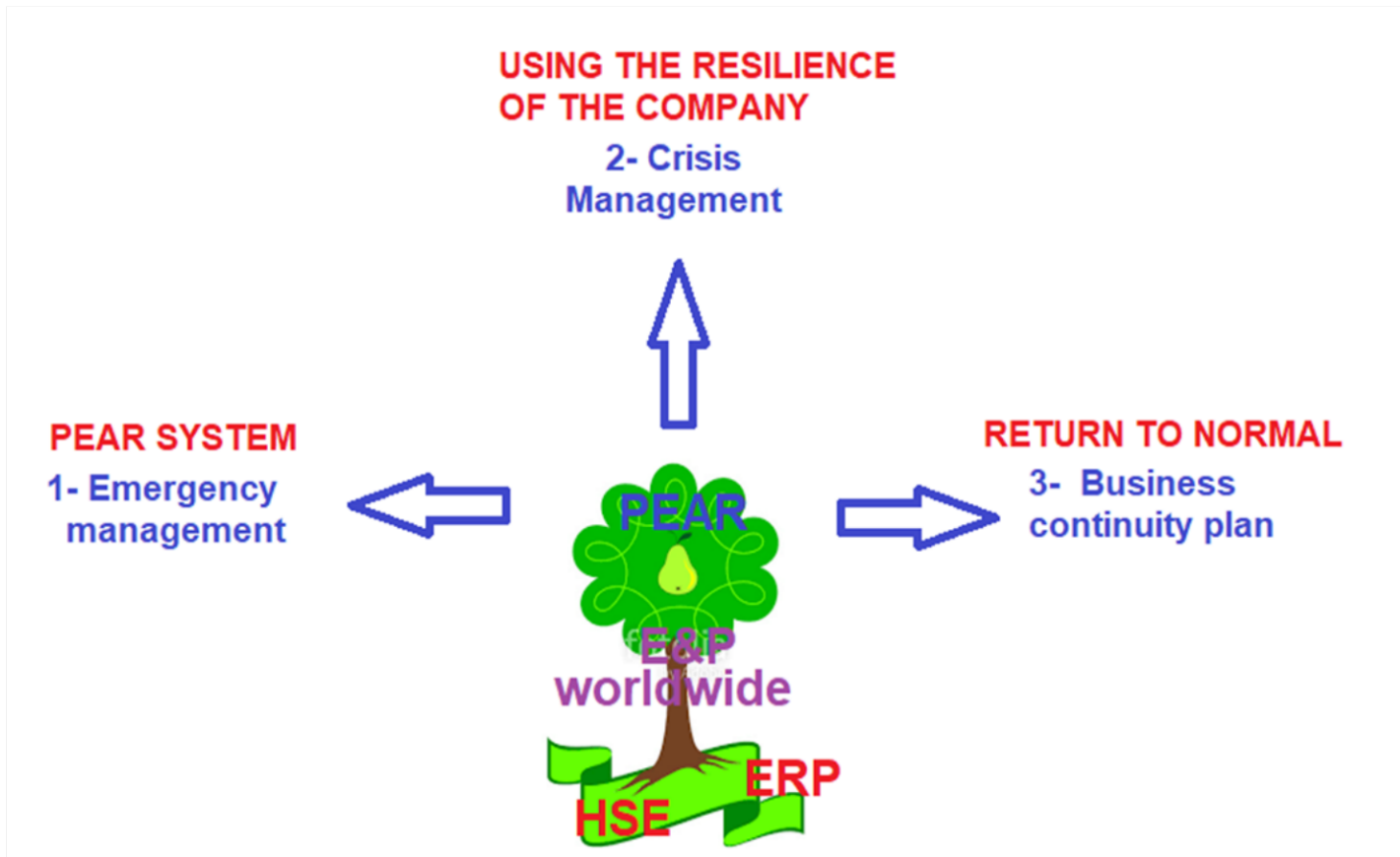
2.2. Requirements

2.2.1. General

In any crisis or emergency our priorities are to ensure the safety of all our people, relevant contractors and any public associated with, or affected by our operations and our activities; secure the site and minimize any effect on the environment by timely and effective management; minimize any effect on property and assets; contain and manage any effect on our company's reputation and business continuity; minimize any disruption to our operations and activities.

2.2.2. Emergency Escalation Process

We have a three-tier structure (Site Emergency, Group Emergency and Crisis) in our emergency response system, as shown in Figure below.

Escalation to the next tier must occur if the emergency team leader decides it is appropriate to do so. In any case, if an adverse event invokes either the site emergency response or group emergency management plan, the next tier leader must be informed, using the requirements of the First Response Protocol. After an event is escalated, the lower tier emergency team must continue operating, in conjunction with the upper tier. The plans outlined above must be developed and effectively implemented for all our operating sites and premises, in accordance with this Directive.
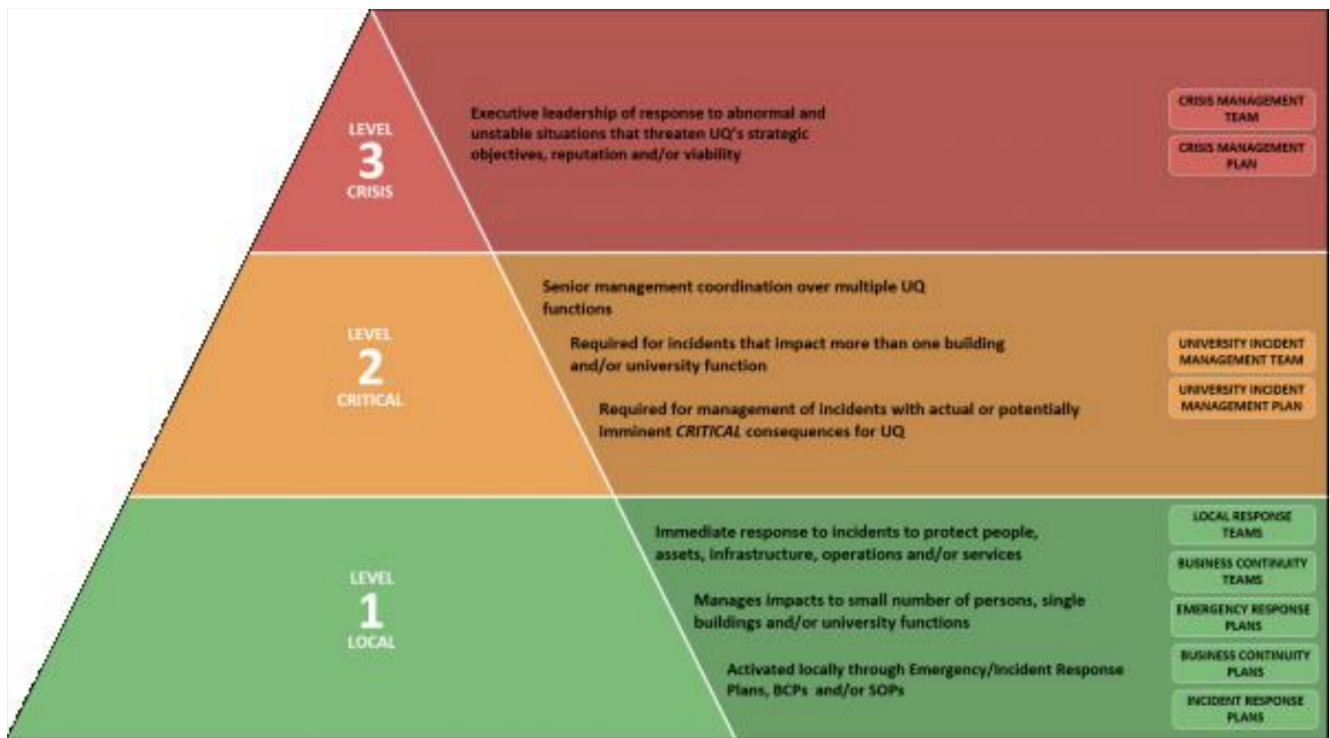
2.3 Crisis and Emergency Management Plans

Plans must be maintained in electronic format and controlled hard copies of relevant plans must be readily available in the designated emergency or crisis control room. Emergency or crisis plans must be reviewed annually to ensure they cover all possible emergency scenarios and contain all the information our people need to deal with them. In addition, relevant plans must be reviewed when improvement opportunities have been identified by post emergency or crisis exercise debriefings.

2.3.1 Site Emergency Response

All operating sites/activities must have a site emergency response plan, for which the emergency team leader is responsible. The site emergency response plan provides guidelines for initiating and maintaining effective emergency responses to likely emergency scenarios.

The plan must include:

- means by which emergency responses are initiated; (flash message, process in verbal communication)
- definitions of key roles and their responsibilities in an emergency response;
- descriptions of facilities and equipment required to coordinate an emergency response;
- a key contacts directory, which is reviewed and updated every quarter;
- the criteria for escalating an emergency and the means by which the group emergency management plan is initiated; typical emergency scenarios and guidelines for responding to them; communication and documentation requirements; evacuation protocols and muster points.

In developing and reviewing a site emergency response plan the relevant site or activity risk register (details are in the Risk Management Directive) must be used to validate the scope (emergency scenarios covered) of the Plan. At sites where Process Hazard Analysis (PHA) (details are in the Asset Integrity Directive) has been conducted, the validation of scope must also consider the consequence analysis. The annual review of the site emergency response

plan must also consider the adequacy of the site's emergency response capability, including the availability of emergency equipment and typical emergency scenarios. Sites classified as a Major Hazard Facility or a Dangerous Goods Location must incorporate the requirements of the National Standard for the Control of Major

Hazard Facilities, or equivalent local or state legislation, into their site emergency response plan. Additional information for developing a site emergency response plan can be found in the Site Emergency Response Plan template.

2.3.2 Group Emergency Management

Group emergency management addresses wider business unit activities that may encompass multiple sites or locations, and supports the site emergency response.
It is the responsibility of the General Manager of each business unit to have an established group emergency management plan, developed using the Group Emergency Management Plan template
The group emergency management plan template outlines the minimum mandatory requirements.

The plan must include:
 a description of how an emergency response is initiated; the first response protocol; criteria for escalating an emergency and how the crisis management plan is initiated; definitions of key roles and their responsibilities in an emergency response; communication and documentation requirements; a list of the facilities and equipment required to coordinate the emergency response; a key contacts directory, which is reviewed and updated every quarter. If the business unit needs additional resources to effectively respond to and manage an emergency situation, they may be added to the provided template. However, business units are not authorized to remove any information in the current template. There is more information about developing the group emergency response plan in the Group Emergency Management Plan template.

2.3.3 Crisis Management

Crisis management is managed by the Chief Risk Officer CCMER officer (or delegate) and focuses on high level support, advice and coordination of additional resources. Their aim is to assist emergency response efforts and determine appropriate strategic responses to protect our reputation and viability.

The crisis management plan must contain:
a description of an established crisis management team, consisting of key personnel, representative of the organization as a whole; criteria for escalating an emergency; the roles and responsibilities of each crisis management team member; reporting processes and requirements for internal and external stakeholders; a key contacts directory, reviewed and updated quarterly; communication and documentation requirements; a list of facilities and equipment required to coordinate the emergency response; a process to regularly review and test the plan; training requirements; details of established rooms and conference calls. There is more information about developing the Crisis Management Plan in the Crisis Management Plan document.

2.3.4 Business Continuity

The aim of business continuity planning is to ensure the availability of the resources needed to support essential business processes. Business continuity plans are invoked as a consequence of adverse events which affect critical activities, as a result of:

- loss of people;
- loss of workplace;
- Crisis and Emergency Management Directive
- loss of technology; or loss of assets.

All business units must follow the Business Continuity Development Process and complete a business impact analysis every 12 months (or when there are significant changes to the business) to identify business critical activities.

Critical activities that are identified must be included within a Business Continuity Plan and have an associated Recovery Plan developed. The Recovery Plan must identify key recovery processes, alternative resources and interdependencies.

The business continuity plan must contain:
a critical activity list; key contacts; technology requirements; recovery plans and associated business procedures.

Business units must complete annual business continuity training for all personnel holding a business continuity role, and test plans annually, at a minimum.

There is more information about developing a business continuity plan in the Business Continuity Plan – Development Guide.

2.3.5 Disaster Recovery

Disaster recovery is the ability to re-instate systems to their production state after an adverse event. Disaster recovery needs access to completely separate infrastructure, including an alternative communications network, server capacity, disk storage capacity, and tape drives, at an alternative site.

Information Technology (IT) must develop a disaster recovery plan, which includes:
processes for the declaration of a disaster; plans for activating the recovery and its ongoing co-ordination; timeframes for recovering systems, software, data and infrastructure outlined as dependencies in business continuity plans; plans for initial and ongoing communications to management and other relevant part of our business. At a minimum, the plan must be tested annually.

2.4 Crisis/Emergency Control Rooms, Equipment Selection, Maintenance and Reporting

Each site or area and relevant business function must establish and maintain a crisis or emergency control room and an alternative location, should the primary room be affected. Where possible, control rooms should be away from areas which may be affected by an emergency situation e.g. a fire in the plant. The emergency control room must have all the equipment and documentation needed to run an effective emergency or crisis response.

People who work in the crisis or emergency control room during an emergency or crisis must be competent in the set-up, running and roles and responsibilities of relevant specified positions of the response plan.

Risk management must be used (see the Risk Management Directive for details) to determine the type, quantity and location of emergency equipment needed for an operational site.   The site or area risk register should be used to help determine and validate emergency equipment

Emergency equipment must:
 be installed in accordance with manufacturer's instructions and/or relevant Australian Standards or equivalent;
 be readily accessible and within a reasonable distance from the source of the hazard; have appropriate signage and lighting.

Each site must have emergency response equipment identified in a site asset register and have a scheduled equipment maintenance program to ensure checks are documented and recorded.

Emergency equipment must be regularly inspected and tested in accordance with the relevant legislative requirements, standards and manufacturer's instructions, including the requirements of AS1851(Maintenance of Fire Protection Systems and Equipment). Inspections must be done by competent people, following controlled inspections check sheets.

2.5 Emergency Exercises

Emergency exercises must be conducted to test the effectiveness of crisis or emergency plans; validate the competency of key emergency response people; assess our capability to respond to an emergency; reinforce prior training; and identify opportunities for improvement. Emergency exercises must be designed to systematically include everyone likely to be involved in an incident, and may be in the form of:
 simulated emergencies;
 practical drills
 desktop exercises;
 resources and equipment check; or other exercises in relation with the necessities of the asset, tech ology or country.

An annual exercise must be conducted at sites with the potential for incidents requiring the initiation of the group emergency response plan or crisis management plan. The annual exercise should involve people from all relevant functional groups and test specific aspects of the site's emergency response plan. Group emergency plans and crisis management plans must be tested annually. A plan will be considered to have been tested if an actual emergency occurs and components of the plan are activated.

2.6 Personnel Location

Sites must maintain a system that enables timely identification of all people who are in the facility; or
 are not accounted for following an emergency evacuation of the facility.

2.7 Layout Drawings

All operational sites must maintain up to date location plans showing the positions of emergency response and fire fighting equipment. A copy of the plan must be available at all times.

2.8 Emergency Power Supply

An emergency power supply must be provided for critical equipment required in the event of an emergency (e.g. warning sirens, communications, fire pumps, extraction fans, etc) and to instruments and control systems needed to safely shut down the plant. Inspection and testing programs for emergency power systems must be incorporated into site critical function testing programs.

2.9. Records

Maintaining appropriate records is an essential part of implementation. The following records must be retained for five years: training records; records of emergency exercises; full records of emergency equipment inspections and testing.

2.10. Training and Competence

Our people must be trained and competent to fulfil their roles as defined in the relevant emergency and crisis management plans. Training must be refreshed annually. People participating in an emergency exercise, in their defined roles, are considered to have met their refresher training requirement. To develop and maintain our emergency process competency, minimum training requirements have been established in a Diagnostic Matrix for each tier of the emergency response framework.
Training and materials provided fall under three main categories.
Crisis Management, which includes the Orion Client crisis management plan; consistent training provider; and one consistent training package.

Group Emergency Management, which includes Group Emergency Management Plan template; consistent training provider; and one consistent training package.

Site Emergency Response, which includes: Site Emergency Response Plan template; consistent competency assessment tool; training delivery coordinated and administered within the business unit.

2.11. Deviations

Deviations from the requirements of the standard and established directive may only be considered when: regulatory obligations dictate otherwise; implementation of the requirement is not technically feasible due to local conditions or the cost of implementing the requirements substantially exceeds the benefits.

To deviate from a Directive, you must:
 Specify the implications of implementing the requirement as specified within the directive. Determine the risk of not implementing the requirement of the directive (in accordance with the Orion Client Risk Management Directive) and document the impact and duration of the deviation and identified control measures. Have the deviation authorized by obtaining documented approval from the Orion Client business unit General Manager (or equivalent person with DOA of 3 or higher) and the Chief Risk Officer.

Authorization of all deviations, whatever their duration, will be recorded on Orion Client's Deviation Register. The risk associated with the deviation is to be recorded on the relevant business unit or site risk register.

In the client HSE MS under the chapter Management of change you must have Deviation Guide and Deviation Request Form.

2.12. Compliance and Assurance

The Orion client must require all of the employees to comply with this directive. Compliance with this directive will be periodically monitored by the Chief Risk Officer or delegate and will be included in the scope of relevant audits/reviews. Compliance against the requirements established within this directive must be reviewed as part

of the business unit internal audit schedule, and the HSE management system audit cycle. Monitoring and verification of key requirements is to be included in business unit key performance indicator reporting requirements, and must include, but is not limited to plan development; exercise schedule; training and testing completion; equipment maintenance and testing; critical function and control testing of emergency equipment and backup power supplies;

corrective action completion following exercise debriefs.
The crisis and emergency management directive audit tool has been established to assist the business in reviewing compliance to the requirements established within this directive. Any breaches of this directive by employees will be addressed in accordance with Orion Client's Employee Counselling and Disciplinary Policy and its associated procedures.

2.13 Toolkits
The following materials support the implementation of this directive:
1. Crisis Management Plan 2. Group Emergency Management Template 3. Site Emergency Response Template 4. Business Continuity Plan – Development Guide 5. Business Continuity Plan – Development Process 6. Critical Process/Activity Recovery Plan - Template 7. Business Continuity Plan – Template 8. Audit Protocol – Crisis and Emergency Management Directive 9. Diagnostic Matrix