# Comintelli Policy on Business Continuity Management and Disaster Recovery

## Background and purpose

According to ISO 22313:2012; "Business continuity is the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. Business continuity management (BCM) is the process of achieving business continuity and is about preparing an organization to deal with disruptive incidents that might otherwise prevent it from achieving its objectives. In this International Standard, the word business is used as an all-embracing term for the operations and services performed by an organization in pursuit of its objectives, goals or mission. As such it is equally applicable to large, medium and small organizations operating in industrial, commercial, public and not-for-profit sectors."

Comintelli's BCM has three key goals in the event of any disruption to the company's operations:

- The continued service to our customers, ensuring as minimal as possible impact on their business and usage of Comintelli systems and services.
- The safety and wellbeing of all Comintelli staff and affiliate subcontractors and partners.
- The retained confidence of financial markets, owners, creditors and suppliers to the business, ensuring continued access to funds and required operations resources.

Furthermore, the herein included Systems Disaster Recovery Plan is to ensure that cloud/SaaS customers of Intelligence2day®, in the event of extended service outages caused by factors beyond Comintelli's control, will have services restored to the widest extent possible in the shortest time frame possible. All customer sites have preventive measures implement to minimize network failure and to enable recovery as rapidly as possible when a failure occurs. The plan identifies vulnerabilities and specifies necessary measures to prevent extended service outages. In particular it:

- serves as a guide for the recovery teams.
- identifies procedures and resources needed to assist in recovery.
- identifies other parties that must be notified in the event of a disaster.
- assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
- identifies alternate sources for supplies, resources and locations.
- documents storage, safeguarding and retrieval procedures for vital records.

## BCM review

The BCM system described herein is monitored, revived and evaluated, at least annually and, as such, annually reviewed and approved by the company board of directors. Further, the plan is exercised on an annual basis. Such test and exercise may be in the form of a walk-through, mock disaster or component testing. This document is stored in a common location where it can be viewed by all personnel.

## Company organization and general operations risk

Comintelli is a highly specialized organization divided into four units; Marketing, Sales, Customer Operation and SW development. In a short-term disruptive perspective, it is the Customer Operations unit that is most exposed to any such risks due to its responsibility to ensure customer system uptime and support. In a mid- to long-term perspective Customer Operations is still key to our customers but from a business going concern perspective all units are of equal risk exposure.

## Disruption risk minimizing operations design

Comintelli has its office facilities in Kista Science tower north of Stockholm. All physical facilities security matters are covered in Comintelli Policy on Security and IT. The company is however fully operational without access to the facilities as all company data and communication services are based on cloud services. Hence, should, for any reason, the office access be disrupted due to e.g. terror attacks, fire or other access delimiting matters, while not physically affect any Comintelli staff, company operations would continue uninterrupted via cloud collaboration within and between the different teams.

Adding to this, all company internal data such as commercial documents, development documents etc. are all stored and managed with one of the major international providers of such cloud services. Should however, for any reason, the access to this provider's services be interrupted more than marginally, the company ensures that all such data, including complete collections of program source code, are physically backed-up daily on three separate encrypted instances. Hence, should disaster struck the company's internal data, operations could be fully restored within 24 hours. The exception would be a general disruption including natural disaster, terror attack, targeted crime, pandemic or other event significantly disrupting Comintelli's staff ability to undertake necessary work procedures, including the loss or death of key personnel.

## Disruptive Event definition

A disruptive event is an event that is deemed as a potential Disaster. The event will remain as a disruptive event, and managed as such by normal procedures, until, after event analysis and assessment, disaster is declared.

## Disaster definition

For the purpose of this Policy, Disaster is defined as any loss of utility service, connectivity, or catastrophic event that causes a disruption to the business and/or and in the service provided to customers.

## Disaster management roles and responsibilities

Comintelli maintains three roles in relation to Disaster Management:

- Incident Response Coordinator (IRC) = Comintelli CTO
- Incident Management Team (IMT) = Comintelli management team
- Incident Response Team (IRT) = as assigned depending on nature of Disaster

Any employee can alert any of the above on the matter of a Disruptive Event and that Disaster might need to be declared. Each role/team has its own directory with change management authority limited to the IRC only. The IRC is responsible for the plan.

On an ongoing basis, the IRC should:

- Provide hard copy of this document to all staff. All staff must store a copy at home or electronically via a hand-held device or laptop computer.
- Regularly review and update information in the disaster recovery plan registers (e.g., contact lists, equipment inventories).
- Communicate with the IMT to get up-to-date information periodically.
- Hold initial team meeting to get team members acquainted with the plan and hold annual meetings to review the plan on an ongoing basis
- Maintain an accurate record of the locations of alternate sites, equipment suppliers, data storage locations, and implementation plans.

Each team member should:

- Designate an alternate backup
- Keep an updated calling list of their work team members' cell phone numbers both at home and at work.
- Familiarize themselves with the contents of this plan.

## Action lists, personnel data and recovery data forms

Named details of teams, data storage and access procedures, physical relocation plans etc. are kept in internally confidential documents, accessible to all employees at all times. Such documents may or may not be referred to from this document due the level of confidentiality and security.

The remainder of this document outlines plans and actions that are to be put in operation at any time of a declared disaster. If a disaster is declared, all steps in the plans outlined herein MUST be followed through, even if the disaster declared is perceived as settled. This plan becomes effective when a disaster is declared and remains in effect until operations are resumed at the original location, or a replacement location and control is returned to the appropriate functional management.

### Event analysis and assessment

In case of a disruptive event, the IRC will contact the IMT and provide the following information:

- Location of event
- Type of event(e.g. server hall failure, malicious attack, staff fatalities or disposition)
- Summarize the event damage (e.g., minimal, heavy, total outage)
- An estimated timeframe of when a damage assessment group can enter the facility (if possible). The damage assessment group may be a third party team that will report their findings

Based on the information obtained, the IMT decides (with the IRC) whether to declare disaster or not.

### Operations Disaster prerequisites

Regardless of the disruptive event circumstances, or the identity of the person(s) first made aware of the disaster, the IMT must be activated immediately in any of the following operations events:

- One or more of Comintelli staff is fatally affected or severely decapacitated.
- One or more of Comintelli staff is rendered non-contactable due to acts of war, kidnapping or other unforeseen events disenabling the employee(s) to undertake their job responsibilities and retain personal safety.
- General infrastructure (transport, internet, etc) affected in such a way that the operations of the organization is more than temporarily unable to remain going concern.

### System Disaster prerequisites

Regardless of the disruptive event circumstances, or the identity of the person(s) first made aware of the disaster, the IMT must be activated immediately in any of the following systems events:

- 10% or more of intelligence2day instances are down concurrently for twentyfour or more hours
- Any problem at any system or network facility that would cause the above condition to be present or there is certain indication that the condition is about to occur.
- Any problem at any system or location that would cause the above condition to be present or there is certain indication that the above condition is about to occur.

### Declaring state of Disaster

The Incident Response Coordinator has the mandate and responsibility to declare a disaster, should that be called for. If for any reason, the IRC is not capable of doing so, any member of the management team in conjunction with the CEO may do so in the absence of the IRC. If the assigned IRC remains not capable of upholding the mandate, the IRC mandate is by default transferred to the CEO (and in his/her absence in order of priority, CFO, SvP Customer Operations) who may by order delegate the mandate to any member of the management team or specialist staff.

A disaster can take on two major forms; an operations disaster or a systems disaster, or both. Depending on which, the disaster recovery actions differ to some extend but there are also many common aspects and activates that should be managed and initiated.

### Executing Disaster recovery - General

The IRC will contact the respective team leader and report that a disaster has taken place.
Under the direction of local authorities and/or IRC/IRM further assess the damage to the affected location and/or assets. The IRC shall include vendors/providers of affected assets to ensure that their expert opinion regarding the condition of the equipment is determined a.s.a.p.

In particular, the IRC should immediately:

- Assess procedures
- Gather requirements
- Review Safety and security issues

Document assessment results using Assessment and Evaluation Forms are contained in separate data forms.

If facilities access permits, the IRC should:

- Conduct an on-site inspection of affected areas to assess damage to essential hardcopy records (files, manuals, contracts, documentation, etc.) and electronic data
- Obtain information regarding damage to the facility (s) (e.g., environmental conditions, physical structure integrity, furniture, and fixtures) from facilities management or relevant authority.

Upon notification of a potential disaster during working hours, ensure that personnel on site have enacted standard emergency and evacuation procedures if appropriate and notify the IRC accordingly. If out of working hours, relevant team members should contact the IRC immediately upon receiving such notification.

## External communications

Public communications is the responsibility of the CEO or the Investor Relations communications manager. Comintelli Public Relations personnel are designated as the principal contacts with the media, regulatory agency, government agencies and other external organizations following a formal disaster declaration. Customer communication is the responsibility of the head off the Customer Operations unit.

## Emergency management procedures

The following procedures are to be followed by assigned personnel in the event of an emergency. Where uncertainty exists, the more reactive action should be followed to provide maximum protection and personnel safety. In the event of any situation where access to a building housing a system is denied, personnel should report to alternate locations.  Primary and secondary locations are listed in an internal confidential document.

## Operations Disaster Recovery

When an operations disaster is declared, the following set of actions should be taken without any delay. Step 1 to 7 must be completed in less than 8 hours disregarding when in a calendar week disaster is declared.

| Step | Action |
|---|---|
| 1 | IRC mobilize IMT |
| 2 | If relevant, initiate contact with appropriate authority to safeguard the safety of affected personnel. IRC to retain such dialogue until staff safety is ensured. |
| 3 | Using the call list in IMT members contact team members, to inform them of the situation. If known, advise as to when operations will be restored or what actions will be taken to restore operations. |
| 4 | The Incident Response Team (IRT) is mobilized. The recovery team will prepare for the appropriate recovery actions. IRT members will, if called for, assemble at agreed location(s) as quickly as possible. |
| 5 | IMT to reassign key responsibilities in case of staff shortages |
| 6 | IMT to document current as-is customer operations capability and address any deficiencies that will more than marginally/temporarily affect such capability. |
| 7 | IRC will, based on discussion with IMT, assess if the status of events shall remain as disaster. If no, proceed to 11. If yes proceed to step 8. |
| 8 | IRC instructs IRT to initiate deployment of response plans and report to IRC immediately upon fulfillment of such deployment. |

| | |
|---|---|
| **9** | With the support of IRT, IRC now monitors all critical operations on an ongoing basis and report to IMT any deviations for a going concern requirement. IMT is stand-by to support IRC with any necessary actions. |
| **10** | Every 24 hours IRC will return to step 7 for evaluation. Step 9 continues until step 7 is deemed No. |
| **11** | IRC calls off the status of disaster. IMT informs all teams and operations returns to normal with the possibility that the reassigned responsibilities according to 5 above may be retained for a period of time depending on the situation. |

## Systems Disaster Recovery

The scope of this Systems Disaster Recovery addresses technical recovery only in the event of a significant disruption.

This disaster recovery plan provides:

- Guidelines for determining plan activation;
- Technical response flow and recovery strategy;
- Guidelines for recovery procedures;
- References to key Business Resumption Plans and technical dependencies;
- Rollback procedures that will be implemented to return to standard operating state;
- Checklists outlining considerations for escalation, incident management, and plan activation.

The specific objectives of this disaster recovery plan are to:

- Immediately mobilize a core group of leaders to assess the technical ramifications of a situation;
- Set technical priorities for the recovery team during the recovery period;
- Minimize the impact of the disruption to the impacted features and business groups;
- Stage the restoration of operations to full processing capabilities;
- Resume normal operations once the disruption has been resolved if determined appropriate by the recovery team.

Within the recovery procedures there are significant dependencies between and supporting technical groups within and outside Comintelli. This plan is designed to identify the steps that are expected to take to coordinate with other groups / vendors to enable their own recovery. This plan is not intended to outline all the steps or recovery procedures that other departments need to take in the event of a disruption, or in the recovery from a disruption.

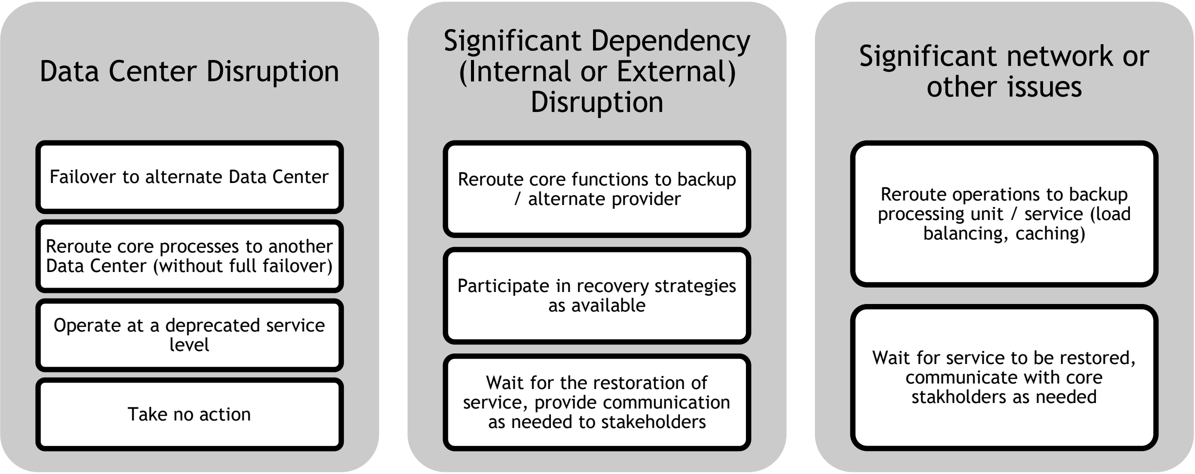
## Dependencies

This section outlines the dependencies made during the development of this Intelligence2day disaster recovery plan. If and when needed the DR team will coordinate with their partner groups as needed to enable recovery.

| Dependency | Assumptions |
|---|---|
| **User Interface components** | • Users (end users, power users, administrators) are unable to access the system through any part of the instance (e.g. client or server side, web interface or downloaded application).<br>• Infrastructure and back-end services are still assumed to be active/running. |
| **Processing components** | • The back end processing of information e.g. delivery of Alerts to end users is not functioning (with or without the user interface layer also being impacted).<br>• Components that process incoming data feeds processing and data parsing are not working. |
| **Network Layers**<br>**Infrastructure components** | • Connectivity to network resources is compromised and/or significant latency issues in the network exist that result in lowered performance in other layers. |
| **Storage Layer Infrastructure components** | • Loss of SAN, local area storage, or other storage component. |
| **Database Layer**<br>**Database storage components** | • Data within the data stores is compromised and is either inaccessible, corrupt, or unavailable |
| **Hardware/Host Layer**<br>**Hardware components** | • Physical components are unavailable or affected by a given event |
| **Virtualizations (VM's)**<br>**Virtual Layer** | • Virtual components are unavailable<br>• Hardware and hosting services are accessible |
| **Administration**<br>**Infrastructure Layer** | • Support functions are disabled such as management services, backup services, and log transfer functions.<br>• Other services are presumed functional |
| **Internal/External Dependencies** | • Interfaces and intersystem communications corrupt or compromised |

## Disaster Recovery Strategies

The overall DR strategy is summarized in the table below and documented in more detail in the supporting sections. These scenarios and strategies are consistent across the technical layers (user interface, processing, etc.)



Data Center Disruption

- Failover to alternate Data Center
- Reroute core processes to another Data Center (without full failover)
- Operate at a deprecated service level
- Take no action

Significant Dependency (Internal or External) Disruption

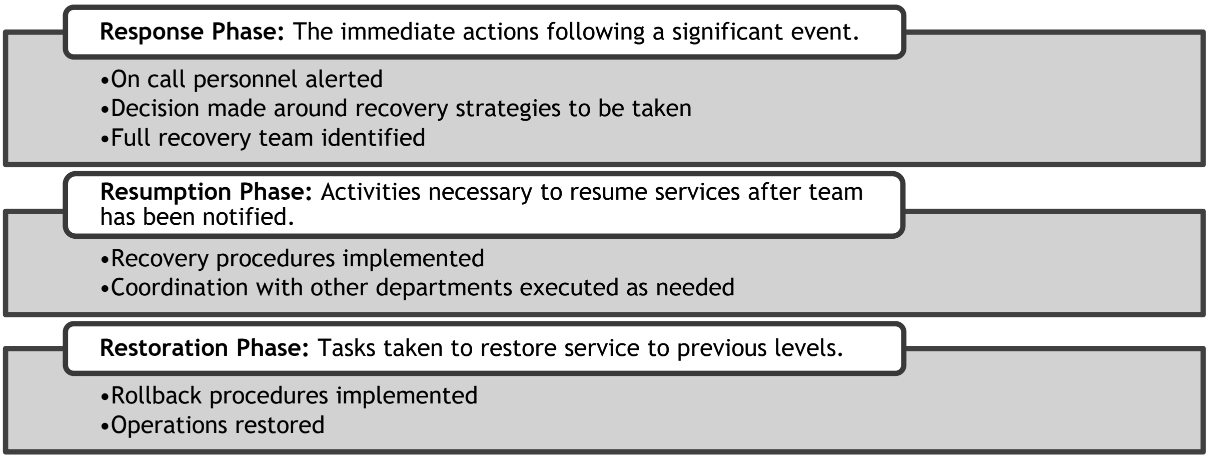
- Reroute core functions to backup / alternate provider
- Participate in recovery strategies as available
- Wait for the restoration of service, provide communication as needed to stakeholders

Significant network or other issues

- Reroute operations to backup processing unit / service (load balancing, caching)
- Wait for service to be restored, communicate with core stakholders as needed

## Disaster Recovery Procedures

A disaster recovery event can be broken out into three phases, the response, the resumption, and the restoration as described below.



**Response Phase:** The immediate actions following a significant event.

- On call personnel alerted
- Decision made around recovery strategies to be taken
- Full recovery team identified

**Resumption Phase:** Activities necessary to resume services after team has been notified.

- Recovery procedures implemented
- Coordination with other departments executed as needed

**Restoration Phase:** Tasks taken to restore service to previous levels.

- Rollback procedures implemented
- Operations restored

## Response Phase

During the response phase, parties and items necessary for a DR response in this phase are identified and alerted. These procedures are the same regardless of the triggering event (e.g. whether caused by a Data Center disruption or other scenario) and includes the following: issue communicated and/or escalated, priorities are set, selection done of core team members required for restoration phase and a creation of disaster recovery event command centers as needed.

## Resumption Phase

During the resumption phase, System Recovery Full System Failover is undertaken. Restoration procedures are identified, risks are assessed for each procedure, and coordination points between groups are defined. Further, issue communication process and triage efforts are established, recovery steps executed, tests assigned and performed and results are summarized and communicated to group

## Restoration Phase

During the restoration phase, steps are taken to enable recovery but will vary based on the type of issue. In general, restoration procedures are determined, server level recovered, tests assigned and performed and results summarized and communicated to group. Declaration of successful failback is communicated to stakeholder group and the Disaster recovery procedures closed.

## Glossary/Terms

Standard Operating State: Production state where services are functioning at standard state levels. In contrast to recovery state operating levels, this can support business functions at minimum but deprecated levels.

Presentation Layer: Layer which users interact with. This typically encompasses systems that support the UI, manage rendering, and captures user interactions. User responses are parsed and system requests are passed for processing and data retrieval to the appropriate layer.

Processing Layer: System layer which processes and synthesizes user input, data output, and transactional operations within an application stack. Typically, this layer processes data from the other layers. Normally, these services are folded into the presentation and database layer, however for intensive applications; this is usually broken out into its own layer.

Data Layer: The data layer is where data typically resides in an application stack. Typically data is stored in a database such as Cassandra or SQL Server, but it can be stored as XML, raw data, search indexes or as binary files on disk. This layer typically is optimized for data querying, processing and retrieval.

Network Layer: The network layer is responsible for directing and managing traffic between physical hosts. It is typically an infrastructure layer and is usually outside the purview of most business units. This layer usually supports load balancing, geo-redundancy, and clustering.

Storage Layer: This is typically an infrastructure layer and provides data storage and access. In most environments this is usually regarded as Local, SAN or NAS storage.

Hardware/Host Layer: This layer refers to the physical machines that all other layers are reliant upon. Depending on the organization, management of the physical layer can be performed by the stack owner or the purview of an infrastructure support group.

Virtualization Layer: In some environments virtual machines (VM's) are used to partition/encapsulate a machine's resources to behave as separate distinct hosts. The virtualization layer refers to these virtual machines.

Administrative Layer: The administrative layer encompasses the supporting technology components which provide access, administration, backups, and monitoring of the other layers.