Business Continuity and

Disaster Recovery Overview

For Unit4 Global Managed Cloud Operations

Introduction

Business Continuity and Disaster Recovery Overview document was prepared to provide information on how Unit4 Global Managed Cloud Operations is prepared to minimize disruption to the services in times of crisis. Since disaster happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster helps Unit4 Global Managed Cloud Operations to continue its operations, minimizing the impact for customers.

Unit4 Global Managed Cloud Operations understands the needs of having a resilient service, this is why it maintains a Business Continuity process supported by Disaster Recovery Plans. Global Head of Cloud Operations is accountable for the proper delivery of those commitments, with full support of Global Service Leader.

Scope

Within scope of Business Continuity process are the delivery services provided by Unit4 Global Managed CloudOperations to customers. A detailed list of services can be found in Unit4 Managed Cloud Services Catalogue. This includes also following components of production systems:

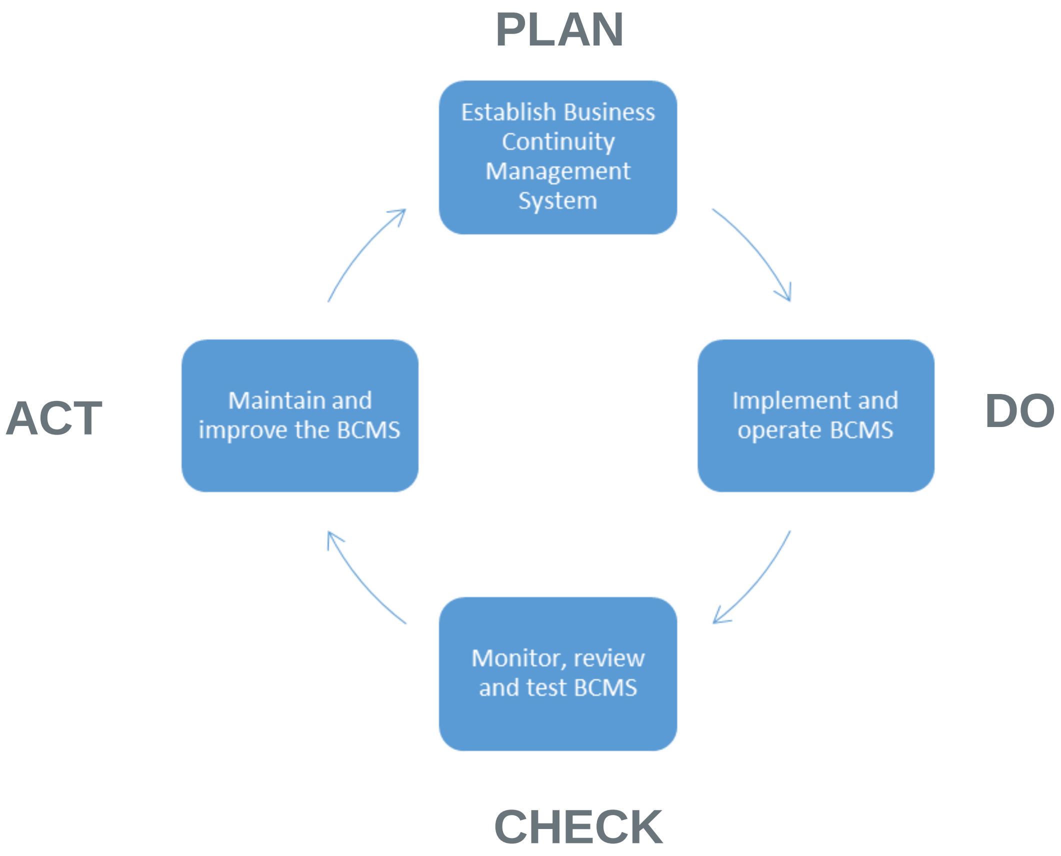
- Infrastructure;
- Software;
- Data;
- Communications link.

Outside the scope are:

- Customer locations & infrastructure;
- Customer (internet) connection;
- External systems interconnected with the Unit4 Service.

Business Continuity Process

Business Continuity Process main objective is to ensure that Unit4 Global Managed Cloud Operations is prepared to continue to operate in case of serious incidents or disasters. The overall process can be presented on a Plan, Do, Check and Act (PDCA) cycle illustrated below.


PLAN
Establish Business Continuity Management System
DO
Implement and operate BCMS
CHECK
Monitor, review and test BCMS
ACT
Maintain and improve the BCMS

1. Establish Business Continuity Management System (BCMS) – preparation of a comprehensive system, which will allow to meet the goal of Business Continuity. This includes development of policies, plans and measurements. An important part of this is risk assessment.
2. Implement and operate BCMS – making sure that the principles of BCMS and guidelines from policies are implemented and working in operational environment, including a resilient architecture.
3. Monitor, review and test BCMS – an ongoing process of monitoring the process. This also includes a major annual review of the system and annual tests of DR plans.
4. Maintain and improve the BCMS – there is always room for improvement, especially in an ever changing environment. All of the lessons learned need to be implemented into the process.

Risk assessment

To cover for threats to business continuity and plan recovery from unexpected disasters it is essential to identify the threats or risks that can jeopardize business continuity. Unit4 Global Managed Cloud Operations is in the process of incorporating a comprehensive risk management framework which will use selected best practices of ISO 31000:2009 – Risk management. The process of risk assessment from Business Continuity is an ongoing effort, which needs to incorporate challenges of rapidly changing environments and factors.

Main identified threats are:

1. Loss of IT
   Information systems are the main assets, which unavailability will impact the customers. This is not only limited to the IT which hosts customer's environments, but also internal IT which support the staff providing services.
2. Loss of premises
   Unit4 Global Managed Cloud Operations is an organization working in different offices across the globe. It is necessary to understand the risk related to losing the buildings and infrastructure.
3. Loss of staff
   Unit4 Global Managed Cloud Operations staff is an important resource, which provides a 24/7 support for the customers and maintains the systems. The risk related to loss of staff, for example due to pandemic events, has to be understood.

Unit4 Global Managed Cloud Operations is committed to prepare contingency and recovery plans for identified threats.

Disaster Recovery

Disaster is defined as catastrophes including (but not limited to): natural disasters such as floods, hurricanes, tornadoes or earthquakes, hazardous material spills, infrastructure failure, and bio-terrorism. Non-catastrophic events such as server outages, IT hardware or software failure and other such disruptions are not considered disasters and are covered by high availability features of the operating environment.

When a disaster strikes, the normal operations of the enterprise are suspended and replaced with operations that spelled out in the Disaster Recovery plan. Comprehensive Disaster Recovery (DR) of the Unit4 Cloud solution is provided for all Unit4 Cloud customers.

Assurance

Disaster Recovery services are audited and there is an annual test of the plans. As the plans and procedures are living documents, they are improved with the lessons learned during the testing. An abstract of the results of the test will be published on the Customer Portal, available to authorized personnel for review.

Recovery objectives

Dependent on the Service Level Agreement, Disaster Recovery will use following objectives:

- Standard service model: RPO 2 hours / RTO 48 hours

In the event of a disaster Unit4 can utilize the secondary data center in the specified zone immediately in order to meet RPO/RTO commitments.

Information Security

It is important to understand that Information Security cannot be forgotten during disaster events. Information Security team reviews the processes and plans to make sure that not only the availability of information is taken into account during restoration procedures, but also the confidentiality and integrity. More details regarding Information Security can be found in Unit4 Managed Cloud Information Security Policy.

Additional benefits

Business Continuity and Disaster Recovery is not the only process which supports the availability and performance of applications for customers. Following standard measures are deployed across the environments:

1. High availability
   Unit4 Global Managed Cloud Operations uses highly available systems, which are set up with redundancy allowing automated failover to the secondary node in case of component outages.

More details regarding Unit4 Global Managed Cloud Operations commitments regarding availability and performance can be found in the Unit4 Managed Cloud Service Level Agreements.

Supporting customer's Disaster Recovery

Unit4 offers additional services which can support customer's disaster recovery:

1. Forgiveness restore

Customers are provided the option for a "Forgiveness" restore, where a recent Production backup can be restored to the Production environment in case of a disastrous user mistake (e.g. running month end processing in Production instead of in Preview as intended). Backups are performed such that the restore contains data no older 2 hours for Standard service model subscribers. Forgiveness restores are initiated within 4 business hours after request and time to complete depends on data volume. Unit4 is retaining the backup data for up to one year.

2. Production database access

Customers can opt to add access to a read-only copy of production data that is within 15 min of the production data (copy can be up to 15 min behind production). This isn't something that is suited for backup, it is intended as a source to run BI ETL and reporting type workloads. It is not permitted to receive direct access to production database.

3. Production database copy

When customers want to have a recent copy of their production database available on another location (for instance on premises), customers can request a copy of production database, which Unit4 can export to another Unit4 SFTP area on a weekly basis as an additional service with extra costs. The export will be in a format usable with the latest version of Microsoft SQL Server. Customers can manually download this export from this location. Each export will be retained for 4 weeks. This functionality can be used to meet some bespoke data retention and data analytics requirements, or to add an additional layer of protection against cloud outages.