|  |  |
| --- | --- |
| **Council 2020 Geneva, 9-19 June 2020** |  |
|  |  |
|  |  |
| **Agenda item: ADM 6** | **Document C20/15-E** |
| **30 March 2020** |
| **Original: English** |
| Report by the Secretary-General | |
| ORGANIZATIONAL RESILIENCE MANAGEMENT SYSTEM (ORMS) | |

|  |
| --- |
| Summary  Council-17 approved the establishment of an Organizational Resilience Management System (ORMS) Project.  This report provides the project background; summarizes the project findings, describing the ORMS framework (Business Continuity and (BC) and Crisis Management (CM)); and contains three recommendations.  Action required  The Council is invited to **note** this report, to **approve** the recommendations and to **advise** on potential sources of funding for a data classification project.  \_\_\_\_\_\_\_\_\_\_\_\_  References  [C16/70](https://www.itu.int/md/S16-CL-C-0070/en), [C17/63](https://www.itu.int/md/S17-CL-C-0063/en), [C20/53](https://www.itu.int/md/S20-CL-C-0053/en) |

**ORMS Project Overview & Deliverables**

# 1 Background

The UN ORMS policy was approved by the UN Chief Executive Board (CEB) in 2014 and adopted by ITU Council in 2016 (document C16/70).

Council 2017 approved the ITU ORMS project, because up until then the ITU only had security emergency planning in place, but no global Crisis Management or Business Continuity since the creation of the Organization in 1865. The project commenced on 1 November 2017 and finished on 31 December 2019, on time and budget. Two consultants were engaged for the project and they carried out research, conducted interviews (several hundred), visited all ITU field offices, briefed colleagues, managed two Crisis Management desk-top exercises, and delivered over 40 reports. All ITU elected officials, senior staff, Regional and Area office staff, and a significant number of other colleagues, including those of UN Agencies, Funds and Programmes (AFPs) in Geneva and New York, were involved. In addition, senior UN officials and staff of the UN Department of Safety and Security (DSS) were visited in ITU’s 12 field locations to ensure ITU staff were included satisfactorily in the UN Security Management System of those countries.

Council 2017 further approved the creation of a P4 post, as of 2020 onwards, to coordinate and manage the ORMS maintenance, exercising and review tasks; at the time of writing the post is currently in the recruitment stages.

# 2 ITU ORMS Framework

There are seven elements within ORMS, which may be divided into two components: Business Continuity (BC) and Crisis Management (CM).

## 2.1 Business Continuity

Business Continuity (BC) is the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruption.

The Business Continuity Management System (BCMS), drafted within the context of current international standards and best practice, comprises a structured group of policy, plans, guidelines and reports which together enable the realization of business continuity. It is presented in four sections: Preparedness, Development, Implementation, and Review, and is detailed in Annex 1.

## 2.2 Crisis Management

A holistic approach has been established for effective Crisis Management (CM) of all ITU activities globally.

Within the context of the prime responsibility of a host country and the UN Security Management System (UNSMS) including global provision for security CM, ITU now has an organizational capacity and developing capability for CM, whether the critical incident occurs within Headquarters, Regional or Area Offices, or involves several or all locations.

Based upon an organizational framework of accountability for security, a CM structure now exists consisting of policy, guidelines and procedures, and an identified membership for the key roles and responsibilities. It is designed to be flexible and capable for use in any critical incident or emergency, including significant business disruption, which may develop into a crisis.

Indeed, the knowledge learning concerning crisis management and business continuity has been demonstrated on two separate incidents where the ITU Crisis Management Team (CMT) has been activated, the first response was in March 2019 when the CMT was convened operationally in response to the ET-302 air crash tragedy in Ethiopia, which caused the death of two staff members of the Africa Regional Office, and the second in February 2020, in response to the Covid-19 outbreak and subsequent pandemic, which is still ongoing at the time of preparing this document.

The components and details are provided in Annex 2.

## 3. UN / ITU Key Performance Indicators

In addition to approving the UN ORMS policy, the CEB also approved an ORMS “Maintenance, Exercise and Review (ME&R) Regime”, and Key Performance Indicators (KPIs). The ME&R includes training and awareness, decision-making responsibilities, crisis response, communication, business continuity, IT disaster recovery, after-action review, testing, and update and endorsement.

The ME&R Regime has been incorporated into this project, as recommended by Council 2016, which also recommended that ITU adopt the UN ORMS KPIs.

## 4. Business Risk Management

**An adverse impact on ITU’s reputation has been recognized as a significant organizational risk. The consolidation of an effective operational business risk assessment and management process is judged to be a priority**, cognisant of the proposals and guidelines emanating from the CEB Cross-Functional Task Force on Risk Management and recognition by the Advisory Committee on Administrative and Budgetary Questions (ACABQ) of the need to consolidate *“...best practices and experiences in risk management and organizational resilience management…”,* it is recommended that a single risk management mechanism be adopted and adapted to embrace both security and business risk management analysis, judgements and decision-making; It is further recommended that an organizational Business Risk Manager post is created to work closely with the ORMS Coordinator and IT BC/DR Manager, under the supervision of the Head of SSD who has responsibility for Security Risk Management within the Union.

## 5. Data Classification for sensitivity and criticality

There is significant organizational risk from cyber-attack and denial of service, which could impact on data provided to ITU by Member States. The ORMS project has concluded that ITU needs a Data Classification system including the determination of ‘Sensitivity and criticality’, to prevent and mitigate this risk. This accords with, and builds upon, the New Building transitional risk assessment, which identified the need to catalogue and index current Radiocommunication Bureau (BR) hard copy documents, to enable BC - a requirement that Council 2019 has endorsed and funded.

## 6. Review of HR Staff Resilience

The Business Risk Assessment has identified a lack of Organizational Human Resource resilience. In particular, the lack of succession-planning and loss of institutional and technical knowledge through delayed replacement of staff in key functions and roles, is potentially a serious risk to the reputation of ITU.

## 7. Recommendations

The deliverables of the ORMS project have been successfully completed and the project’s finding have resulted in the following recommendations:

1. Adoption of a single risk management mechanism to embrace both security and business risk management analysis, judgements and decision-making;
2. Creation of an organizational Business Risk Manager post, within available budget, to work closely with the ORMS Coordinator and IT BC/DR Manager, under the supervision of the Head of SSD who has responsibility for Security Risk Management within the Union;
3. Creation of a project to define an ITU Data Classification system and apply it to newly received data.

The Council is requested to advise on potential sources of funding for the above-mentioned data classification project.

Annex 1

Business Continuity

Business Continuity (BC) is presented in four sections: Preparedness, Development, Implementation, and Review, as follows:

# Preparedness

#### Business Continuity Policy (BC Policy)

The BC Policy was developed during the ORMS project. The purpose of this policy is to ensure that following a disruption, the organization is capable of delivering prioritized activities at acceptable pre-determined levels. The scope of this policy includes all personnel, locations, and equipment of the organization globally.

**Strategic Business Impact Analysis (SBIA)**

The SBIA undertaken in 2018 resulted in a list of activities prioritized by senior management for recovery in the event of a disruption; and a list of all other key activities which they also prioritized for recovery in the event of a significant disruption.

A Business Impact Analysis was conducted in 2018, and enabling processes and dependencies were established. BC and IT Disaster Recovery (DR) plans were created. The SBIA should be revisited if there are substantial changes to the organization, or after several years have elapsed.

The SBIA is the responsibility of the ORMS Coordinator.

#### Business Risk Assessment (BRA)

The BRA for the organization was initially carried out in 2018 as part of the SBIA. The BRA was reassessed in December 2019. The BRA should be revisited annually, or if there are substantial changes to the organization including a significant disruption. The BRA is the responsibility of the ORMS Coordinator.

#### Business Continuity Plan (BCP)

The BCP is the organizational, strategic, plan for ITU and for all its business components globally. It clarifies roles, responsibilities and structure for planning, decision-making, coordination, communication and information-exchange during a disruption.

The BCP is supported by Activity Recovery Plans (ARPs) which are the detailed operational and technical requirements for recovering prioritized and other key activities which are addressed in the ARPs. There should be a plan for each business unit.

The ARPs are intended as an operational tool, aide-memoires for business managers following disruption, providing key information relating to people, location, and equipment, and continuity solutions to enable an effective response and recovery.

Completion of individual plans will be the responsibility of the business unit BC Focal Points (FP) as determined by senior management. All ARPs will be reviewed annually. The ORMS Coordinator is responsible for the management of ARPs.

# Development

#### Mitigation

There will be a planned programme of examining current working practices relating to the prioritized activities to determine if practical cost-effective measures could be identified to prevent and/or mitigate the impact of disruption. Planning and monitoring the mitigation programme by means of BRA and review, will be the responsibility of the ORMS coordinator working with BC FPs.

#### Resources

The need for additional resources for mitigation measures should be considered annually, and any resources must be clearly identified and justified.

#### Training

The BC Policy will be communicated to all personnel together with appropriate, regular, awareness training. The BCMS should be included in future induction training.

Training is the responsibility of the ORMS Coordinator.

#### Exercise

A regime of BC tabletop exercises ideally conducted annually, will be organized by the ORMS Coordinator working with the IT BC/DR Manager.

# Implementation

* Response and recovery;
* activation and de-activation

The delegated responsible officer will be responsible for activating and de-activating the BCP.

# Review

* Compliance, monitoring, reviewing & audit will be conducted;
* The ORMS Coordinator is responsible for the facilitation of compliance, monitoring and audit, in liaison with IAU;
* Any event which requires an ARP to be activated will be reviewed for lessons learnt and best practice, and changes made to the plans if appropriate. Similarly, any event which requires an IT recovery plan will be reviewed for lessons learnt. The ORMS Coordinator will be responsible for ensuring lessons learnt reviews are conducted, working with the BC/DR Manager if the IT DR plan was involved;
* The BCMS generally and the BCP, in particular, must be reviewed annually;
* IT Disaster Recovery (IT DR) is the ability of the ICT elements of an organization to support its critical business functions to an acceptable level within a predetermined period of time following a disruption;
* The IT DR is part of the BCMS. There is an IT DR Policy which complements the BCP Policy, and an overall IT DR Plan which similarly complements the BCP;
* The IT DR Plan is supported by Business IT Services Recovery Plans (BITSRPs) and by ISD IT Service Recovery Plans (ISDITRPs) which are the detailed technical plans for recovery following a disruption directly impacting on the Business IT applications or the ISD infrastructure/environment respectively;
* BITSRPs and ISDITRPs will be reviewed annually;
* The IT BC/DR Manager is responsible for the management of these technical plans.

Annex 2

Crisis Management

**The organizational CM structure includes:**

* CM Policy;
* Governance accountability;
* Crisis Management Team (CMT) and Operational Response Team (ORT) designation;
* Guidelines and standard operating procedures (SOP);
* Training programme;
* Compliance and after-action review;

CMT ‘table-top’ training exercises were conducted during 2018 and 2019.

The CM structure is designed for ITU-specific crisis, in the knowledge that HQ, Regional or Field offices may be subject to crisis involving other UN Agencies, Funds and Programmes which necessitate additional organizational membership of a duty station CMT.

### Crisis Communication

There are two essential elements of organizational crisis communication:

* The capacity for staff to receive and send critical safety and security information 24/7; and for staff to seek urgent assistance from SSD;
* the organization to have an effective structure for internal and external corporate communication during crisis.

### Staff Crisis Communication

SSD provides operational crisis communication capacity, where necessary in liaison with UNOG DSS; or with UNDSS personnel based at other relevant ITU duty stations, or event locations globally.

ITU has piloted, evaluated and chosen to partner with IOM and adopt the use of the Security Communication And Analysis Network (SCAAN) for all staff serving in Regional and Area Offices including the New York Liaison Office, HQ frequent travellers and any other HQ staff member who chooses to be SCAAN-enabled.

The SCAAN App. provides a 24/7 capacity and capability to meet ITU staff crisis communication requirement.

### Corporate Crisis Communication

In respect of external and internal corporate crisis communication, the Head of Corporate Communications Division (CCD), Strategic Planning and Management Department (SPM) is a key member of the CMT and instrumental in the provision of timely guidance of crisis communication for members of the CMT, based upon current UNSMS and UN Department of Public Information’s UN Communications Group (UNCG) crisis communication best practice .

Crisis Communication Standard Operating Procedures (SOP) for CMT members have been drafted for incorporation within the CM policy and guidelines.

### Security Support & Response

The ITU Safety and Security Division (SSD), including the out-sourced uniformed guard company Protectas, provides this capacity at HQ, when necessary in liaison with Geneva Police and UN DSS/SSS.

Within ITU region and area office duty stations, and for global or regional ITU Events, the Head of SSD provides the capacity for security advice and guidance, including risk assessments, and can liaise with or facilitate security support from host country emergency authorities and local UNDSS.

### Mass Casualty Incident Response

In the event of a crisis involving mass casualties within HQ, the prime ITU para-medic triage response will be coordinated by the Head of SSD, together with the Medical Advisor and Nurse of the Medical Service (MS), and the Staff Counsellor, if all are on duty at the time of the critical incident.

In addition, it is likely that the Canton of Geneva emergency services including Ambulance, Police and Fire specialists will attend and enter ITU premises by delegated consent. The UNOG Mass Casualty Incident Guide has been used by the Medical Advisor of MS in liaison with the Canton Health authorities to draft similar ITU-specific guidelines.

Within regional and area office duty stations, or duty stations where ITU international or regional events are taking place, the respective Host Country Agreements and UN Area Security Plans, and Event Safety and Security Plans, contain similar response provisions for ITU staff, delegates and visitors;

### Crisis Management – Support to Staff, Survivors and their families

It is inevitable that during a crisis, staff, survivors, and families, and members of the CMT will experience stress beyond their norm and may in consequence require specialist support both during and after the crisis is resolved.

A Staff Counsellor who is available to provide/coordinate the required initial, mid- and long-term post crisis support to staff, survivors and their families at HQ and within field offices. The Staff Counsellor has access to a network that is managed by the UNDSS Critical Incident Stress Management Unit (CISMU).