IT Security
IT Security

Business Continuity (BC)

Disaster Recovery (DR)

Cybersecurity

Identity Management & Access Control
**IT Security**

**Business Continuity (BC)**

**Actions taken:**
- Review of IT related critical processes
- Business Continuity Plan (BCP)
- Measures to address major risks
- Alerts for staff and delegations – emergency management software installed

**Actions planned:**
- Further operationalization of BCP
- Include field offices and institutes in BCP
- Improve remote access to corporate resources
- Tool to update emergency information of staff
**IT Security**

**Disaster Recovery (DR)**

**Actions taken:**
- Disaster Recovery Plan based on BCP and review of IT-related critical business processes
- Assessment by UNICC

**Actions planned:**
- Select solution for secondary data centre
- Review backup solution in Miollis/Bonvin
- Detail DRP, including regular tests of failover scenarios
Secondary Data Centre

Top priority, included in the Invest for Efficient Delivery Programme

Disaster Recovery (DR)

Options for Secondary Data Centre:
• Local
• Distant – UNICC (Geneva)
• Cloud

IT Security
Actions taken:
• IT security guidelines and policies
• IT security training materials
• Regular user alerts
• Technical control measures
• Investment in hardware & software

Actions planned:
• Security guidelines and policies for fields units
• Increase reliability of UNESCO websites
• Secure Data Management Tools
• External security tests
• Improve user awareness/culture
• Review/implement audit recommendations
User behaviour - a key factor of IT security

No protection can be fully effective unless users respect basic security principles:

• Do not open attachments from unsolicited emails. Unexpected email from unknown sender = RISK!

• Beware of emails asking for personal data, passwords or other sensitive data. Never provide such data to anyone.

• Report suspicious behaviour to Helpdesk.

• Always use strong passwords and never common words.

• Never share your password...

IT Security
Actions taken:
• New Identity Management solution identified, purchased and under implementation
• Smart cards introduced for printing

Actions planned:
• Extend use of smart cards to access sensitive areas
• Review current security ID management and integrate with new Identity Management solution
• Extend use of smart cards to networks and systems
Same badge to assure physical and logical access – entrance, sensitive areas, computers and printers