Phone +41 31 327 17 17
Fax +41 31 327 17 38
www.bdo.ch

BDO SA
Hodlerstrasse 5
3001 Berne

To the Council of Administration of the

UNIVERSAL POSTAL UNION - UPU

Bern

Internal audit report 04.2020
Annual internal audit activity reporting 2020

15 September 2020
2122'0573/1-2
HIM/BIT

Report number	04.2020
Audit period	2020 (January - September)
Draft report distribution	14 September 2020
Date of the report	15 September 2020
Distribution of the report	Director general Internal Audit Committee General Management External auditor

Table of contents

1 ANNUAL ACTIVITY REPORT

Internal audit function

The internal audit charter establishes that "the internal auditor writes an annual report, with view to be presented, in its entirety, at the next Council of administration meeting, together with the appropriate observations from the Director General".

Handover of the internal audit mandate

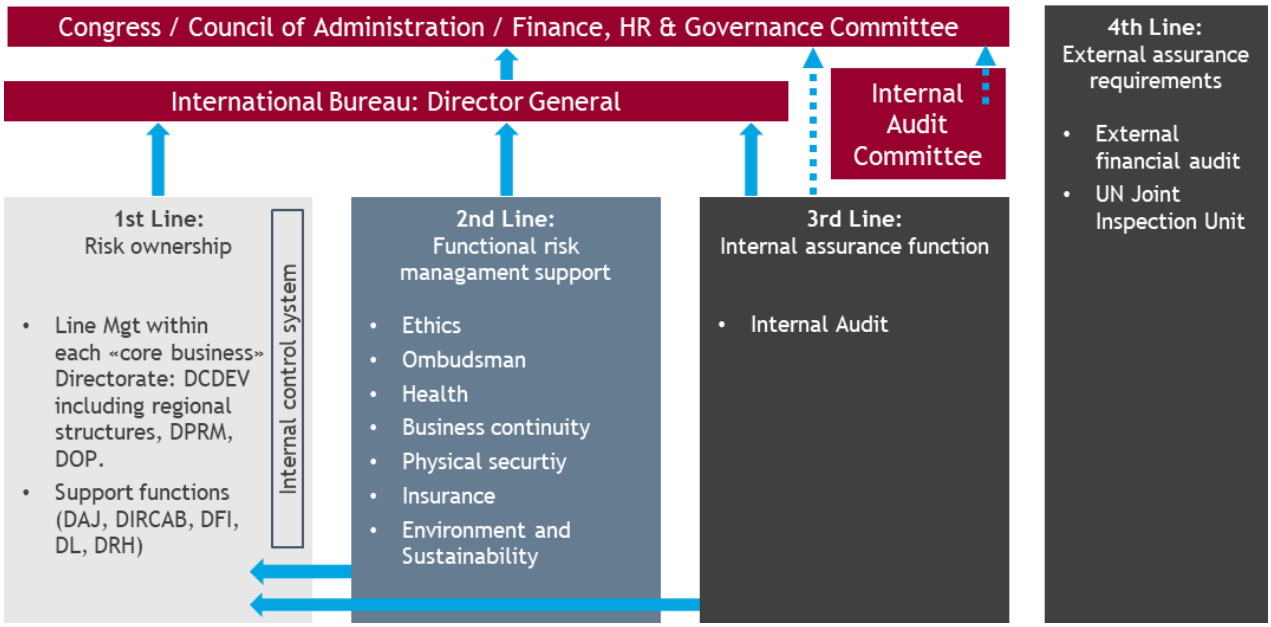
Following a "UPU internal audit" tender, BDO was selected by the Tender and Procurement Committee to take over the internal audit function for six years 2018 - 2023.

In order to confirm our understanding of the environment of the UPU in its various business segments, BDO gained knowledge on the basis of actual documentation of the organisation. Moreover, meetings with the external auditor, le contrôle fédéral des finances, were conducted to obtain a better understanding of the institution. On this basis, a risk assessment, an audit planning for the year 2018 and a rotation plan for the years 2018 - 2023 were established. In consultation with UPU, the audit plan was adjusted due to the corona pandemic. This means that the audit of "The Business Continuity Management" will be carried out in 2020 instead of 2021. In turn, the audit of the "Organisation of the international bureau" will be postponed from 2020 to 2021.

Internal audit as part of the wider UPU risk management framework

The above-mentioned charter states that, "internal auditing is defined, at UPU, as an independent function bringing to the Director General and, through him, to the Governing Bodies, the assurance that the organisation is managed in an efficient manner".

Internal audit forms part of the wider risk management framework that is based on the concept of the "lines of defence". The UPU framework is outlined below:



Risk assessment & audit planning 2020

According to the IIA norms, the internal audit evaluates the risk of the organisation at the planning stage. The risk assessment and the audit planning were elaborated on the basis of the strategy 2017-2020 presented at the congress in Istanbul in 2016, the existing risk assessment from 2017, the knowledge gained through the handover process and eventual specific expectations from the International Bureau.

The 2020 audit planning was approved by the Director General.

2 INTERNAL AUDIT 2020 - MAIN OBSERVATIONS

For the year 2020, we have issued four audit reports, three as scheduled in the audit plan, one concerning the audit tracking and one further audit will occur during the 4th quarter of 2020.

For each of those assignments, a planning memorandum was issued, the main objectives of those assignments were:

- Review the coverage of the identified risks;
- Review the organisation of the area audited;
- Identify and discuss management's actions and responses to the risk drivers;
- Identify areas of potential further improvement in Management's actions and responses.

All the recommendations issued in our reports were presented to the General Management in order to obtain their comments. The General Management has accepted our recommendations.

All the internal audit reports were presented to the Internal Audit Committee.

The conclusions of those audits were not designed to underline those well-functioning elements in the internal control system, but rather to draw Management's attention to relative weaknesses if any.

The findings and recommendations stemming from the internal audits performed have been discussed with the management teams concerned. Those teams share the conclusions and have established action plans with a view to strengthening Management's responses to the risk drivers.

Internal audit report 06.2019 - Communication of the IB

The aim of this audit was to assess the organisation and the internal controls related to the internal communication at the IB. We evaluated / reviewed the following processes / areas:

- Communication Channel
- Communication from staff members

Our main observations are the following:

1. *Rethink and simplify the approbation and publications process*

   The approbation process for an internal memorandum can take up to 5 days. In some cases this does not allow employees to be informed in a timely manner.

   We recommend rethinking and simplifying the approbation process in order to be able to react more quickly in the event of a crisis. This would also ensure that the daily-communication arrives on time.

   An internal memorandum has been published on the International Bureau intranet and addresses time limits for approval and publication of internal memoranda. The time limit is five days for an internal memoranda of a non-urgent nature and three days for an internal memoranda of an urgent nature.

2. *Changes in the Administrative Instructions*

Changes made in administrative instructions are not systematically communicated to staff members.

We recommend to systematically communicate all modifications.

3. *Written record of the Town Hall Meetings*

There are no documents produced after a Town Hall meeting. If staff members were on a mission or could not be present, there is no summary of the given information.

We recommend to protocol the Town Hall Meetings in order to provide to all staff members the important information.

In the future there will always be a summary of the items discussed, so that absent members can also be informed about the meeting. The summary of the Town Hall meeting on 19 December 2019 was sent to BDO.

Internal audit report 02.2020 - Communication with member countries

The aim of this audit is to assess the organisation and the internal controls related to the communication with member countries.

We evaluated / reviewed the following processes / areas:

- Communication in relation with the preparation of the Congress
- Voting System
- Impact of the CoVid19 on the 27th Congress

Our main observations are the following:

4. *Extend the deadline for submitting a proposal*

The member countries were informed that the deadline of 10 of June should be respected even though an extension may be considered.

We recommend you to extend the deadline of 10 of June for the member countries to submit their proposal and allow them to make amendment to the already submitted topics.

5. *Clarify the actual situation in the General Rules of the UPU*

The General Rules of the UPU do not comprise regulations on who is responsible and what happens if a Congress cannot take place in case of force majeure.

We recommend you to clarify in the General Regulations what happens in the case a Congress cannot take place worldwide and has to be postponed. Currently, only a geographic dislocation is regulated as the authority can be given, under certain circumstances, to the CA. We also recommend you to clarify the impacts of the postponement with the external auditor.

Internal audit report 03.2020 - Cyber Security

The aim of this audit is to assess employee awareness and IT behaviour in the event of a phishing attack, and to evaluate existing internal processes with regard to cyber security incidents.

We assessed employee behaviour based on the responses to a phishing email we created and distributed. The assessment was divided into the following 3 main phases:

- Creation of the phishing Email
- Verification of functionality
- Execution of Phishing attack

Our main observations are the following:

6. *Promote and train existing processes in the IT Department more strongly*

   At 9:23 a.m. and 9:24 a.m. three participants (member of the IT staff) sent e-mail alerts to all IB employees. Those e-mails were sent independently from each other. The reaction seems uncoordinated, as two e-mails were sent one minute apart from each other and with different style and wording. Such reaction is generally as likely to further confuse employees as it is to help them.

   One alert included the forwarded phishing message with a fully functional phishing link.

   We recommend that the process described in document IS-DOC-A16-021-InfoSec Incident Management Procedure is trained internally and, if necessary, extended with a process specialized for phishing or hacking attacks. At the same time, IT staff as well as all other employees should be clearly trained which department, team or point of contact should be informing about such attacks and to which department, team or point of contact such attacks should be reported.

   If an alert message is sent to all the employees we recommend sending a screenshot of the phishing message attached to the warning instead of forwarding the message itself. It should tell you what to do if you have already clicked on the link and what the IT department will do to calm the situation down.

   In addition to these procedural recommendations, IT can also make technical interventions that can prevent the further spread of such an attack after it has been detected. We recommend to immediately block all systems involved in a phishing incident (e-mail sender, IP address, domains of embedded links, etc.) in case of an emergency in order to prevent sensitive data from being transmitted to attackers.

7. *Cyber Security Awareness Training for all employees*

   10% of all employees have submitted data.

   We recommend information on the intranet and training for all employees to increase awareness, this should be done at regular intervals.

8. *More Phishing Assessment in the Future*

   5% of all already trained employees have nevertheless transmitted data. This is worth more than 10% of all employees. So the positive effect of an awareness campaign can be recognized.

   We recommend after an awareness training of all employees and the training of the IT department in dealing with the right processes to start another phishing campaign to make the success visible.

9. *Responsible teams should know processes*

   We realized that not all the responsible teams concerned with the documents related to the policies for the ISO27001 certification are completely trained. Further the information are not yet shared with all employees.

We recommend the training of the responsible teams with the documents ref. 1 and also the sharing of information with all employees in order to increase the knowledge and awareness of the largest possible factor.

10. *Updating existent documentation*

    The document Administrative Instruction (PER) No. 23/Rev 4 from May 2009 does not completely reflect the current situation. Especially there are still no information regarding contact points.

    We recommend, updating and supplementing the document with the necessary contact points.

Internal audit report 05.2020 - Follow up of recommendations

As per good practices, a specific audit focused on the follow up on the recommendations put forward by internal audit over the period 2011-2019. This review evidence a completion of 12 recommendations out of 23 open in March 2019, 1 was closed whereas the remaining 10 are in progress.

3 FINAL REMARK

Following the decision by the Finance and Administrative Commission of the Council of Administration in November 2014, member countries can request access to Internal Audit reports to the International Bureau, as per the terms of circular 61 sent to member countries on 11 May 2015.

Through the following statements, we confirm that we comply and have complied during the period with the independence requirements. We confirm that we received full support and cooperation from the persons involved in our audit and we would like to thank them.

Berne, 15 September 2020

BDO SA

Matthias Hildebrandt
Partner, Swiss CPA

Thomas Bigler
Senior Manager, Swiss CPA
Auditor in Charge