Questions and Answers (Q&A)

in relation to the Request for Proposal – Audit of the OSCE's ISMS

19 October 2017

Question no. 1

What is the size of the ISMS in terms of documents and pages (policies and standards/ procedures/ registrations).

Answer no. 1

The OSCE does not have an ISMS per se, but a policy on Information Security (around 6 pages) with some annexes to that document (on User Security, User Access and Authorization, System Operations, Software Development, totalling 16 pages). This needs to be reviewed in conjunction with the following documents: the policy on OSCE Computing Resources (10 pages); the policy document on Records Management (15 pages); the Archives and Records Management Manual (25 pages).

Question no. 2

Are there concrete reference tables available that show the relationship between the ISO27001 114 controls / 14 groups and the ISMS?

No, the OSCE does not have concrete reference tables available that show the relationship between the ISO27001 114 controls / 14 groups and the ISMS.

Answer no. 2

No, the OSCE does not have concrete reference tables available that show the relationship between the ISO27001 114 controls / 14 groups and the ISMS.

Question no. 3

How many locations are there (3 institutions and 16 operational units? Are support tasks centralised or decentralised (HR/ procurement/ finance etc). Can you provide us with a organogram with number of people involved and a description of activities per unit (in order to make an estimation of the number of audits per location/ unit per location.

Answer no. 3

The file attached includes an organigram with the different Executive Structures of the OSCE together with their regular budget (Unified Budget) and the number of approved posts. The activities of each of the Executive Structures can be seen under the following link: http://www.osce.org/where-we-are

With regard to support tasks, this are handled – in general – in a decentralized manner. Each Executive Structure has a Fund Administration Unit or a Department of Administration and Finance with, inter alia, dedicated Procurement, HR, Finance functions. Depending on *the size of the Executive Structure, these departments or units may also include dedicated material / asset management and treasury roles and to some extent dedicated IT support staff. However, it should be noted that certain functions / transactions are executed centrally from the Secretariat (e.g. procurement transactions exceeding certain amounts; determined steps in the payroll process; etc.)*

Question no. 4

We have developed an app that we can use for measuring the level of awareness. Are we allowed to use that within the entire organisation (for that all email addresses have to be provided to us). It requires remote access.

Answer no. 4

In principle, OSCE policies prevent the installation of third-party software / applications onto our network. Provision of email addresses and remote access may need to be further discussed.

Question no. 5

In Annex C – Terms of Reference it is stated in section 2 b) that the "analysis will include OSCE Secretariat in Vienna, Austria, as well as a sample of other executive structures [...] it is expected that three/four locations outside Vienna will be visited.."

Could you please specify how the additional locations outside will be selected, e.g. which criteria are basis of decision to audit a location?

As the OSCE has 57 member states it would be helpful to have a clearer picture of the focus of the audit.

Answer no. 5

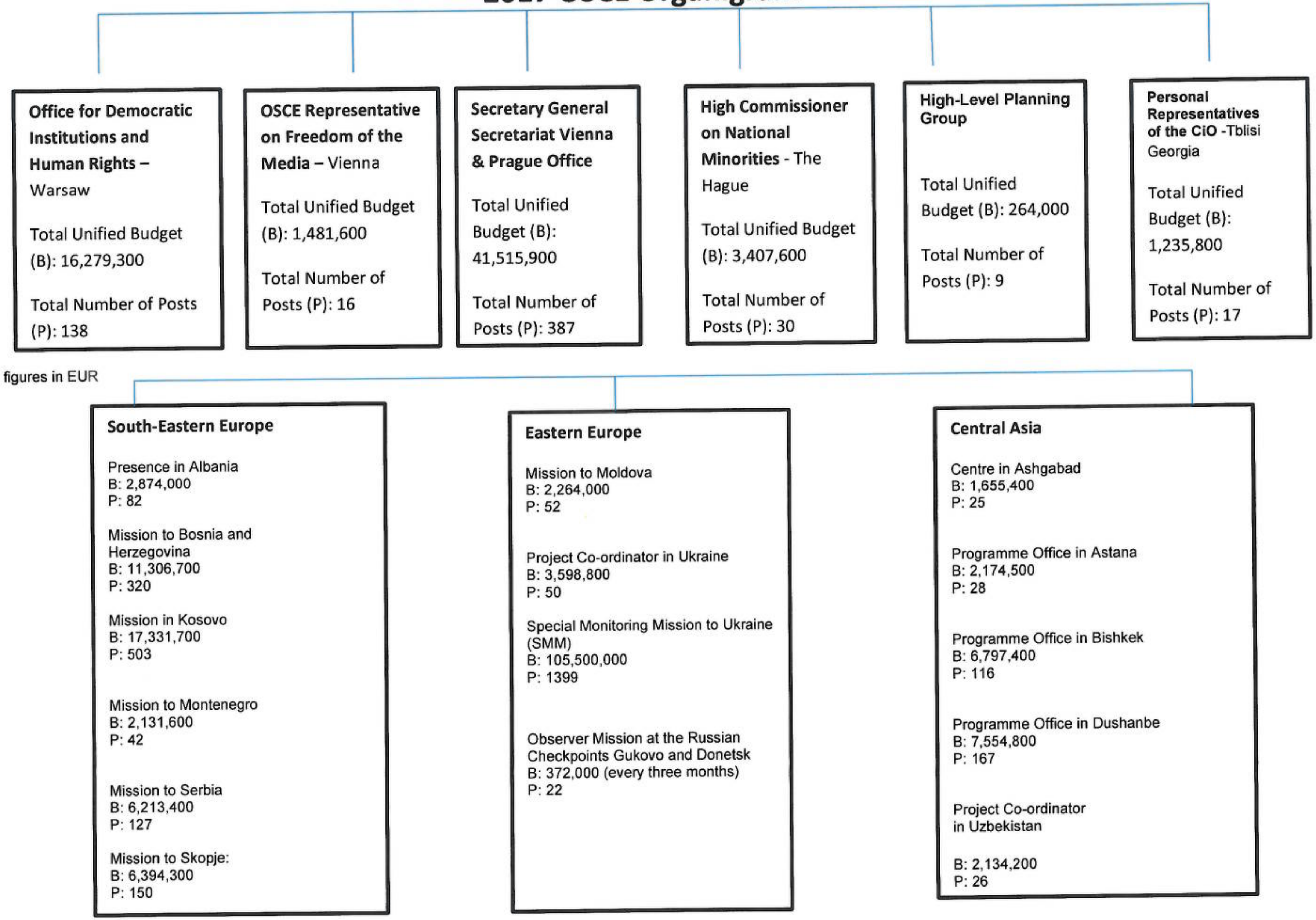
Selection of locations outside Vienna will be done by OIO in conjunction with the successful bidder during Phase I of the assignment when developing the detailed audit plan and programme. A 'high-level' risk assessment of the 16 executive structures of the OSCE will be conducted using criteria such as: complexity of the operations; sensitivity of information assets; budget size; perceived maturity level of their Information Security system and practices.

* * *

Deadline for the tender clarification questions: 20 October 2017, 14:00HRS CET

END.

2017 OSCE Organigram



Office for Democratic Institutions and Human Rights – Warsaw

Total Unified Budget (B): 16,279,300

Total Number of Posts (P): 138

OSCE Representative on Freedom of the Media – Vienna

Total Unified Budget (B): 1,481,600

Total Number of Posts (P): 16

Secretary General Secretariat Vienna & Prague Office

Total Unified Budget (B): 41,515,900

Total Number of Posts (P): 387

High Commissioner on National Minorities - The Hague

Total Unified Budget (B): 3,407,600

Total Number of Posts (P): 30

High-Level Planning Group

Total Unified Budget (B): 264,000

Total Number of Posts (P): 9

Personal Representatives of the CiO -Tblisi Georgia

Total Unified Budget (B): 1,235,800

Total Number of Posts (P): 17

*all Budget figures in EUR

South-Eastern Europe

Presence in Albania
B: 2,874,000
P: 82

Mission to Bosnia and Herzegovina
B: 11,306,700
P: 320

Mission in Kosovo
B: 17,331,700
P: 503

Mission to Montenegro
B: 2,131,600
P: 42

Mission to Serbia
B: 6,213,400
P: 127

Mission to Skopje:
B: 6,394,300
P: 150

Eastern Europe

Mission to Moldova
B: 2,264,000
P: 52

Project Co-ordinator in Ukraine
B: 3,598,800
P: 50

Special Monitoring Mission to Ukraine (SMM)
B: 105,500,000
P: 1399

Observer Mission at the Russian Checkpoints Gukovo and Donetsk
B: 372,000 (every three months)
P: 22

Central Asia

Centre in Ashgabad
B: 1,655,400
P: 25

Programme Office in Astana
B: 2,174,500
P: 28

Programme Office in Bishkek
B: 6,797,400
P: 116

Programme Office in Dushanbe
B: 7,554,800
P: 167

Project Co-ordinator in Uzbekistan

B: 2,134,200
P: 26