Handling Legal Gaps While Practicing Financial Oversight in the Security Sector

DCAF
a centre for security, development and the rule of law

Tool 6

Tool 6
Handling Legal Gaps While Practicing Financial Oversight in the Security Sector

Domenico Polloni

DCAF
a centre for security, development and the rule of law

About DCAF

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) promotes good governance and reform of the security sector. The Centre conducts research on good practices, encourages the development of appropriate norms at the national and international levels, makes policy recommendations and provides in-country advice and assistance programmes. DCAF's partners include governments, parliaments, civil society, international organisations and the core security and justice providers such as police, judiciary, intelligence agencies, border security services and the military.

Publisher

Geneva Centre for the Democratic Control of Armed Forces (DCAF)
Chemin Eugène-Rigot 2E
1202 Geneva
Switzerland

Tel: +41 (0) 22 730 9400
Fax:+41 (0) 22 730 9405

www.dcaf.ch

Disclaimer

This publication has been produced with the assistance of the European Union. The contents of this publication are the sole responsibility of the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and can in no way be taken to reflect the views of the European Union**.**

Author

Domenico Polloni

Editing and Proofreading

Intisar Abu Khalaf
John McAndrew

Design and Layout

Wael Dwaik

Cover picture: © Zoltan Venczel, 2014

ISBN: 978-92-9222-355-7

Table of Contents

Acknowledgements

DCAF would also like to gratefully acknowledge the assistance of partner organisations in the occupied Palestinian territory. These are:

- Mr Jaffal Jaffal, Expert at the State Audit and Administrative Control Bureau
- State Audit and Administrative Control Bureau
- Palestinian Legislative Council
- Office of the President
- Council of Ministers
- Ministry of Finance
- Ministry of Interior
- Central Military Financial Administration
- Palestinian Anti-Corruption Commission
- Palestinian National Security Forces

Introduction

Why is financial oversight in the security sector important?

Financial oversight in the security sector is a key instrument for ensuring that public funds allocated by the state for the security of the people are spent in a transparent and accountable manner.

However, the financial management of security sector institutions is often characterised by opacity rather than transparency. Even in established democracies, the budgets and financial operations of law-enforcement, military and intelligence organisations are often concealed from public scrutiny and sometimes even from formal external oversight by parliament or audit institutions. Furthermore, in many developing countries, disproportionate security expenditures prevent the use of public funds for socio-economic development.

Why this Toolkit?

Building the conceptual and technical capacities of specialised practitioners is a crucial step towards strengthening financial oversight in the security sector. This Toolkit is designed for financial oversight practitioners who wish to:

- Gain access to best international practice in financial oversight of the security sector
- Improve their professional ability to financially oversee security sector institutions
- Acquire a more proactive attitude toward conducting thorough financial oversight activities of security sector institutions
- Assert their authority in scrutinising budgets and financial operations conducted by security sector institutions.

How was this Toolkit developed?

The exercises and training material included in this Toolkit were developed in the framework of the Geneva Centre for the Democratic Control of Armed Forces (DCAF)'s work in the occupied Palestinian territory in 2013-2014 to promote strengthening of financial oversight in the security sector. In 2013, DCAF facilitated a training needs assessment of financial oversight practitioners, followed by a training course in 2014 for employees from key financial oversight institutions in the occupied Palestinian Territory. DCAF developed this training material in cooperation with international experts and with the financial support of the European Union.

The tools that are part of this training manual contain a generic component to be used in virtually any country where financial oversight practitioners in the security sector require capacity building. The tools also contain a locally adapted component, which offers examples from the Palestinian training course and suggestions for how to adapt activities and materials to suit the trainer's own context.

Other DCAF publications on financial oversight in the security sector

In addition to this Toolkit, DCAF has published other reference material on financial oversight in the security sector. These publications include:

1. Guidebook: Strengthening Financial Oversight in the Security Sector, 2012.
2. A Palestinian Legal Collection: Financial and Administrative Oversight in the Security Sector, 2013.
3. Financial Oversight in the Security Sector: A Compilation of International Standards, 2015.

To download these or other publications please visit: www.dcaf.ch/publications

Using the Training Toolkit

Overview

The training toolkit has been designed to be used as a whole training course, which covers six different topics relevant to financial oversight and security sector governance. The six topics may also be used individually as 'stand-alone' training sessions.

What does the Toolkit include?

The training Toolkit includes one introductory tool (Tool 1) and six training tools on financial oversight in the security sector. Each tool has a three-hour generic component. The generic material is internationally applicable and can be used without adaptation in any training context. In addition, there are suggestions and example activities for further localised material. This material is designed to be adapted by the trainer to engage with local issues specific to the trainer's own context. It is envisaged that the localised session would take two hours, but the session can be as long as the trainer deems necessary.

The toolkit contains the following seven tools (including this one):

Tool 1. Using the Toolkit and Acquiring Trainings Skills

Tool 2. Concepts and Main Actors of Financial Oversight in the Security Sector

Tool 3. Medium-term Strategic Financial Planning for Security Sector Institutions: Tools and Techniques

Tool 4. The Budget Cycle and the Security Sector

Tool 5. Building Integrity of Security and Defence Institutions and the Audit Function

Tool 6. Handling Legal Gaps while Practicing Financial Oversight in the Security Sector

Tool 7. Financial Oversight of Intelligence Agencies

These tools may be used for individual training workshops on each topic or as a comprehensive training course.

The toolkit user

The training sessions in the Toolkit are intended to be read and used by trainers with expertise in financial oversight and security sector governance and reform.

The target audience

The target audience for the training course outlined in the Toolkit is mainly practitioners involved in financial oversight of public institutions, including security sector organisations. These practitioners include specifically, but not exclusively:

- Parliamentarians and their staffers who are involved in financial oversight and budget control activities
- Members of Supreme Audit Institutions (SAIs) who provide expertise and support in financial oversight activities
- Strategic-level members of security and defence institutions in charge of preparing and executing budgets
- Representatives of executive authorities, including ministries who oversee the preparation and execution of security and defence budgets
- Officers and auditors working in core security and justice institutions whose role is to perform internal controls and audits.

The ideal number of participants for the course is around 15 participants. However, the course may be used with more participants.

Using the toolkit in the trainer's own context

As mentioned above, the tools in this toolkit consist of generic training sessions and locally adapted training sessions. The generic training sessions included in the toolkit have been developed to be used in any context. However, if possible, the trainer should conduct some form of needs assessment in his/her own context. Based on the results of the analysis, the trainer can understand which training sessions to use, which to prioritise, and which to adapt. The localised training sessions also give examples and offer suggested objectives for use in the trainer's own context.

When choosing which of the sessions in the toolkit to use, the trainer can choose to use only part of a session or to rearrange the order of the activities if desired. However, the trainer should be aware that some of the activities in a session follow each other, and one activity may often build on a previous activity.

The structure of a generic training session

A generic training session consists of the following six elements:

1. **The introduction** lists the learning objectives and focus questions for the session. It also gives an overview, which lists the handouts and trainer resources that are used in the session.
2. **The session plan** gives a full overview of the training session. It is a guide for the trainer to get a quick understanding of the session. It is also used as a quick reference to help the trainer to keep track of activities and of timing during the training.
3. **The description of activities** explains in more detail how to carry out the activities listed in the session plan individually.
4. **The handouts** are given to the participants during the activities in the sessions. They are easily photocopied and can include:
    - Worksheets with tasks for the participants to complete
    - Hardcopies of PowerPoint presentations
    - Summaries of key information
    - Extracts of, or references to, publications
5. **The trainer resources** provide supporting information for the trainer. They can include:
    - Summaries of international best practices
    - Answer sheets

(There are no trainer resources supplied for this Tool's generic training session as the handouts contain the necessary information.)

6. **The suggested resources** contain references relevant to the activities.

Types of activities

The types of activities in the sessions are designed to involve and engage the participants. The participants are expected to build their own understanding of the concepts and issues presented. Often this means encouraging participants to work and provide feedback in groups rather than 'teaching' them topics in a non-participative way.

Trainers might nevertheless be advised to make PowerPoint presentations. The training tools do include handouts with PowerPoint presentations, which may be adapted by the trainer as required. However, the trainers are encouraged to use a minimum number of slides. It is also recommended that they use images or other types of documents that are likely to trigger participants' attention and active participation. The trainer may provide the participants with a hardcopy of the presentation before or after it is shown. The trainer may also ask the participants to discuss a question in pairs before asking for feedback.

The structure of a local training session

A local training session contains example materials and objectives for the local sessions to cover. It is given as an example for the trainer to draw on in his or her own context when devising his or her own localised sessions and materials.

The structure of a local training session is similar to that of the generic training session (see above). Suggested example activities are given instead of a full session plan. A local training session consists of the following five elements:

1. **Introduction:** This consists of learning objectives and focus questions that are relevant to the trainer's own context. An overview of handouts and trainer resources is also given.

2. **Example activities:** These are example activities of the suggested content to be covered. This content can be adapted by the trainer to fit his or her own context. It includes a description of the activity, timing, and.

3. **Example handouts:** The handouts are given to the participants during the activities in the sessions. They are easily photocopied.

4. **Example trainer resources:** These provide supporting information for the trainer.

5. **Suggested resources:** The suggested resources are references for the trainer to use when adapting these example activities.

Handling legal gaps while practicing financial oversight in the security sector: the training session

Introduction

Learning objectives

This session aims to give participants a working knowledge of the legal framework of the security sector and how to deal with areas that are not covered by specific legislation or if covered not sufficiently detailed when practicing financial oversight. The session allows participants to understand their role in addressing such legal gaps in their own financial oversight work in the security sector. The specific learning objectives include:

- Understanding the concept of 'right to access information' and recognising common exceptions to this right
- Becoming aware of the challenge of finding the right balance between full access to information through a freedom of information law and secrecy requirements related to national security matters
- Sharing experiences on how gaps in the existing national legislation can be practically addressed or overcome
- Getting introduced to the frameworks of various countries with regards to parliamentary oversight of the security sector
- Sharing experiences of field practices and developing solutions to be applied in the participants' work practices.

Focus questions

The following questions are addressed through the activities in this session:

- What is the concept of 'right to access information'?
- How can needs for access to information be balanced with national security, and what is the role of the freedom of information law?
- What are different countries' approaches to parliamentary oversight of the security sector?
- How can gaps in existing national legislation be overcome, and how can solutions be applied in participants' workplaces?

Overview

Session Plan *Handling legal gaps while practicing financial oversight in the security sector*

Description of Activities

Handout 6.1 *PowerPoint Presentation Hardcopy: Handling legal gaps while practicing financial oversight in the security sector*

Handouts 6.2 and 6.3 *Two successive versions of South Africa's Protection of Information Bill (2010 and 2013)*

Handout 6.4 *Excerpts from the Italian Code of Public Procurement*

Handouts 6.5 and 6.6 *Two Financial Times articles on a public parliamentary hearing of the United Kingdom's intelligence agencies*

Handout 6.7 *Excerpt of the 2012-2013 report of the Intelligence and Security Committee of the British Parliament*

Session plan

Handling legal gaps while practicing financial oversight in the security sector					
Learning objectives	Participants will be able to: 1. Understand the concept of the right to access information and the common restrictions of this right 2. Become aware of the importance of finding a balance between full access to information/ full transparency and secrecy/ confidentiality requirements related to national security 3. Gather ideas of how to address gaps in the existing national legislation (for example, absence of an access to information law) 4. Learn from other countries' experiences about how Parliament can handle legal gaps when practicing financial oversight in the security sector 5. Share experiences of field practices and develop solutions to be applied in the participants' contexts				
Content to be covered	• Public right to information • Oversight role of Parliament with regards to the work of security sector agencies • Transparency of security and defence budgets and the confidentiality requirements • Some exceptions to normal rules • Urgency requirements of financial operations related to security and defence • 'Whistleblower' protection • Codes of conduct, values, behaviour				
Time	180 minutes				
Activity	**Time**	**Description of activity**	**Grouping and materials**	**Session objectives**	**Comments**
1.	5 min	*Introduction*	Trainer to whole group	–	The trainer briefly introduces the learning objectives of the session.
2.	20 min	*PowerPoint Presentation: Introduction to Handling legal gaps while practicing financial oversight in the security sector (slides 1 to 6)*	Whole group discussion *Handout 6.1: PowerPoint Presentation Hardcopy: Handling legal gaps while practicing financial oversight in the security sector*	Objs.1,2,3 and 4	The trainer introduces the concept of right of access to information and its importance for practitioners (Handout 6.1 slides 2 to 4). The trainer discusses the value of having a robust legal framework that allows for a sound budgetary oversight of security agencies and presents practical steps to conduct procurement oversight (Handout 6.1 slide 5). The trainer also presents the role of the Parliament in practising oversight of security and defence institutions (Handout 6.1 slide 6).

Activity	Time	Description of activity	Grouping and materials	Session objectives	Comments
3.	40 min	Worksheet and discussion: Handling legal gaps in the definition of secrecy and protection of information	Whole group discussion Highlights of the discussion on a flipchart sheet *Handouts 6.2 and 6.3: Two successive versions of South Africa's Protection of Information Bill (2010 and 2013)*	Objs. 1,2,3, 4 and 5	The trainer moderates a discussion on how to handle legal gaps in the definition of secrecy and protection of information. This activity is based on a practical example from South Africa. The trainer distributes **Handout 6.2** and **Handout 6.3** for the debate. The activity focuses on the definition and scope of 'sensitive' information in two successive drafts of the South African Protection of Information Bill. The trainer introduces the history of this bill and then asks the participants to read and compare the two texts with the following four guiding questions in mind:. • Does the draft enshrine a general right of access to state information (art. 6 in the first draft, art. 4 in the second)? • If it does, what are the general exceptions to the right of access (art. 6 in the first draft, art. 4 in the second)? • What is the rationale that allows state information to be classified (arts. 11 and 12 in the first draft, art. 8 in the second draft)? • Specifically, what are the criteria to decide whether state information must be classified (arts. 11 and 12 in the first draft, art. 8 in the second draft)? The participants discuss how confidential information/ state information is defined in their contexts and discuss what lessons can be learned from the South African example. The participants write down in a flipchart sheet their conclusions.
4.	35 min	Worksheet and discussion: Handling legal gaps in the exceptions to normal financial oversight rules due to secrecy requirements	Whole group discussion Highlights of the discussion on a flipchart sheet *Handout 6.4: Excerpts from the Italian code of public procurement*	Objs. 2,4 and 5	The trainer moderates a discussion on handling legal gaps in the exceptions to normal financial oversight rules due to secrecy requirements. This activity is based on an example from Italy and follows the same format as Activity 3. The debate focuses on the strict limits to the use of exceptional financial procedures due to special security requirements. The trainer asks the participants to read the excerpt of the Italian code of public procurement (**Handout 6.4)** and analyse the text with the following guiding questions in mind: • Exactly which contracts are exempted from the usual procurement rules in this Italian legislation? Does such an exception apply systematically? • Who decides which procurement contracts are concerned by special security requirements? • Is a procurement contract under special security requirements always a sole source procurement contract? • Are all firms allowed to work as suppliers for contracts under special security requirements? • Are procurement contracts under special security requirements no longer subject to audit? • How does the Italian Parliament oversee public procurement under special security requirements? The participants reflect on how their contexts look like and compare it with the Italian example. The participants write down in a flipchart sheet their conclusions.

Activity	Time	Description of activity	Grouping and materials	Session objectives	Comments
5	75 min	*Worksheet and discussion: Handling legal gaps in the balance between access to information and secrecy requirements related to national security*	Whole group discussion Highlights of the discussion on a flipchart sheet ***Handouts 6.5 and 6.6:*** *Two Financial Times articles on a public Parliamentary hearing of the United Kingdom's intelligence agencies* ***Handout 6.7:*** *Excerpt of the 2012-2013 report of the Intelligence and Security Committee of the British Parliament*	Objectives 1, 2, 4 and 5	The trainer moderates a discussion on transparency and secrecy requirements related to national security, taking as an example the relations of security agencies with Parliament. The activity follows the same format as activities 3 and 4 but with two parts. The first part makes use of two newspaper articles about the situation in the United Kingdom to focus the discussion on the role of the Parliament while practising financial oversight in the security agencies and access to information of the public. The trainer distributes the two Financial Times articles (**Handout 6.5** and **Handout 6.6)** and proposes the following guiding questions: • Who is responsible in the UK Parliament for security sector oversight? • What do the articles say about the current powers of the UK Parliament in relation to intelligence agencies, and possible future reforms? • What used to be made public of the functioning of intelligence agencies, and what has become public of late? As a result of what has there been more openness? • Does the UK intelligence ever provide evidence to Parliament, and if so in what form? • What did the UK Parliament want to know from intelligence services during this live TV session? Was all the information required by the British MPs asked during the public session? • What are according to the journalists the constraints to the effective oversight of intelligence by the UK Parliament? The second part of the exercise is based on the 2012-2013 annual report of the Intelligence and Security Committee (ISC). The trainer distributes Handout 6.7. to the participants and proposes the following guiding questions for the debate: • What are the functions of the ISC? • What kind of intelligence material does the ISC have access to? • Is all information processed by the ISC made public? • Is the aggregate amount of money spent by intelligence agencies known to the public? And the amount spent by each of them? • Does the public get an idea of what the main items of expenditure of intelligence agencies are? • Are the agencies' accounts subject to external audit? • What are the financial management areas British MPs have been most sensitive to? • What was the reason why Parliament did not publish its earlier findings on the failure of a major IT programme? The participants reflect on how their contexts look like and compare it with the British example.
6.	5 min	*Conclusion and re-cap*	Trainer to whole group	-	The trainer summarises the main points of the session and shares them with the participants.

Description of activities

This section describes in more detail the activities listed above in the Session Plan. It also provides alternatives to several activities.

Activity 1: Introduction

The trainer overviews the learning objectives of this session and explains that best practice with regards to the topic under discussion is still in the process of being defined. For this reason, to maximise the learning experience, sharing experiences and discussions will be even more important in this session than they were in previous sessions.

Activity 2. PowerPoint Presentation: Handling legal gaps while practicing financial oversight in the security sector

The trainer presents an introduction to the topic of how oversight actors can handle legal gaps that they encounter when practicing financial oversight in the security sector (***Handout 6.1)***. The short presentation provides a summary of the key topics that will be covered in this session, namely:

- Access to information as an international standard
- Practical ways of protecting sensitive information in the security sector without compromising accountability
- The use of exceptional financial procedures for matters with specific security requirements
- Practicing parliamentary oversight in the absence of an access to information law, with a particular focus on the work of security and defence committees

Materials:

- ***Handout 6.1*** PowerPoint Presentation Hardcopy: Handling legal gaps while practicing financial oversight in the security sector

Activity 3. Guided discussion on how to handle the absence of a clear legal definition of information that needs to be protected

This activity aims to involve the participants in a discussion about which information should be protected and how such a protection should be enshrined in the law. Most countries have chosen one of the three following options:

1. No legal definition => problem of wide legal gap.
2. Defined most information to be confidential except if mentioned otherwise.
3. Defined all information to be public except if it falls under clearly defined categories of confidential information.

There is no standard way of dealing with legal gaps in the definition of confidential information. Therefore, the trainer should focus on ideas coming from the participants and encourage a discussion.

Looking at experiences from other countries can be an efficient way to identify issues for reflection and analysis in the participants' own work context. Before diving into the example of South Africa, the trainer asks a volunteer to note on a flip-chart sheet the issues that participants mention in a brainstorming as being the most relevant in their contexts.

The trainer briefly outlines the history behind the definition and scope of 'sensitive' information in two successive drafts of the South African protection of information bill.

The first draft was tabled in 2010 (***Handout 6.2***) and drew nearly unanimous criticism from

South African and international civil society organisations for its extremely loose and extensive definition of information to protect.

The latest version of the bill, amended several times in the South African legislative process (***Handout 6.3***), was still met with widespread concern inside South Africa. The President eventually bowed to public pressure by refusing to sign it into law, despite the text having been approved by the National Assembly in March 2013.

The trainer invites the participants to take 15 minutes to read and compare the two texts before the discussion.

The discussion may take as point of departure some or all of the following points:

- Does the draft enshrine a general right of access to information held by public entities/ the state (art. 6 in the first draft, art. 4 in the second)?
- If it does, what are the general exceptions to the right of access (art. 6 in the first draft, art. 4 in the second)?
- What is the rationale that allows state information to be classified (arts. 11 and 12 in the first draft, art. 8 in the second draft)?
- Specifically, what are the criteria to decide whether state information is to be classified or not (arts. 11 and 12 in the first draft, art. 8 in the second draft)?

♣ *Alternative*: Small groups: The trainer could first take the participants through the questions and then ask them to work on each question in small groups prior to the whole-group feedback. In this case, the trainer gives each group the set of questions shown above or presents them on a PowerPoint slide.

Materials:

- ***Handouts 6.2 and 6.3*** Two successive drafts of South Africa's Protection of Information Bill (2010 and 2013)
- Flip chart sheet

Activity 4. Handling legal gaps in the exceptions to normal financial oversight rules due to secrecy requirements

This activity consists of a discussion about how to handle legal gaps concerning special financial oversight rules due to secrecy requirements.

This activity follows the same format as the activity above (Activity 3.). It focuses on the strict limits to the use of exceptional financial procedures due to special security requirements.

It could take as a starting point a practical exercise on an excerpt of the Italian legislation on public procurement, itself an application of a European Union directive. The trainer will need to allow participants some time (10 minutes) to read the text beforehand (***Handout 6.4***).

The discussion may be guided by some or all of the following questions:

- Which contracts exactly are exempted from the usual procurement rules in this Italian law? Does such an exemption apply systematically?
- Who decides which procurement contracts are concerned by special security requirements?
- Is a procurement contract under special security requirements always a sole source procurement contract?
- Are all firms allowed to work as suppliers for contracts under special security requirements? If not, what are the criteria for participation in a tender?
- Are procurement contracts under special security requirements no longer subject to audit?
- How does the Italian Parliament oversee public procurement under special security requirements?

♣ *Alternative*: Small groups: The trainer could first take the participants through the questions and then ask them to work on each question in small groups prior to the whole-group feedback. In this case, the trainer gives each group the set

of questions shown above or presents them on a PowerPoint slide.

Materials:

- ***Handouts 6.4*** Excerpt of the Italian Code of Public Procurement
- Flip chart sheet

Activity 5. Guided discussion on how to find the right balance between access to information and secrecy requirements related to national security

This activity consists of a discussion on how to find a balance between full access to information and secrecy requirements related to national security. To make it more concrete, the discussion focuses on the relations between security agencies and Parliament.

This activity follows the same format as activities 3 and 4, but is divided into two.

Part 1:

The trainer distributes two newspaper articles, reporting on a recent case from the United Kingdom. The participants take 15 minutes to read the articles. The trainer asks them to already think about some of the following topics while reading the articles. He/she then guides the discussion.

- Who in the UK Parliament is responsible for financial oversight of the security sector? – [What is the equivalent organ in their own country/countries?]
- What do the articles say about the current powers of the UK Parliament in relation to intelligence agencies, and possible future reforms?
- In past, what information was made public about the functioning of intelligence agencies? Recently, what additional information was made public? As a result of what has there been a change in making more information publicly accessible?
- Does the UK intelligence community ever provide evidence to Parliament, and if so in what form?
- What did the UK Parliament want to know from intelligence services during this session which was broadcast on live TV?
- According to the journalists, what are the constraints to the effective oversight of the intelligence services by the UK Parliament?

♣ *Alternative*: Small groups: The trainer could first take the participants through the questions and then ask them to work on each question in small groups prior to the whole-group feedback. In this case, the trainer gives each group the set of questions shown above or presents them on a PowerPoint slide.

Part 2:

The Parliament hearing covered by the Financial Times was rather exceptional both in its format (a live TV hearing) and the participation of all heads of intelligence agencies in one hearing.

The trainer will now explain to the participants the regular financial oversight work of the British Parliament on intelligence agencies. A short excerpt from the 2012-2013 annual report of the Intelligence and Security Committee (ISC) of Parliament, chaired by a former UK Foreign Secretary, Malcolm Rifkind, can provide some useful ideas for discussion. The trainer will remind participants that this is a **public** document, widely available on the internet.

The trainer will give participants some time (max 10 min.) to read the text and start the discussion at the end. Some or all of the following topics may be addressed in the discussion:

- What are the functions of the Intelligence and Security Committee (ISC)?
- What kind of intelligence material does the ISC have access to?
- Is all information processed by the ISC made public?

- Is the aggregate amount of money spent by intelligence agencies known to the public? And what about the amount spent by each of them?
- Does the public get an idea of what the main items of expenditure of intelligence agencies are?
- Are the agencies' accounts subject to external audit?
- What are the financial management areas British MPs have been most sensitive to?
- What was the reason why Parliament did not publish its earlier findings on the failure of a major IT programme?

♣ *Alternative*: Small groups: The trainer could first take the participants through the questions and then ask them to work on each question in small groups prior to the whole-group feedback. In this case, the trainer gives each group the set of questions shown above or presents them on a PowerPoint slide.

Materials:

- ***Handouts 6.5 and 6.6*** Two Financial Times articles on a public Parliamentary hearing of the UK intelligence agencies
- ***Handout 6.7*** Excerpt of the 2012-2013 report of the Intelligence and Security Committee of the British Parliament
- Flip chart sheet

Activity 6. Wrap-up of the session

The trainer summarises the main points of the session and shares them with the participants.

Handout 6.1

Power-point presentation hardcopy: Handling legal gaps while practicing financial oversight in the security sector

Handling legal gaps while practicing financial oversight in the security sector

Tool 6

Overall Considerations

- Legal gaps should be addressed to avoid leaving too much room for executive decisions that lack a legal basis.
- Nowadays, to make information held by public entities available to the public tends to be regarded as a basic human right.
- The executive must explain and substantiate the need for special protection of certain types of information.
- Financial oversight procedures remain by default the normal ones. Any exception must be based on relevant legislation.

2

Practicalities: Protection of Information

- A culture of secrecy can become a breeding ground for corruption in defence and security agencies.
- Therefore, secrecy and protection of information requirements should be defined by law as restrictively as possible:
  - Sweeping references to 'national interests' ought to be avoided
  - Internal review mechanisms should be established, e.g., a committee reporting to the President or Prime Minister
  - Protection of whistleblowers should be ensured

3

Practicalities: Budgetary Oversight

- Creating a sound legal framework for budgetary oversight is a must.
- The Ministry of Finance should be included as much as possible in the programming and budgeting work.
- Keeping secret intelligence budgets as small as possible ---> **No extrabudgetary expenditures!**
- The defence budget should be divided into categories of differing secrecy, such as:
  - Items presented for discussion to Parliament in aggregated form; and
  - Items presented to members of a parliamentary committee with the required clearance in a more disaggregated and detailed form

4

Practicalities: Procurement Oversight

- The executive should present its defence and procurement plans and organise roundtable debates.
- The executive and legislative should ensure to strictly limit special confidentiality conditions in defence and security procurement. This includes avoiding confidentiality markings for the purchase of boots, uniforms, transport vehicles, office facilities and even patrol vessels.
- Defence agencies should build internal specialist procurement skills and centralise the most important purchases in order to minimize undue hierarchical influence in the decision-making.
- Defence agencies should submit tender specifications to an independent technical review
- Sole source arrangements should be avoided as much as possible: while restricted, some sort of competition should still apply ---> e.g. hearings behind closed doors.
- Key procurement decisions of defence agencies should be made or reviewed by a tender board with external participation.

5

Practicalities: Parliamentary Oversight

- **Security and defence committees:**
  - drafting **legislation**
  - reviewing security **policies**
  - expenditure **oversight**
  - monitoring of **procurement**, especially large-scale ones -> need for parliamentary approval
  - consulting on **international agreements**
  - reviewing senior **appointments**
- Requirements:
  - **authority** delineated in legislation
  - **capacity** and qualifications
  - **non-partisan** attitude

6

Handout 6.2

Extract from the First draft of the South African Protection of Information Bill, as introduced to Parliament on 5 March 2010

Source: Website of the South African Parliament [accessed April 2015]: http://pmg-assets.s3-website-eu-west-1.amazonaws.com/bills/b6-10.pdf

REPUBLIC OF SOUTH AFRICA

Protection of Information Bill

(As introduced in the National Assembly (proposed section 75); explanatory summary of Bill published in Government Gazette No. 32999 of 5 March 2010)
(The English text is the official text of the Bill)
[B 6—2010] ISBN 978-1-77037-630-4
No. of copies printed 1 800

(4 March 2010)

BILL

To provide for the protection of certain information from destruction, loss or unlawful disclosure; to regulate the manner in which information may be protected; to repeal the Protection of Information Act, 1982; and to provide for matters connected therewith.

PREAMBLE

RECOGNISING the importance of information to the national security, territorial integrity and well-being of the Republic;

ACKNOWLEDGING the harm of excessive secrecy;

AFFIRMING the constitutional framework for the protection and regulation of access to information;

DESIRING to put the protection of information within a transparent and sustainable legislative framework;

AIMING to promote the free flow of information within an open and democratic society without compromising the security of the Republic,

BE IT THEREFORE ENACTED by the Parliament of the Republic of South Africa,

as follows:—

[…]

CHAPTER 2

GENERAL PRINCIPLES OF STATE INFORMATION

State information

4. State information may, in terms of this Act, be protected against unlawful disclosure, destruction, alteration or loss.

Protected information

5. (1) State information which requires protection against unlawful alteration, destruction or loss, is referred to as "valuable information".

(2) State information in material or documented form which requires protection against unlawful disclosure may be protected by way of classification and access to such information may be restricted to certain individuals who carry a commensurate security clearance.

General principles of State information

6. The following principles underpin this Act and inform its implementation and interpretation:

(a) Unless restricted by law or by justifiable public or private considerations, State information should be available and accessible to all persons;

(b) information that is accessible to all is the basis of a transparent, open and democratic society;

(c) access to information is a basic human right and promotes human dignity, freedom and the achievement of equality;

(d) the free flow of information promotes openness, responsiveness, informed debate, accountability and good governance;

(e) the free flow of information can promote safety and security;

(f) accessible information builds knowledge and understanding and promotes creativity, education, research, the exchange of ideas and economic growth;

(g) some confidentiality and secrecy is, however, vital to save lives, to enhance and to protect the freedom and security of persons, to bring criminals to justice, to protect the national security and to engage in effective government and diplomacy;

(h) measures to protect State information should not infringe unduly on personal rights and liberties or make the rights and liberties of citizens unduly dependent on administrative decisions; and

(i) measures taken in terms of this Act must—

(i) have regard to the freedom of expression, the right of access to information and the other rights and freedoms enshrined in the Bill of Rights; and

(ii) be consistent with article 19 of the International Covenant on Civil and Political Rights and have regard to South Africa's international obligations;

(j) paragraphs (a) to (i) are subject to the security of the Republic, in that the national security of the Republic may not be compromised.

[…]

CHAPTER 5

INFORMATION WHICH REQUIRES PROTECTION AGAINST DISCLOSURE

Part A

Sensitive Information

National interest of Republic

11. (1) The national interest of the Republic includes, but is not limited to—

(a) all matters relating to the advancement of the public good; and

(b) all matters relating to the protection and preservation of all things owned or maintained for the public by the State.

(2) The national interest is multi-faceted and includes—

(a) the survival and security of the State and the people of South Africa; and

(b) the pursuit of justice, democracy, economic growth, free trade, a stable monetary system and sound international relations.

(3) Matters in the national interest include—

(a) security from all forms of crime;

(b) protection against attacks or incursions on the Republic or acts of foreign interference;

(c) defence and security plans and operations;

(d) details of criminal investigations and police and law enforcement methods;

(e) significant political and economic relations with international organisations and foreign governments;

(f) economic, scientific or technological matters vital to the Republic's stability, security, integrity and development; and

(g) all matters that are subject to mandatory protection in terms of sections 34 to 42 of the Promotion of Access to Information Act, whether in classified form or not.

(4) The determination of what is in the national interest of the Republic must at all times be guided by the values referred to in section 1 of the Constitution.

Part B

Commercial information

Nature of commercial information

12. (1) Commercial information becomes the subject matter of possible protection from disclosure under the following circumstances:

(a) Commercial information of an organ of state or information which has been given by an organisation, firm or individual to an organ of state or an official representing the State, on request or invitation or in terms of a statutory or regulatory provision, the disclosure

of which would prejudice the commercial, business, financial or industrial interests of the organ of state, organisation or individual concerned;

(b) information that could endanger the national interest of the Republic.

(2) Commercial information which may prejudice the commercial, business or industrial interests of an organisation or individual, if disclosed, includes—

(a) commercial information that is not in the public domain, which if released publicly would cause financial loss or competitive or reputational injury to the organisation or individual concerned;

(b) trade secrets, including all confidential processes, operations, styles of work, apparatus, and the identity, amount or source of income, profits, losses or expenditures of any person, firm, partnership, corporation or association.

(3) Only commercial information which the State is not otherwise authorised by law to release may be protected against disclosure.

(4) Government-prepared reports should be protected from disclosure to the extent they restate classified commercial information.

Handout 6.3

Final Draft of the South African Protection of State Information Bill, as adopted by Parliament on 23 April 2013 and submitted to the President who sent it back to Parliament on 12 September 2013 for re-consideration

Source: Website of the South African Parliament [accessed April 2015]: http://pmg-assets.s3-website-eu-west-1.amazonaws.com/131016b6f-2010.pdf

REPUBLIC OF SOUTH AFRICA

Protection of State Information Bill

(As amended by Ad Hoc Committee on Protection of State Information Bill (National Assembly))
(introduced as Protection of Information Bill [B 6—2010])
(The English text is the official text of the Bill)
(MINISTER OF STATE SECURITY)
[B 6F—2010]
ISBN 978-1-77597-083-5
No. of copies printed 1800
(24 April 2013)

BILL

To provide for the protection of sensitive state information; to provide for a system of classification, reclassification and declassification of state information; to provide for the protection of certain valuable state information against alteration, destruction or loss or unlawful disclosure; to regulate the manner in which state information may be protected; to repeal the Protection of Information Act, 1982 (Act No. 84 of 1982); and to provide for matters connected therewith.

PREAMBLE

RECOGNISING that national security is subject to the authority of Parliament and the national executive, as contemplated in section 198 of the Constitution;

MINDFUL of the right of access to any information held by the State provided for in section 32 of the Constitution;

ACCEPTING that the right of access to information is a cornerstone of our democracy

ACKNOWLEDGING in accordance with section 36 of the Constitution that the right of access to any information held by the State may be restricted when necessary for reasons of national security;

RECOGNISING the harm caused by excessive secrecy;

DESIRING to put the protection of state information within a transparent and sustainable legislative framework; and

AIMING to promote the free flow of information within an open and democratic society without compromising the national security of the Republic,

BE IT THEREFORE ENACTED by the Parliament of the Republic of South Africa, as follows:—

[…]

CHAPTER 2

GENERAL PRINCIPLES OF STATE INFORMATION

General principles of state information

4. (1) The following principles underpin this Act and inform its implementation and interpretation:

(a) Unless restricted by law that clearly sets out reasonable and objectively justified public or private considerations, state information should be available and accessible to all persons;

(b) state information that is accessible to all is the basis of a transparent, open and democratic society;

(c) access to state information is a basic human right and promotes human dignity, freedom and the achievement of equality;

(d) the free flow of state information promotes openness, responsiveness, informed debate, accountability and good governance;

(e) the free flow of state information can promote safety and security;

(f) accessible state information builds knowledge and understanding and promotes creativity, education, research, the exchange of ideas and economic growth;

(g) the protection and classification of certain state information is however vital to save lives, to enhance and to protect the freedom and security of persons, bring criminals to justice, protect the national security and to engage in effective government and diplomacy;

(h) measures to protect state information should not infringe unduly on personal rights and liberties or make the rights and liberties of citizens unduly dependent on administrative decisions;

(i) measures taken in terms of this Act must—

(i) have regard to the freedom of expression, the right of access to information and the other rights and freedoms enshrined in the Bill of Rights;

(ii) promote and support the functions and effectiveness of the Constitutional Institutions Supporting Democracy; and

(iii) be consistent with article 19 of the International Covenant on Civil andPolitical Rights and have regard to South Africa's international obligations; and

(j) in balancing the legitimate interests referred to in paragraphs (a) to (i) The relevant Minister, relevant official or a court must have due regard to the security of the Republic, in that the national security of the Republic may not be compromised.

(2) Certain state information may, in terms of this Act, be protected against unlawful disclosure, alteration, destruction or loss.

(3) State information in material or documented form which requires protection against unlawful disclosure may be protected by way of classification and access to such information may be restricted to the Cabinet, institutions referred to in section 181 of the Constitution and certain individuals who carry a commensurate security clearance.

[…]

CHAPTER 5

SYSTEM OF CLASSIFICATION, RECLASSIFICATION AND

DECLASSIFICATION OF STATE INFORMATION

Conditions for classification, reclassification and declassification

8. (1) The decision to classify information must be based solely on the conditions set out in this Act.

(2) (a) Classification of state information is justifiable only when it is necessary to protect national security.

(b) Classification of state information may not under any circumstances be used to—

(i) conceal breaches of the Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004) or any other unlawful act or omission, incompetence, inefficiency or administrative error;

(ii) restrict access to state information in order to limit scrutiny and thereby avoid criticism;

(iii) prevent embarrassment to a person, organisation, or organ of state or agency;

(iv) unlawfully restrain or lessen competition; or

(v) prevent, delay or obstruct the release of state information that does not require protection under this Act.

(c) The classification of state information is an exceptional measure and should be conducted strictly in accordance with section 11.

(d) State information is classified only when there is—

(i) a clear, justifiable and legitimate need to do so; and

(ii) a demonstrable need to protect the state information in the interest of the national security.

(e) If there is significant doubt as to whether state information requires protection, the matter must be referred to the relevant Minister for a decision.

(f) The decision to classify may not be based on any extraneous or irrelevant reason.

(g) Classification decisions must balance the right to access to state information against the need to classify state information in terms of this Act.

(h) Scientific and research information not clearly related to the national security may not be classified.

(i) State information may not be reclassified after it has been declassified and released to the public under proper authority.

(j) Classification must be in place only for as long as the protection is actually necessary.

(k) Where there is still a need for classification it may be that the state information in question no longer requires a high classification level and should be downgraded.

(3) Specific considerations with regard to the decision whether to classify state information must include whether the disclosure may—

(a) expose the identity of a confidential source, or reveal information about the application of an intelligence or police source when the unlawful disclosure of that source would clearly and demonstrably damage the national security of the Republic or the interests of the source or his or her family;

(b) clearly and demonstrably impair the ability of government to protect officials or persons for whom protection services, in the interest of the national security, are authorised;

(c) seriously and substantially impair the national security, defence or intelligence systems, plans or activities;

(d) seriously and demonstrably impair relations between South Africa and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the Republic;

(e) violate a statute, treaty, or international agreement, including an agreement between South African government and another government or international institution;

(f) cause life threatening or other physical harm to a person or persons; or

(g) cause demonstrable, irreparable or exceptionally grave harm to the national security of the Republic.

(4) The application of the classification conditions may not in any way inhibit or prevent officials from informing authorised officials of such information in order to fulfil law enforcement or intelligence functions authorised or prescribed by law.

(5) When the conditions for classification contemplated in this section no longer exist classified information must be declassified.

Nature of classified information

9. Classified information—

(a) is sensitive state information which is in material or record form;

(b) must be protected from unlawful disclosure and against alteration, destruction or loss as prescribed;

(c) must be safeguarded according to the degree of harm that could result from its unlawful disclosure;

(d) may be made accessible only to those holding an appropriate security clearance and who have a legitimate need to access the state information in order to fulfil their official duties or contractual responsibilities; and

(e) must be classified in terms of section 11.

Handout 6.4

Extract from the Italian Republic's Legislative Decree 12 April 2006, n. 163 ("Code of Public Procurement, in conformity with the European Union's Directives 2004/17/CE and 2004/18/CE")

Title II – Contracts wholly or partially excluded from the scope of the present Code

Art. 16: Contracts related to the production or commerce of armament, ammunition and other war equipment

1. Subordinate to art. 296 of the Treaty establishing the European Community, the present code does not apply to contracts in the field of defence, related to the production and commerce of armament, ammunitions and other war equipment that serves specifically military purposes, as spelled out in the list established by the Council of the European Community.

2. This article is without prejudice to the prevailing provisions arising from international agreements, or regulations of the Defence Ministry.

Art. 17: Secret contracts or contracts requiring special security measures

1. Whenever special security or confidentiality requirements apply – either in conformity with prevailing legislative, normative or administrative measures, or whenever so required by the protection of essential national security interests – works, services and supplies affected to the activity of the Bank of Italy [i.e. the Central Bank], the armed forces, the police for the sake of the Nation's defence, or for institutional tasks, or to the activity of contracting authorities mentioned in Part III, may be carried out regardless of the provisions stipulating the publicity of public procurement, and in conformity with the procedures established in this article.

2. The ministries and agencies identify in a decree, duly motivating their decision, the works, services and supplies to be considered 'secret'… or 'to be executed under special security measures'.

3. Such contracts are performed by private firms possessing, in addition to the requirements spelled out in the Civil Code, a security clearance.

4. Adjudication of the contracts declared 'secret', or 'to be executed under special security measures' takes place following an informal call for proposals, to which at least five private firms are invited, inasmuch as such number of qualified firms exists in relation to the objectives of the procurement, and as long as a negotiation with more than one firm is compatible with the requirements for secrecy.

5. […]

6. Those responsible for planning, project management and testing, if they are outside the agency concerned, must possess a valid security clearance.

7. Under this article, contracts entered into by state agencies are only subject to an audit ex-post by the Court of Accounts, which makes an appraisal on the regularity, integrity and effectiveness of management. Activities under this paragraph are reported to Parliament on a yearly basis before 30 June.

Handout 6.5

Financial Times Article 'Top UK Spies Accept Need for More Openness'

Top UK spies accept need for more openness

By Kiran Stacey and John Aglionby

Last updated: November 7, 2013 4:40 pm

http://www.ft.com/cms/s/0/981300f8-47c0-11e3-9398-00144feabdc0.html#axzz3bv6NaQgg [last accessed April 2015]

Britain's top spies have said they are considering making more of their tactics public amid anger about apparent mass surveillance techniques, but warned that recent revelations have made the UK less safe.

The heads of MI5, MI6 and GCHQ were facing public questioning for the first time in an open hearing of parliament's intelligence and security committee.

Sir Iain Lobban, head of GCHQ, the communications intelligence service, said recent revelations in the Guardian newspaper and elsewhere had added to an already "active debate" within the intelligence service over what they should make public.

But he added that the publication of British spies' methods, mostly based on leaks by Edward Snowden, a former US National Security Agency contractor, was a "gift to the terrorists" and had led to an "inexorable darkening" of intelligence available to them as hostile groups change the way they communicate.

Sir Iain told MPs: "What we have seen over the last five months is near daily discussion by some of our targets…on how to avoid what they now perceive to be vulnerable communications methods."

He added: "The cumulative effect of the media coverage, the global media coverage, will make the job we have far, far harder for years to come."

Sir John Sawers, head of MI6, said the leaks had been "very damaging".

"It's clear that our adversaries are rubbing their hands in glee, al-Qaeda is lapping this up…and western security has suffered as a consequence."

Guardian News & Media, which has insisted that its articles on Mr Snowden's revelations were only published after consultation with officials, said it was "only the involvement of global newspapers that prevented this information from spilling out across the web and genuinely causing a catastrophic leak".

"We understand that the agencies will always warn that any form of disclosure has a damaging impact on their work – but this cannot mean the end of all questioning and debate," it said.

Mark Field, one of the committee members, said the committee had not been aware of all the "intricacies" of the spying revealed by the Guardian and others. He asked Sir Iain for a "comprehensive update" of links with foreign agencies in a closed session, a request to which the GCHQ chief agreed.

Sir Iain insisted his staff did not listen to everyone's communications. He said the systems were designed only to gather the pertinent "needles or fragments of needles" of the "haystacks" of information that are gathered.

"We do not spend our time listening to the telephone calls or reading the emails of the majority, the vast majority. That would not be proportionate. It would not be legal," he said. "We do not do it."

GCHQ staff would "walk out of the building" if they were asked to snoop on innocent people.

When asked about the extent of UK spying operations overseas, Sir John said MI6 had operations in only a few countries, without being specific. "Everything we do is authorised by ministers," he added.

Both Sir John and Andrew Parker, the head of MI5, said they would never ask a foreign agency to question someone if they thought that might result in torture.

Mr Parker said the security agencies had disrupted 34 plots since 2005, the year of the 7/7 attack on London, including one or two major ones each year.

He said the number of people who had travelled from Britain to Syria and returned, possibly radicalised, was in the "low hundreds". There were "several thousand" people in Britain that MI5 thought posed a potential terrorist threat.

Critics accused MPs of being too soft on the security chiefs. Lord Foulkes, the Labour peer, said the committee's oversight of UK intelligence had been "inadequate".

Handout 6.6

Financial Times Article 'Britain's Spymasters Step Out Of Shadows'

Britain's spymasters step out of shadows

By James Blitz, Defence and Diplomatic Editor

November 6, 2013 6:36 pm

http://www.ft.com/intl/cms/s/0/449667da-4707-11e3-bdd2-00144feabdc0.html#axzz3bv6NaQgg [last accessed April 2015]

The heads of the UK security services have long been the most secretive officials in the British state, people who almost never make a public appearance. But at 2pm on Thursday, history will be made when they step out of the shadows and appear live on TV before parliament's Intelligence and Security Committee.

It was only in 1992 that the name of the head of MI5 was made public. It was only two years later that the UK government officially acknowledged that MI6 existed. Since then, the service chiefs have regularly give evidence to parliament – but strictly in private.

Today, however, the three heads – Sir John Sawers, the chief of MI6; Sir Iain Lobban, the head of GCHQ; and Andrew Parker of MI5 – will appear before the ISC in a 90-minute open session.

"I am not sure the heads of the services are going to find this an easy experience," says one MP on the ISC, which is made up of MPs, peers and former civil servants. "These people didn't take on their jobs to do live speeches and hearings. Indeed, until very recently, we didn't admit these people existed."

The decision to hold the open hearing is part of the beefing-up of the ISC's remit and independence, says Sir Malcolm Rifkind, the committee's chairman and a former foreign secretary.

Sir Malcolm says the ISC now has significant new powers, in particular the right to send its staff into the intelligence services' headquarters and examine any material they wish. "The idea that the agencies are allowing outsiders into their premises like this is remarkable," he says.

However, the timing of Thursday's hearing is also important. It comes as the secret world reels from allegations over the work of GCHQ and the role it plays alongside the US National Security Agency in hoovering up huge quantities of personal data on the internet.

As a result, there is certain to be a strong focus by the ISC on Sir Iain Lobban, a reclusive figure whose Cheltenham-based agency is by far the most reticent of the three in its dealings with MPs and journalists.

The ISC may want to know how much damage Sir Iain believes the revelations by Edward Snowden, the former NSA contractor, have done to UK intelligence.

They may well ask whether Sir Iain agrees with the assessment by his predecessor, Sir David Omand, that the Snowden revelations are "the most catastrophic loss to British intelligence ever, much worse than Burgess and MacLean in the 1950s."

But the ISC will also want to know whether Sir Iain accepts legislation is now needed to give better ministerial and parliamentary oversight of GCHQ activities. One ISC member says there has been "vigorous debate within the committee" on these issues as it prepares to make recommendations.

For the other two heads of service, there will be less pressure. Mr Parker's agency, MI5, is widely seen as having had considerable success in preventing jihadist bomb plots across the UK in recent years.

MI6 was for a long time living under the shadow of its flawed 2002 assessment that Iraq possessed weapons of mass destruction. On Thursday, questioning of Sir John Sawers is likely to be on current issues, in particular how he sees the evolving jihadist threats arising out of Syria and the Maghreb.

Some commentators believe the hearing will test the ISC as well as the intelligence chiefs. This is because some believe it is unable to hold the services to account, despite its new powers.

Alan Rusbridger, editor of the Guardian, which has published much of the Snowden leaks, said in a recent article that the committee chairman was not "to put it mildly, a child of the digital age". He says Sir Malcolm, like his counterparts in the US Congress, "would have struggled to understand" some of the documents on GCHQ activity leaked by Mr Snowden.

But Sir Malcolm is confident that the ISC is becoming a robust interrogator of the security services. "Thursday's hearing is not going to be some kind of scripted event," he says. "There will be time for follow-up questions. The agency heads are not going to know those questions in advance."

Heads of the intelligence services

Sir John Sawers, chief of MI6, the foreign intelligence service

At 57, Sir John will be the most comfortable of the three service chiefs when they appear before the ISC on Thursday. After a lengthy diplomatic career, which took him to some of the highest posts in the Foreign Office, he is well used to engaging with politicians and appearing at high profile events. Sir John's four-year tenure at MI6 has been troubled, partly because he ended up having to manage legal challenges against the agency arising out of its previous work in Iraq and Libya. He is respected in Downing Street and is seen as the leading UK government figure on Iran policy.

Andrew Parker, director-general of MI5, the domestic security service

After just six months in the job, Mr Parker triggered controversy last month with a toughly worded speech that effectively attacked The Guardian for publishing documents relating to GCHQ's operations. In that speech, he said the leaks by NSA contractor Edward Snowden had caused "enormous damage" to UK national security. Mr Parker, 51, has a quietly spoken manner which colleagues say exudes a tough inner streak. He was director of counter terrorism at MI5 on the day al-Qaeda murdered 52 people in London on 7 July, 2005. MI5 has won considerable credit in Whitehall for the way it has contained jihadist threats since 2005.

Sir Iain Lobban, director of GCHQ, the cyber-intelligence service

Sir Iain has headed GCHQ since 2008. He is the most reclusive of the three heads of service and the only one who is completely unknown to the British media. Yet he is also the agency chief with most questions to answer about the way his organisation functions. GCHQ is at the centre of a huge political controversy because of the Snowden leaks. It is collaborating with the US National Security Agency in hoovering up huge quantities of personal data on the internet.

Handout 6.7

Short excerpt of the 2012-2013 Report of the Intelligence and Security Committee of the British Parliament.

Intelligence and Security Committee of Parliament

Annual Report 2012–2013

Chairman:
The Rt. Hon. Sir Malcolm Rifkind, MP

Presented to Parliament pursuant to section 3 of the Justice and Security Act 2013

Ordered by the House of Commons to be printed on 10 July 2013

HC 547 £16.00

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

The Rt. Hon. Sir Malcolm Rifkind, MP (Chairman)

The Rt. Hon. Hazel Blears, MP
The Rt. Hon. Lord Butler KG GCB CVO
The Rt. Hon. Sir Menzies Campbell CH CBE QC, MP
Mr Mark Field, MP
The Rt. Hon. Paul Goggins, MP
The Rt. Hon. George Howarth, MP
Dr Julian Lewis, MP
Lord Lothian QC PC

The Intelligence and Security Committee of Parliament (ISC) is a statutory committee of Parliament that has responsibility for oversight of the UK intelligence community. The Committee was originally established by the Intelligence Services Act 1994, and has recently been reformed by the Justice and Security Act 2013.

The Committee oversees the intelligence and security activities of the UK, including the policies, expenditure, administration and operations of the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarters (GCHQ). The Committee also scrutinises the work of other parts of the UK intelligence community, including the Joint Intelligence Organisation and the National Security Secretariat in the Cabinet Office; Defence Intelligence in the Ministry of Defence; and the Office for Security and Counter-Terrorism in the Home Office.

The Committee consists of nine Members drawn from both Houses of Parliament. The Chair is elected by its Members. The Members of the Committee are subject to Section 1(1)(b) of the Official Secrets Act 1989 and are routinely given access to highly classified material in carrying out their duties.

The Committee sets its own agenda and work programme. It takes evidence from Government Ministers, the Heads of the intelligence and security Agencies, officials from the intelligence community, and other witnesses as required. The Committee is supported in its work by an independent Secretariat and an Investigator. It also has access to legal and financial expertise where necessary.

The Committee produces an Annual Report on the discharge of its functions. The Committee may also produce Reports on specific investigations. Prior to the Committee publishing its Reports, sensitive material that would damage national security is blanked out ('redacted'). This is indicated by *** in the text. The intelligence and security Agencies may request the redaction of sensitive material in the Report which would damage their work, for example by revealing their targets, methods, sources or operational capabilities. The Committee considers these requests for redaction in considerable detail. The Agencies have to demonstrate clearly how publication of the material in question would be damaging before the Committee agrees to redact it. The Committee aims to ensure that only the bare minimum of text is redacted from the Report. The Committee believes that it is important that Parliament and the public should be able to see where information had to be redacted, rather than keeping this secret. This means that the Report that is published is the same as the classified version sent to the Prime Minister (albeit with redactions): there is no 'secret' report.

CONTENTS

SECTION 9: AGENCY EXPENDITURE

101. In 2011/12, the Single Intelligence Account (SIA) was approximately £2 billion.[107]

	2011/12	2012/13	2013/14	2014/15
Single Intelligence Account (£m)[108]	1,928	1,991	1,908	1,883
Cyber Security funding and Critical Capability Pool Funding (£m)[109]	70	95	171	123

Each Agency's actual expenditure in 2011/12 was as follows:

- GCHQ spent £***m (within 0.3% of its budget);
- the Security Service spent £***m (within 0.9% of its budget); and
- SIS spent £***m (within 0.8% of its budget).

102. This is the third year of the 2010 Spending Review (SR10) settlement. In our 2010–2011 Annual Report[110] we expressed concerns that the real-terms cut of approximately 11.3% in the SIA might have an impact on the ability of all three Agencies to maintain coverage of the threat. We noted that factors such as public sector pay constraints and procurement savings meant that, despite inflation, front-line capabilities were being protected.

103. The 2011/12 resource accounts for all three Agencies were certified by the Comptroller and Auditor General in June 2012. The National Audit Office's (NAO's) audits raised a number of financial management and accounting issues which needed to be addressed. The majority of these relate to adherence to accounting standards, but other issues of note raised by the auditors included:

- an SIS payment of several million pounds relating to an operation with a foreign intelligence service which was not adequately documented;
- spending in excess of Treasury limits on advertising and marketing (SIS exceeded these limits in one of their external recruitment campaigns, although retrospective approval was eventually obtained); and
- incorrect treatment of ongoing liabilities relating to agent payments (Security Service).

Work is under way to address these issues, and all three Agencies continue to make improvements to their financial systems and management, with the assistance of the NAO.

[107] *In addition to the Agencies' budgets, the SIA also includes funding for the National Cyber Security Programme, elements of the Critical Capability Pool Funding and funding for a small part of the National Security Secretariat in the Cabinet Office. Since SR10 there have been changes to the SIA settlement to take account of transfers between departments; there have also been reductions to the settlement following the Chancellor's Autumn and Main Budget Statement.*

[108] *SIA settlement – 'near-cash' (Resource DEL plus Capital DEL, excluding depreciation, Annually Managed Expenditure and ring-fenced funding for cyber security).*

[109] *Resource DEL plus Capital DEL.*

[110] *Cm 8403.*

Major projects

104. The Agencies continue to spend a significant proportion of their overall budgets on capital projects. These projects primarily relate to improvements to IT systems, communications equipment and accommodation. This year the NAO has assisted the Committee in scrutinising the Agencies' finances and administration, including undertaking a detailed review of each Agency's biggest capital projects.[111]

105. In general terms, and across all three Agencies, most capital projects are on track to deliver their main objectives within budget and on time. In their latest formal reviews[112] nearly all projects have been assessed as 'Green' (on target to succeed) or 'Amber' (some changes or improvements required). The following summarises the key findings of the NAO's review:[113]

- In GCHQ, most projects are delivering the required business benefits.[114] While forecast costs can sometimes vary substantially from initial plans (often due to changing mission requirements during the course of projects), taken as a whole there is a net underspend.
- SIS has a number of major IT, communications and infrastructure projects under way. Of their seven largest projects, two have been assessed as 'Amber' in formal gateway reviews. While there have been minor delays and some issues with the other projects they are, in general terms, making satisfactory progress.
- The Security Service has eight major projects under way, with half reviewed as 'Amber'. These ratings largely reflect projects running behind schedule: in several instances this is because projects were postponed to allow the Service to focus on the Olympics. In cost terms the projects, as a whole, are running to budget (with one project considerably over budget balanced by one considerably under budget).

106. The ISC has, for a number of years, taken a close interest in the SCOPE IT programme, led by the Cabinet Office. The programme sought to provide a secure IT system and connectivity between a number of government departments and agencies and was to be delivered in two phases. While the first of these was successfully delivered at the end of 2007, Phase 2 was beset by problems and eventually abandoned by the Cabinet Office in July 2008. While the Committee investigated this failure in some detail, we did not publish our findings whilst the parties involved were engaged in arbitration. These negotiations have now concluded and a settlement has been reached. We are therefore able to report on our findings, which are included at Annex B.

---

[111] *This review was based on data provided by the Agencies.*
[112] *Gateway Reviews are carried out as a series of assurance 'gates' where projects are independently assessed before key project milestones are met.*
[113] *This review was based on data provided by the Agencies.*
[114] *The Desktop project continues to face difficulties. This is an issue that we will return to in due course.*

Additional resources

- Andersson, Lena and Salah Aldin, Mohammad. *Guidebook: Strengthening Financial Oversight in the Security Sector*. Geneva: DCAF, 2011, Sections 3 & 5.
- *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices*. Ed. Todor Tagarev. Geneva: NATO-DCAF, 2010, Part I, Part III, Part IV & Chapter 18.
- *Le Principe de Transparence en Suisse et dans le Monde*. Ed. Pasquier, Martial. Lausanne: Presses Polytechniques et Universitaires Romandes, 2013. (Especially: Cottier, Bertil and Nicolas Masson. «Le domaine de la sécurité ou comment concilier confidentialité, **légitime et transparence nécessaire**».)
- Transparency International. *Building Integrity and Countering Corruption in Defence and Security: 20 practical reforms*. London: Transparency International, 2011.
- Transparency International. *Codes of Conduct in Defence Ministries and Armed Forces. What makes a Good Code of Conduct?* London: Transparency International, 2011.
- Hendrickson, Dylan, and Ball, Nicole. *Off-Budget Military Expenditure and Revenue: Issues and Policy Perspectives for Donors*. London, King's College: DFID, 2002.

Annex A.

Handling legal gaps while practicing financial oversight in the security sector: the local training session

Introduction

The following objectives, suggested content, example activities and suggested sources are designed to give suggestions and examples of how materials can be developed by the trainer to suit their own particular local context.

Learning objectives

Participants will be able to:

1. Understand the role of the State Audit and Administrative Bureau (SAACB) as the supreme external oversight and audit body in the local context
2. Become aware of the legislations governed by the State Audit and Administrative Bureau (SAACB)

Suggested content to be covered

- General comments of the SAACB and recommendations
- Oversight activities between the law and the implementation: the work of the SAACB with the security agencies

Focus questions

- What is the role of the State Audit and Administrative Bureau (SAACB) in the local context?
- What legislations are governed by the State Audit and Administrative Bureau (SAACB)?

Overview

Handout L.6.1 *Questionnaire: 'Legal gaps in the State Audit and Administrative Control Bureau'*

Trainer Resource L6.1 *PowerPoint Presentation Hardcopy: Legal Gaps of Audit State Audit and Administrative Control Bureau (SAACB)*

Description of example activities

The following example activities are taken from the two hours of localised content that was created for use in trainings conducted in the occupied Palestinian territory. They are given here as a model or example for the trainer to adapt if desired.

Activity 1. Questionnaire: 'Legal gaps in the State Audit and Administrative Control Bureau'

Time 30 min

The trainer gives a copy of the multiple-choice questionnaire to each participant. The questionnaire contains questions on the role of the State Audit and Administrative Control Bureau (SAACB). It also asks about the relation between SAACB and the Palestinian security agencies. Once the questionnaire is completed, each question is discussed and explained among the whole group (30 minutes).

Materials

- ***Handout L.6.1*** Questionnaire: 'Legal gaps in the State Audit and Administrative Control Bureau'

Activity 2. PowerPoint presentation: Legal Gaps of Audit State Audit and Administrative Control Bureau (SAACB)

Time 30 min

The trainer presents the PowerPoint (***Trainer Resource L.6.1***) and asks and answers questions of the participants.

Materials

- Trainer Resource L6.1 PowerPoint: Legal Gaps of Audit State Audit and Administrative Control Bureau (SAACB)

Handout L.6.1

Questionnaire: 'Legal gaps in the State Audit and Administrative Control Bureau'.

Question 1: Does the constitution authorize a particular agency to perform the function of a public auditor for the state?

1. There is a constitutional provision
2. There isn't a constitutional provision
3. By legal delegation only

Question 2: Are security agencies subject to oversight by SAACB?

1. Security agencies are subject to SAACB oversight
2. Security agencies are not subject to SAACB oversight

Question 3: Are all security agencies subject to oversight by SAACB?

1. All security agencies are subject to SAACB oversight
2. Not all security agencies are subject to SAACB oversight
3. Specify exceptions in the law or the implementation:
   - Law
   - implementation

Question 4: Does the law offer sufficient guarantees for SAACB to perform its work impartially as far as security agencies are concerned? (independence and impartiality of oversight bodies)

1. Yes
2. No

Question 5: Does the law provide immunity to SAACB when performing its work as far as security agencies are concerned? (Immunity of SAACB personnel)

1. Yes
2. No

Question 6: Does SAACB have special procedures when auditing the security sector?

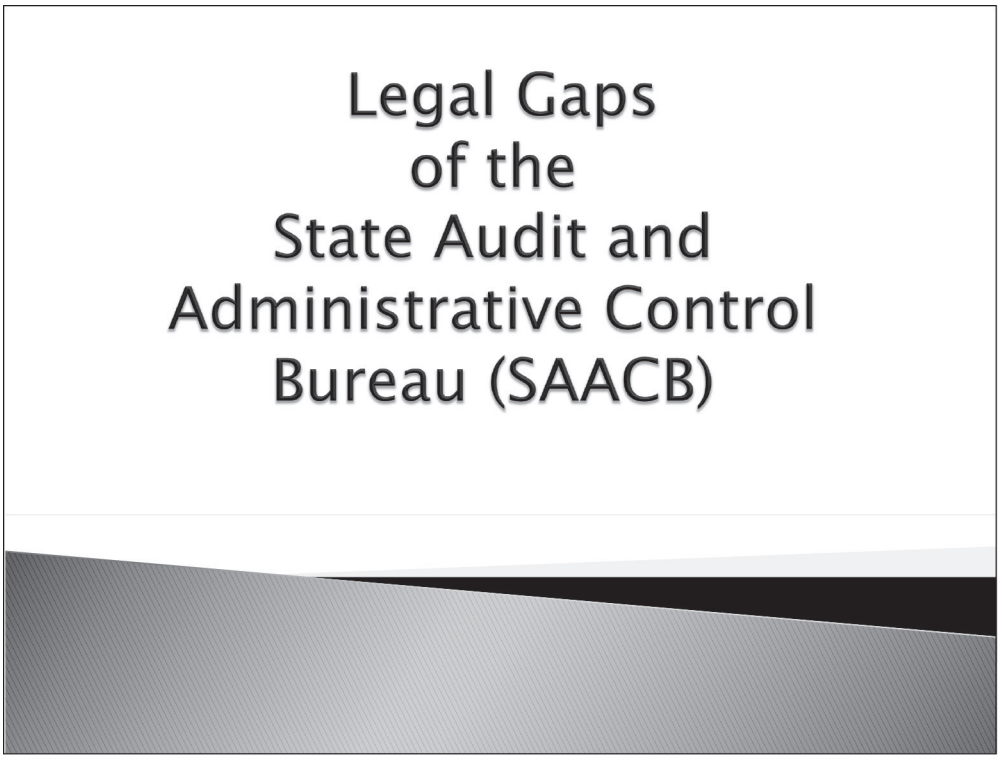
1. Yes
2. No

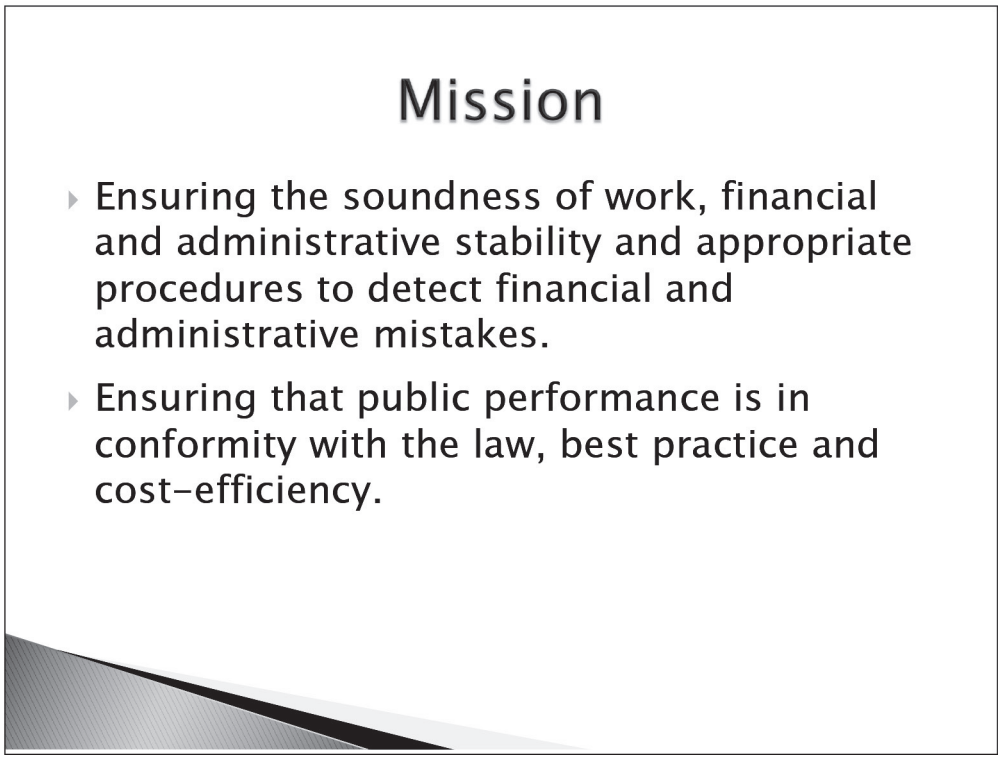
Question 7: Are there confidentiality-related measures to which SAACB is committed and which include planning, implementation and publication?

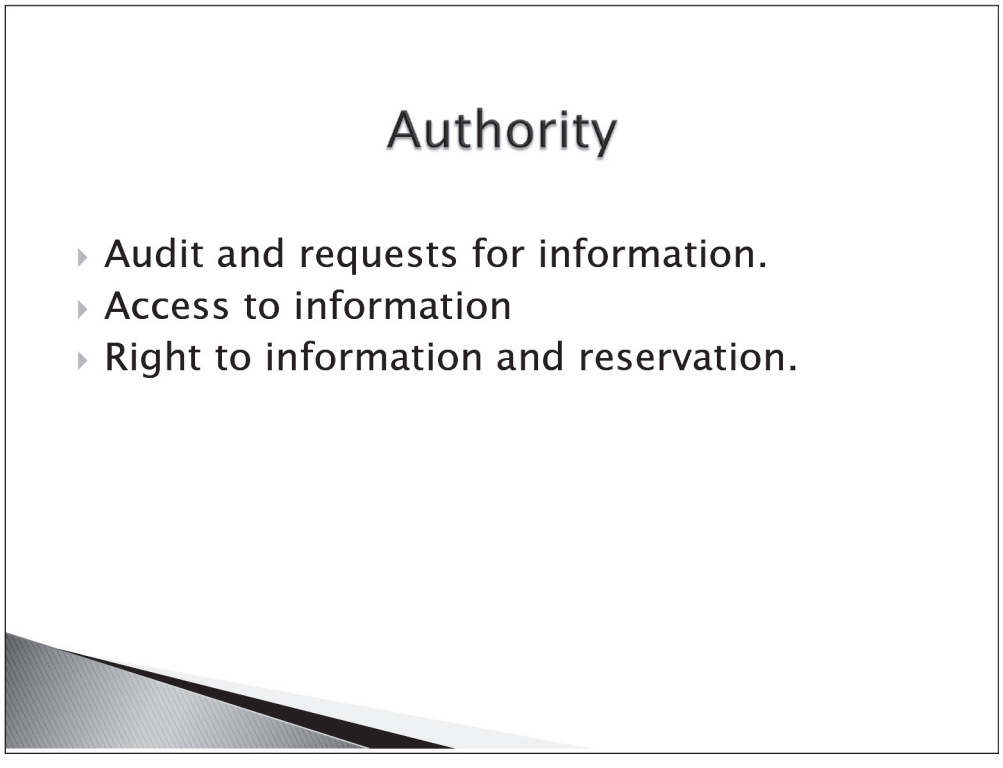
1. Yes
2. No
   - Law (planning, implementation and publication)
   - Implementation (planning, implementation and publication)

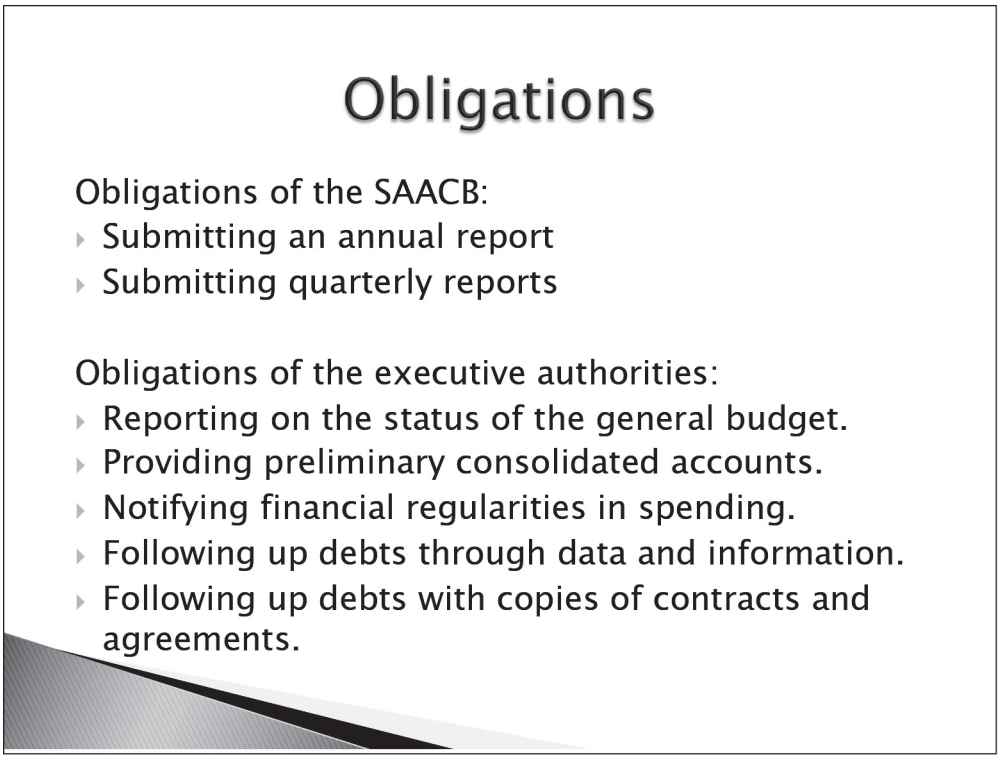
Trainer Resource L6.1

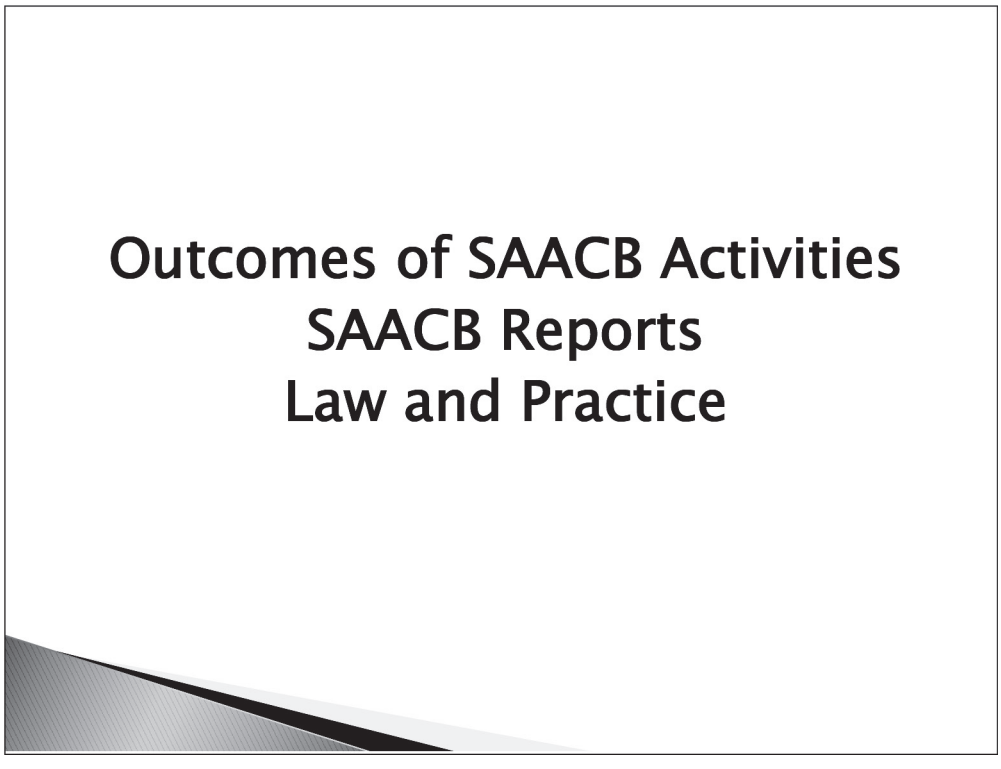
PowerPoint: Legal Gaps of Audit State Audit and Administrative Control Bureau (SAACB)








Obligations
Obligations of the SAACB:
Submitting an annual report
Submitting quarterly reports
Obligations of the executive authorities:
Reporting on the status of the general budget.
Providing preliminary consolidated accounts.
Notifying financial regularities in spending.
Following up debts through data and information.
Following up debts with copies of contracts and agreements.


Outcomes of SAACB Activities
SAACB Reports
Law and Practice

Security Agencies

- Subordination.
- Organisational charts.
- Budget.
- Financial affairs (expenditures/ revenues).
- Procurements (1998 Public Procurement Law No. 9).
- Procurement stages (planning, bidding, evaluation, awarding, referral, reception).
- Oversight of procurements.

Administrative Affairs

- Law of Service in the Palestinian Security Forces.
- Appointment.
- Promotion.
- Accountability.
- Disciplinary penalties, corrective penalties, military courts penalties.

Suggested resources

1. Andersson, Lena, Masson, Nicolas and Salah Aldin, Mohammad. *Guidebook: Strengthening Financial Oversight in the Security Sector*. Geneva: DCAF, 2011, Sections 3 & 4.
2. *The Security Sector Legislation of the Palestinian National Authority*. Geneva: DCAF, 2008, pages 77-91, pages 91-98.
3. *A Palestinian Legal Collection: Financial and Administrative Oversight in the Security Sector*. Geneva: DCAF, 2012, pages 16-23 (in Arabic language).
4. State of Palestine, State Audit and Administrative Control Bureau. *Laws and Regulations related to Financial Audit in Palestine*, 22 September 2014. http://saacb.ps/SaacbLaws.aspx

DCAF Head Office, Geneva
By Post:
Geneva Centre for the Democratic Control of Armed Forces (DCAF)
P.O.Box 1360
CH-1211 Geneva 1
Switzerland

For Visitors:
Chemin Eugène-Rigot 2E
1202 Geneva
Switzerland

Tel: +41 (0) 22 730 9400
Fax:+41 (0) 22 730 9405

www.dcaf.ch

DCAF Beirut

Gefinor Center - Block C - 6th Floor
Clemenceau Street
Beirut
Lebanon

Tel: +961 (0) 1 738 401
Fax: +961 (0) 1 738 402

مكتب بيروت

مركز جفينور - بلوك ج - الطابق السادس
شارع كليمنصو
بيروت
لبنان

تلفون: ٤٠١ ٧٣٨ ١ (٠) ٩٦١+
فاكس: ٤٠٢ ٧٣٨ ١ (٠) ٩٦١+

DCAF Ramallah

Al-Maaref Street 34
Ramallah / Al-Bireh
West Bank
Palestine

Tel: +972 (2) 295 6297
Fax: +972 (2) 295 6295

مكتب رام الله

شارع المعارف ٣٤
رام الله / البيرة
الضفة الغربية
فلسطين

تلفون: ٦٢٩٧ ٢٩٥ (٢) ٩٧٢+
فاكس: ٦٢٩٥ ٢٩٥ (٢) ٩٧٢+

DCAF Tunis

14, Rue Ibn Zohr – 1er étage
Cité Jardins
1082 Tunis
Tunisie

Tel: +216 71 786 755
Fax: +216 71 286 865

مكتب تونس

١٤ نهج ابن زهر
شقة عدد ١ - الطابق الأول
الحدائق ١٠٨٢
تونس

تلفون: ٧٥٥ ٧٨٦ ٧١ ٢١٦+
فاكس: ٨٦٥ ٢٨٦ ٧١ ٢١٦+