SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

risk assessment

José Viegas Ribeiro
IGF, Portugal
SIGMA

PEM PAL workshop
Lviv, 8/9 October 2012

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

outline

1. Why risk assessment

2. Risk assessment at macro level (per Ministry) – a key tool for audit planning in Portugal

3. Risk assessment at micro level (per organization) - a key tool for auditing the internal control systems

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Risk assessment – Why ?

- Basis for the audit strategy
- Planning audit work (risk-based plan)
- Prioritise audit work, consistent with the organization's goals
- Mitigate the risks ASAP
- Increase audit efficiency/*focus* on risk areas
- Consider expectations of senior management, the board and other stakeholders

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Why risk assessment – ISA 315 and 330

ISA 315 gives an overview of the procedures that the auditor should follow in order to obtain a sufficient understanding to assess audit risks, and these risks must then be considered when designing the audit plan.

Of central importance to both ISA 315 and ISA 330 is the recognition that assessing risks is at the core of the audit process, and these two ISAs specify that the auditor is required to obtain an understanding of the key risks (sometimes described as 'significant' risks) relevant to the financial statements.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

audit standards

- ISA 315 - Identifying and assessing the risks of material misstatement through understanding the entity and its environment
- ISA 330 - The Auditor's responses to assessed risks

- IASB Performance standard 2010 - Planning

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

A- Risk assessment at macro level (Ministry) – a key tool for audit planning in Portugal

Steps:

1 - Understanding the entities and their functions, business and environment; gathering information (also using in house information and available recent data)

2 - Risk assessment check list (per each organization of each Ministry)

3 – Assessment of the results (per organization of each Ministry)

4 – Setting priorities for the audit annual plan

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

1st step – Understanding the entity and its business/environment and gathering information

ISA 315 gives detailed guidance about the understanding required of the entity and its environment by auditors, including the entity's internal control systems.

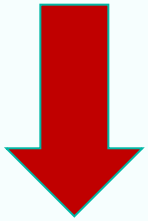
Understanding of the entity and its environment is important for the auditor in order to help identify the risks, to provide a basis for designing and implementing responses to assessed risk (see also ISA 330, *The Auditor's Responses to Assessed Risks*), and to ensure that sufficient appropriate audit evidence is collected.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

2nd step – Risk assessment check list

Risk assessment
summary table with the key risk factors



Risk assessment
detailed table (risk factors break down)

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

2nd step – Risk assessment summary table

quantitative assessment

RISK FACTORS		Maximum Score
F1	Nature of the Department/Unit	2
F2	Materiality	3
F3	Expenditure Structure	10
F4	Own Resources	10
F5	European Union financing	8
F6	Debt management	7
F7	Financial and Economic indicators	10
F8	Internal Control	28
F9	Results of previous audits	22
	MAXIMUM SCORE	100

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

2nd step – Risk assessment check list

- Check list as a section of the audit manual
- check list detailing each risk factor, with a maximum score per factor *(example of the check list shown in a separate file)*
- applied to each organization of each Ministry (eg, general directorates, agencies, departments)
- Input from senior management (eg, interviews or revising management documentation)
- basis for audit priorities and annual planning

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

2nd step – Risk assessment (included in the score of factor F8)

Probability assessment	Level	
Not verified in previous audits	1	Ocasional
Verified in 5% of the expenditure audited in previous audits	2	Possible
Verified in more than 5% of the expenditure audited in previous audits	3	Frequent

Impact assessment	Level	
Does not afect expenditure	1	Low
Does not afect expenditure in a material way	2	Moderate
Affects expenditure in a material way	3	High

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

3rd step – Risk assessment results

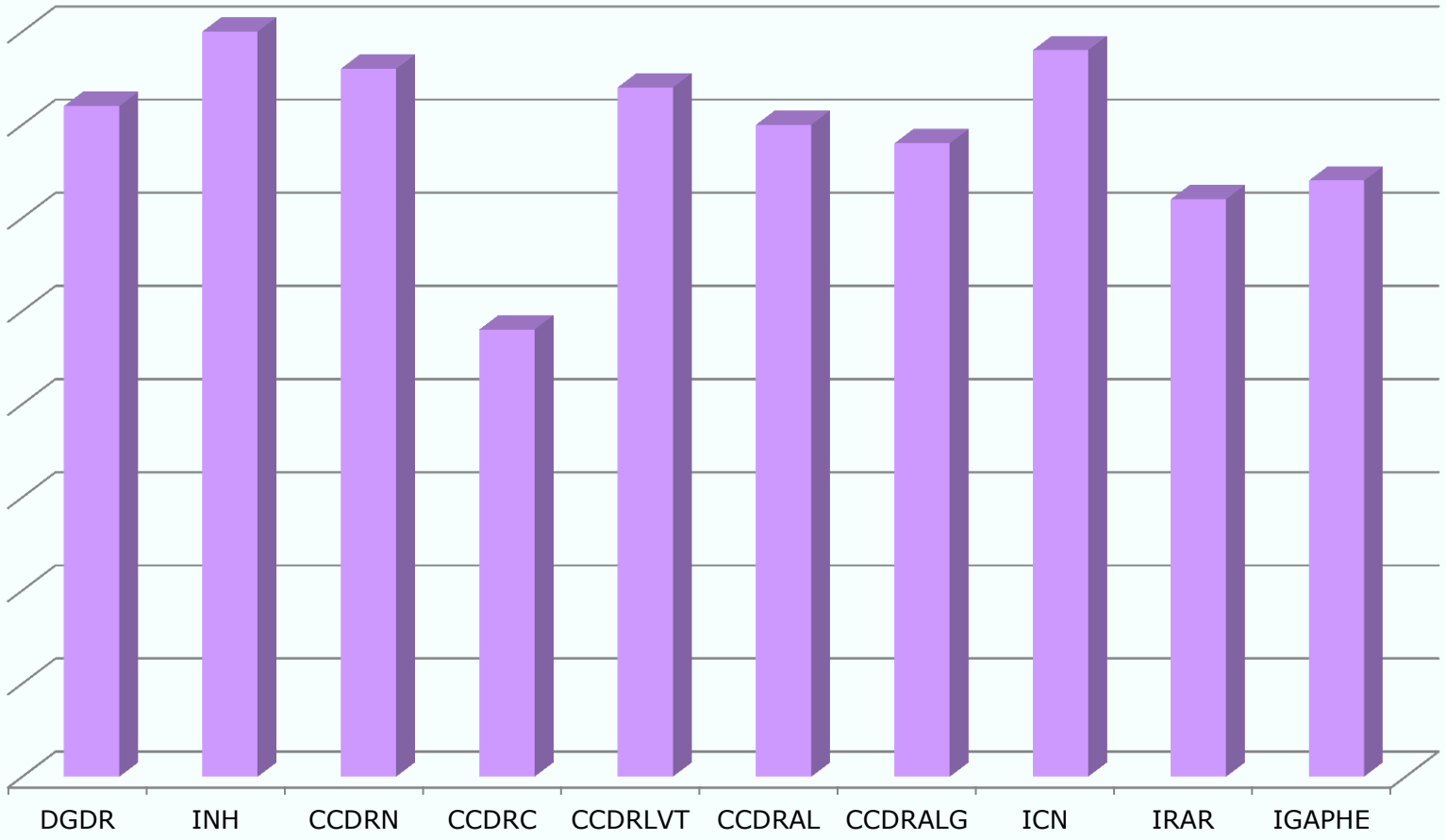
from quantitative to qualitative assessment

Assessment	Lower Limit	Higher Limit
Very Low	20	36
Low	36	52
Medium	52	68
High	68	84
Very High	84	100

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

3rd step – Risk assessment results



3rd step – Risk assessment results

another method – European Commission final audit systems assessment

Verifications carried out should allow the auditor to issue a final audit opinion on the internal control system

- **Work Well**: if key risks are properly addressed by controls operating effectively
- **Work, but minor improvements are needed**: if key risks are properly addressed by controls operating effectively, with some minor exceptions
- **Work, but important improvements are needed**: if some risks are addressed by controls, that in relevant situations are weak and not operating effectively
- **Does not work**: major key risks are not properly addressed by controls and/or key controls are not operating effectively

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

B - Risk assessment at micro level (per organization)

a key tool for auditing the internal control systems

1 – focus on key internal control areas (COSO based)

2 - internal control check list (key controls)

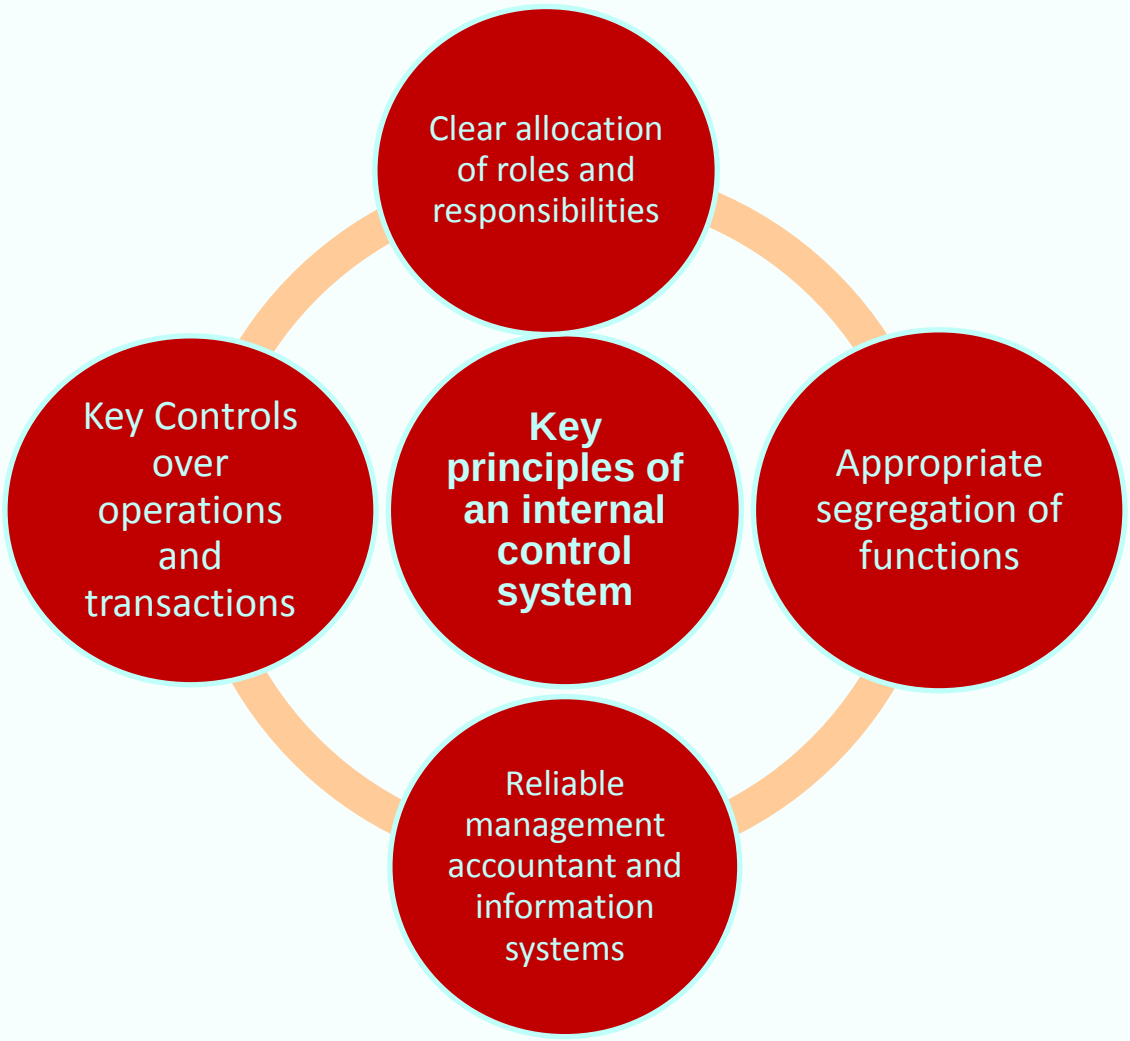
3 – guidance note for the auditors – how to use

4 – final assessment of the results (clear indication of the high risk internal control areas – important for the management, the board and the audited organization)

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

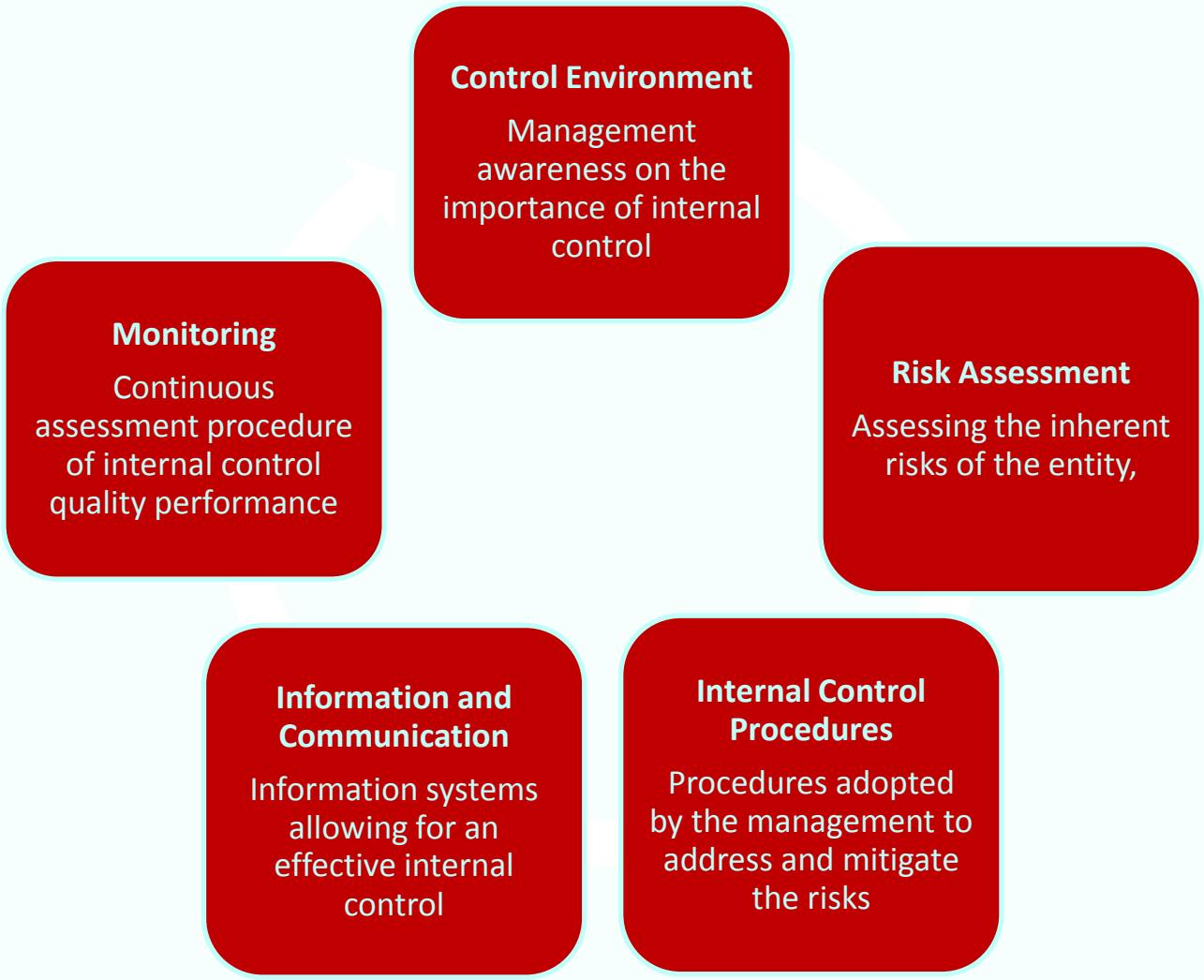
Terms of Reference



SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

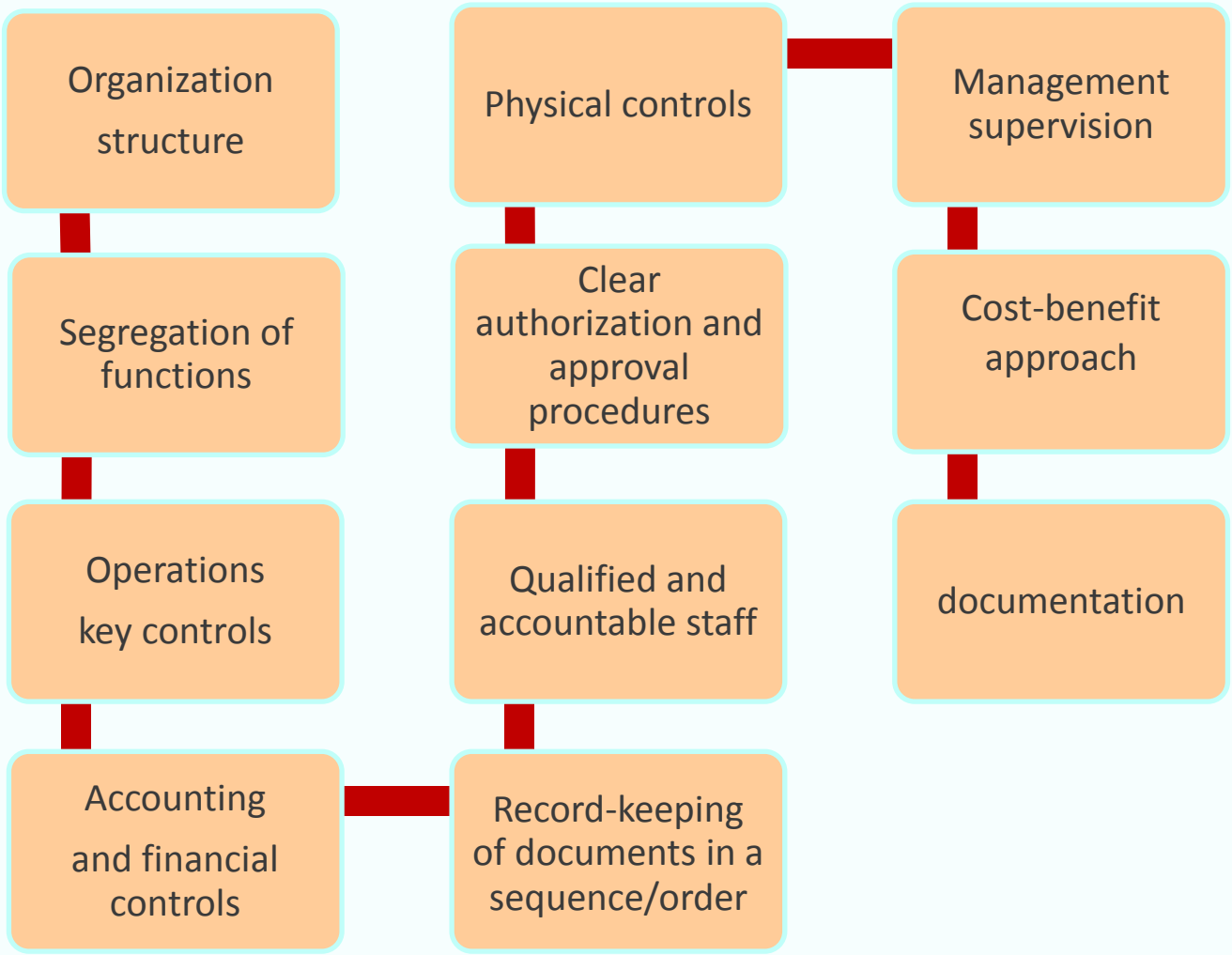
Terms of Reference - Internal control components



SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

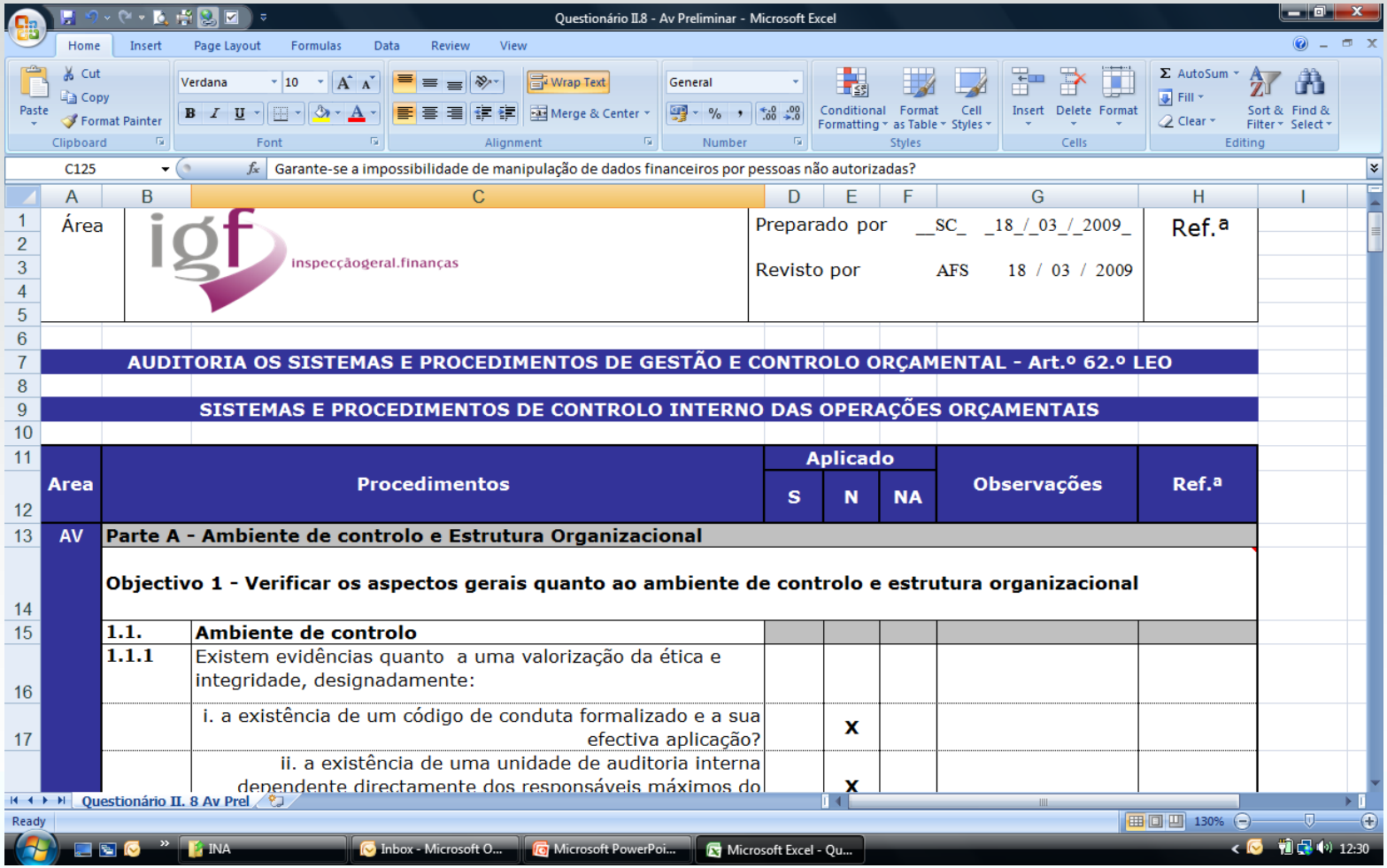
Terms of Reference – internal control elements



SIGMA

focus on Internal control

example of a check list



Questionário II.8 - Av Preliminar - Microsoft Excel

Home | Insert | Page Layout | Formulas | Data | Review | View

Cell C125: Garante-se a impossibilidade de manipulação de dados financeiros por pessoas não autorizadas?

	A	B	C	D	E	F	G	H	I
1	Área		igf inspecçãogeral.finanças		Preparado por	__SC_	_18_/_03_/_2009_	Ref.ª	
2									
3					Revisto por	AFS	18 / 03 / 2009		
4									
5									
6									
7	AUDITORIA OS SISTEMAS E PROCEDIMENTOS DE GESTÃO E CONTROLO ORÇAMENTAL - Art.º 62.º LEO								
8									
9	SISTEMAS E PROCEDIMENTOS DE CONTROLO INTERNO DAS OPERAÇÕES ORÇAMENTAIS								
10									
11	Area	Procedimentos		Aplicado			Observações	Ref.ª	
12				S	N	NA			
13	AV	Parte A - Ambiente de controlo e Estrutura Organizacional							
14		Objectivo 1 - Verificar os aspectos gerais quanto ao ambiente de controlo e estrutura organizacional							
15		1.1.	Ambiente de controlo						
16		1.1.1	Existem evidências quanto a uma valorização da ética e integridade, designadamente:						
17			i. a existência de um código de conduta formalizado e a sua efectiva aplicação?		X				
			ii. a existência de uma unidade de auditoria interna dependente directamente dos responsáveis máximos do		X				

Questionário II. 8 Av Prel

Ready

130%

INA | Inbox - Microsoft O... | Microsoft PowerPoi... | Microsoft Excel - Qu...

12:30

OECD

SIGMA

focus on Internal control

example of a detailed internal control check list (key controls)

igf inspecçãogeral.finanças

Instituto Nacional da Propriedade Industrial

ANEXO I

AVALIAÇÃO DE PROCESSOS E CONTROLOS-CHAVE DE ÁREAS DO SISTEMA DE CONTROLO-INTERNO

ÁREA ⇨	AC - AMBIENTE DE CONTROLO					
PROCESSOS		**O que se pretende avaliar?**	**CONTROLOS-CHAVE**	**Classif.**		**NOTAÇÃO**
AC1	Integridade e ética	Integridade e valores éticos - em que medida é que a falta de formulação e comunicação destes valores afecta a concepção, administração e monitorização dos outros componentes do sistema de controlo interno? Filosofia e estilo operacional da gestão – As atitudes e acções dos altos dirigentes perante o relato financeiro, o processamento da informação, as funções contabilísticas e o pessoal são as adequadas ao prosseguimento das actividades e cumprimento dos objectivos de forma económica, eficaz e eficiente? As suas atitudes cumprem com os princípios da gestão pública da transparência, equidade, legalidade e *accountability* ? Os riscos operacionais são conhecidos e tratados?	Carta de missão	Sim ☐ Não ☐	4	BOM
			Código de ética	Sim ☐ Não ☐	3	SUFICIENTE
			Cultura organizacional	Sim ☐ Não ☐	4	BOM
			Gestão do risco	Sim ☐ Não ☐	4	BOM
					4	BOM
AC2	Estratégia e operacionalização das actividades	Planeamento e monitorização de resultados – Existe uma estratégia delineada através da comunicação da missão, valores e visão? As actividades são planeadas, executadas, controladas e monitorizadas para atingir os objectivos da entidade? Os objectivos do QUAR estão alinhados com a estratégia? Existe um processo de cascata *top-down* e *bottom-up* de estabelecimento de objectivos desde os organizacionais aos individuais? Os instrumentos e fontes de dados são confiáveis? Os Relatórios de Actividades são publicados dentro dos prazos? Contendo toda a informação, designadamente a auto-avaliação e uma análise do desempenho do organismo?	Planeamento	Sim ☐ Não ☐	4	BOM
			Monitorização	Sim ☐ Não ☐	4	BOM
					4	BOM
AC3	Estrutura organizacional e sistema de informação	Estrutura organizacional e sistemas de suporte – A estrutura organizacional proporciona a estrutura conceptual na qual as actividades são planeadas, executadas, controladas e monitorizadas para atingir os objectivos? Os sistemas de informação são adequados às necessidades operacionais? A estrutura facilita a comunicação interna?	Organização	Sim ☐ Não ☐	4	BOM
			Comunicação interna	Sim ☐ Não ☐	3	SUFICIENTE
			Sistema de informação	Sim ☐ Não ☐	4	BOM
					4	BOM

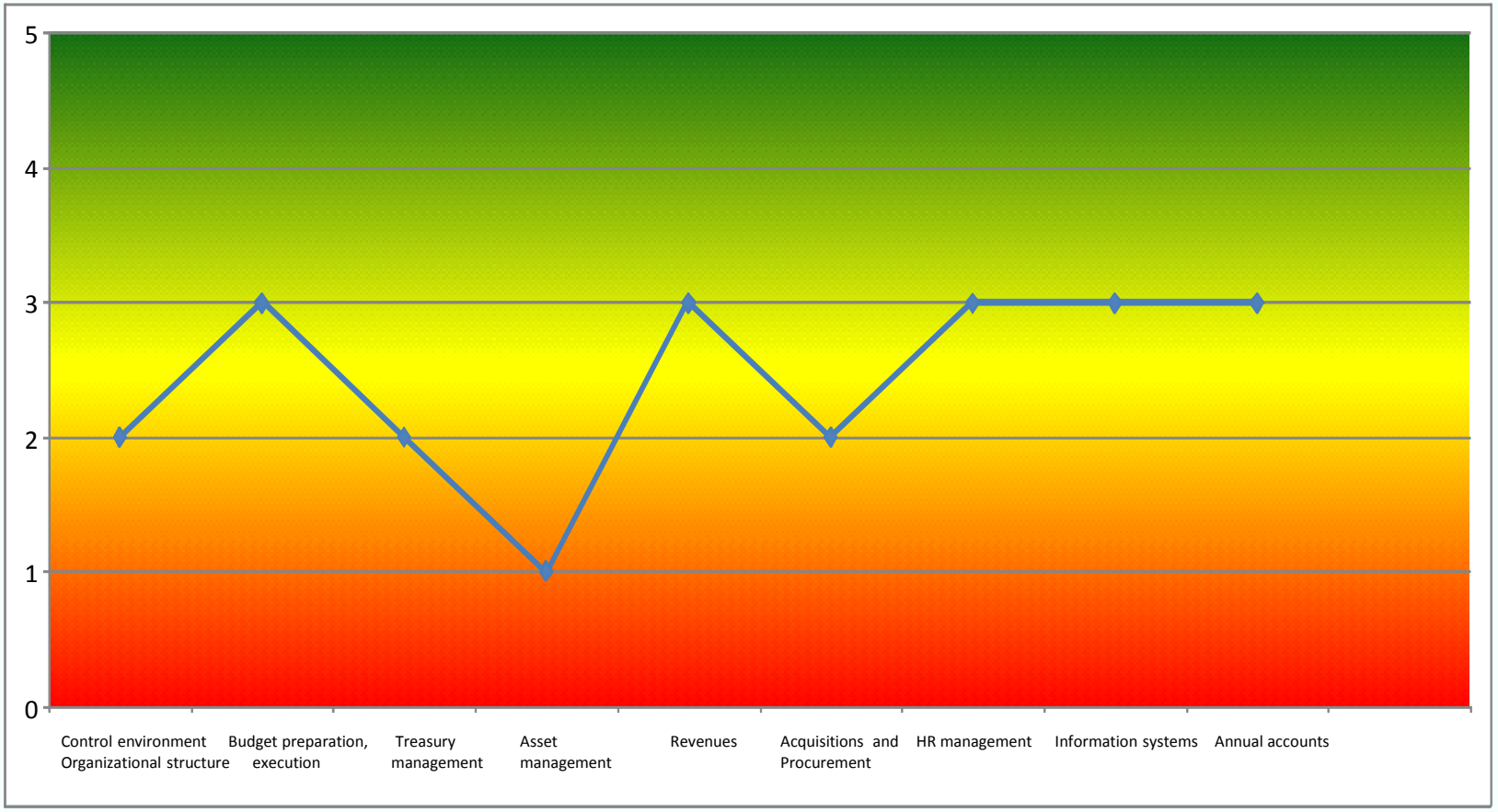
OECD

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

final assessment table

an example for internal control areas



0 – Non existent 1 – Very Poor 2 – Poor 3 – Sufficient 4 – Good 5 – Excellent

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

RA areas to follow and improve - I

- RA is key for the auditor - need to have a deep and comprehensive understanding of the audited organization business and environment *(auditor must not feel "lost in the forest", but going straight to the "right trees")*

- Without a robust RA it's not possible to have a good planning, and without a good planning it's very difficult to have an effective and valuable audit report

- Need to improve the reliability of the inherent risk assessment, in particular in organizations with complex and composite financial transactions and several sources of funding

OECD

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

RA areas to follow and improve - II

- Example of operations of this nature, which are often difficult to the auditors – revenue generating projects, financial engineering operations, state aid operations
- Also public procurement, concessions and PPP's are areas of high materiality and complexity and increasing difficulties in RA (both inherent and control risk), requiring specific knowledge and *fine tuning* RA
- Example of the most common findings requiring experienced auditors – additional works, modification of the physical object of the contract and artificial splitting of the contracts

OECD

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

RA areas to follow and improve - III

- From our experience, public procurement, concessions and PPP's are responsible for some of the most material and important audit findings (also deviations and errors)

- accordingly, we decided to improve the risk assessment and also to develop a separate and very detailed check list to audit public procurement, concessions and PPP's (that was included as an additional annex to the audit manual – other high risk areas will be subject to specific check lists as well)

- auditing management information systems, running in high complex IT platforms (even when not a IT audit, IT capabilities are very useful).