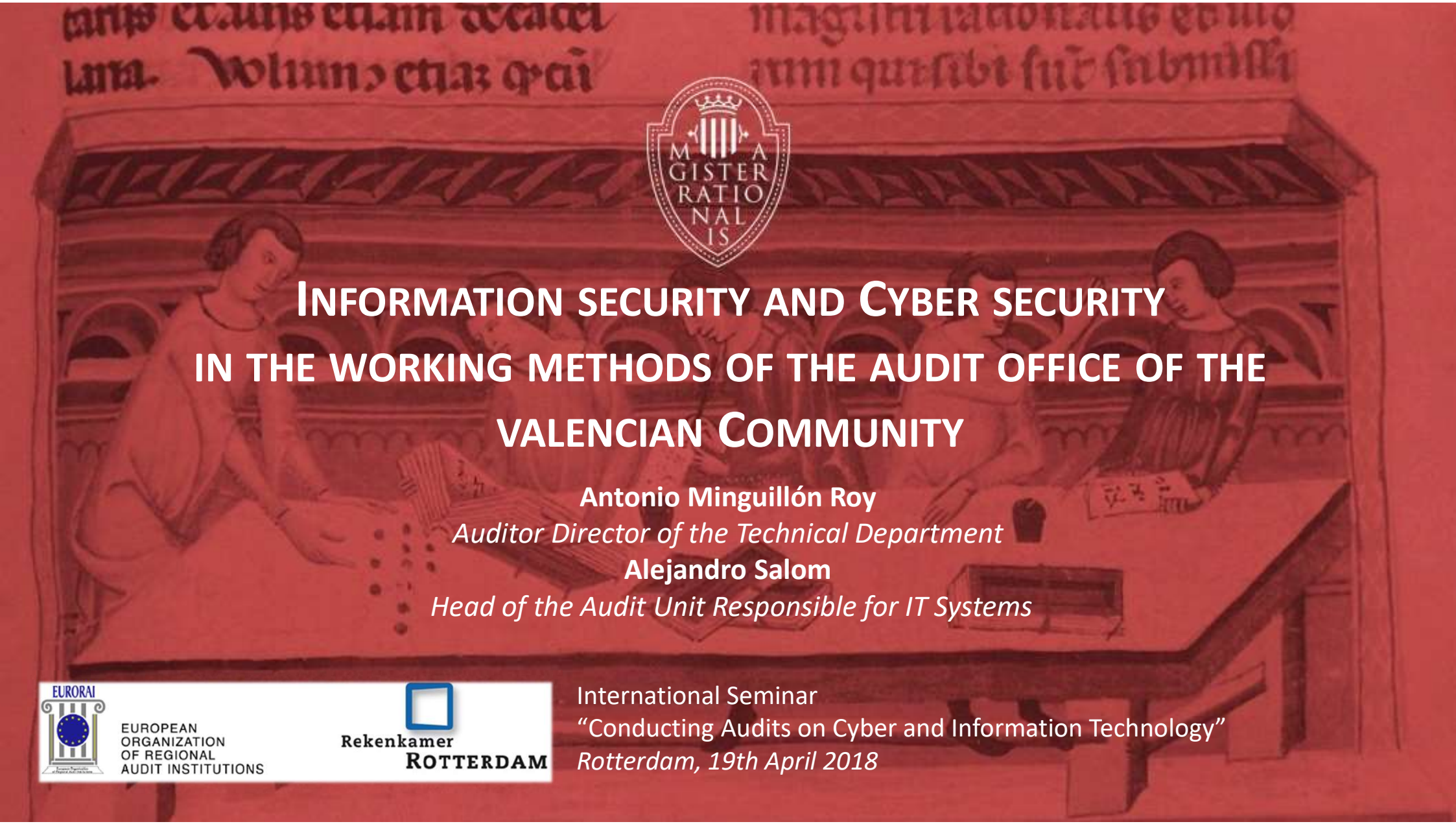


INFORMATION SECURITY AND CYBER SECURITY IN THE WORKING METHODS OF THE AUDIT OFFICE OF THE VALENCIAN COMMUNITY

Antonio Minguillón Roy

Auditor Director of the Technical Department

Alejandro Salom

Head of the Audit Unit Responsible for IT Systems

EUROPEAN ORGANIZATION OF REGIONAL AUDIT INSTITUTIONS

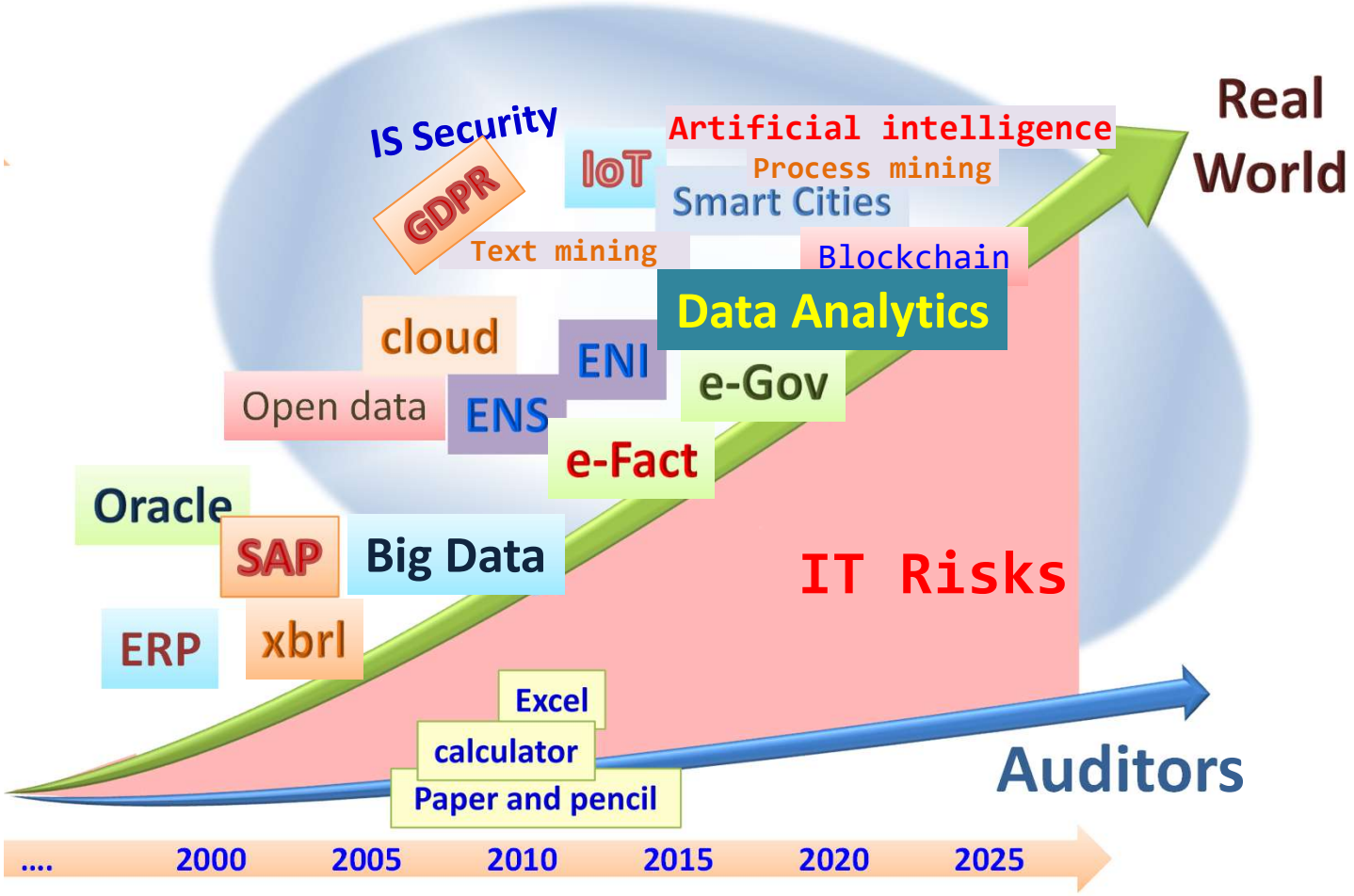
Rekenkamer ROTTERDAM

International Seminar

"Conducting Audits on Cyber and Information Technology"

Rotterdam, 19th April 2018

The Digital Breach



"… For the most part, auditors use legacy processes that are not much different from those of fifty years ago, except that they have been computerized.

The emphasis has been on improving efficiency, and while effectiveness has improved as well, there has not been the quantum leap that technology can enable".

AICPA,
White Paper
Agosto 2014

Main challenges to be faced by RAIs

- Electronic administration
- Big Data
- Cyber security
- Audit Data Analytics
- Data visualization
- Cognitive technology (AI)

Digital Transformation *(Revolution?)*

- Fight against fraud and corruption
- More useful and understandable reports
- Quality of audits
- Introduce the new technical standards
- Performance and environmental audits

RISKS

OPPORTUNITIES

ACTION

Importance of cyber issues

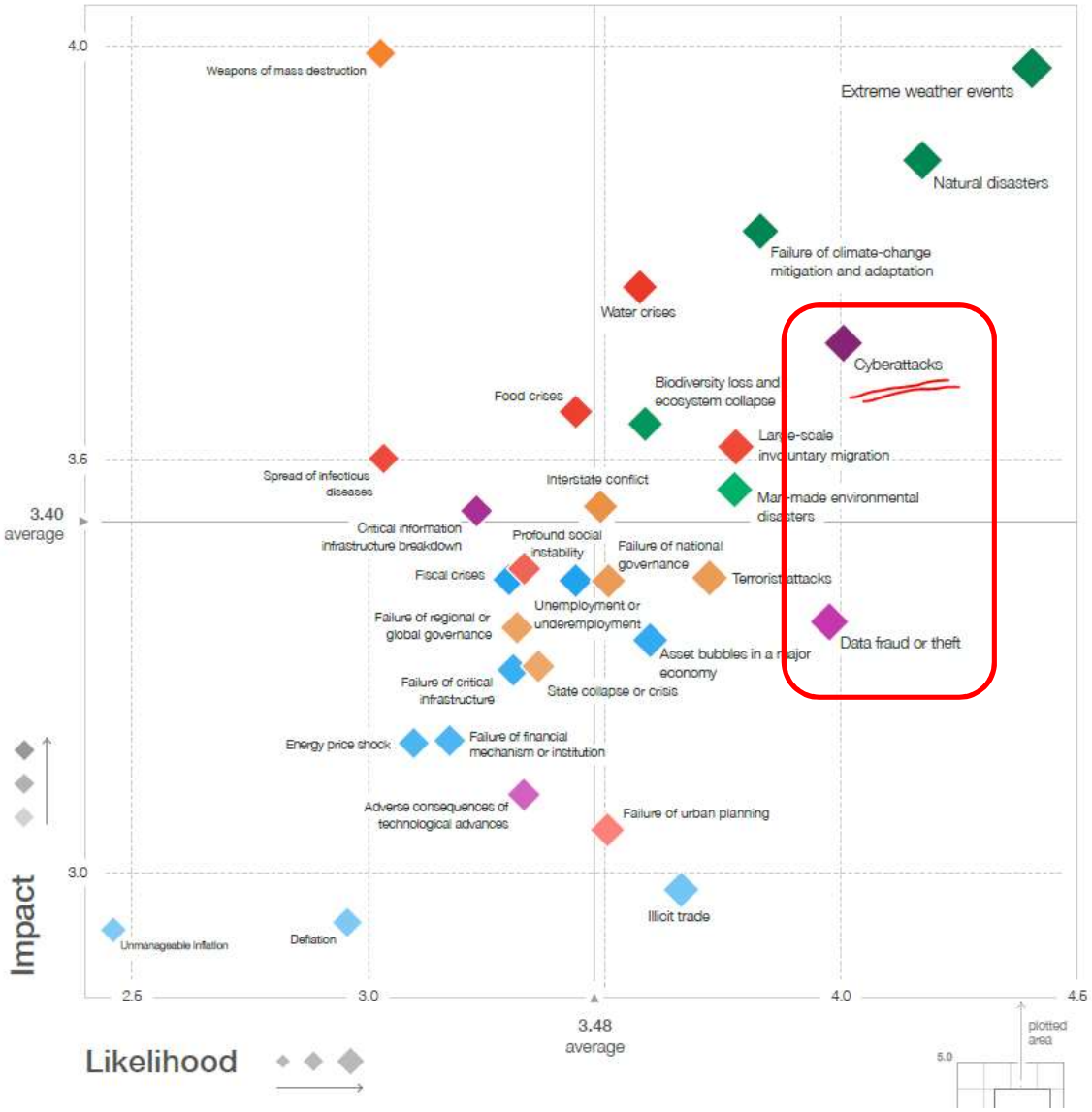
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

The Global Risks Report 2018
13th Edition

Figure I: The Global Risks Landscape 2018



Cyber threats

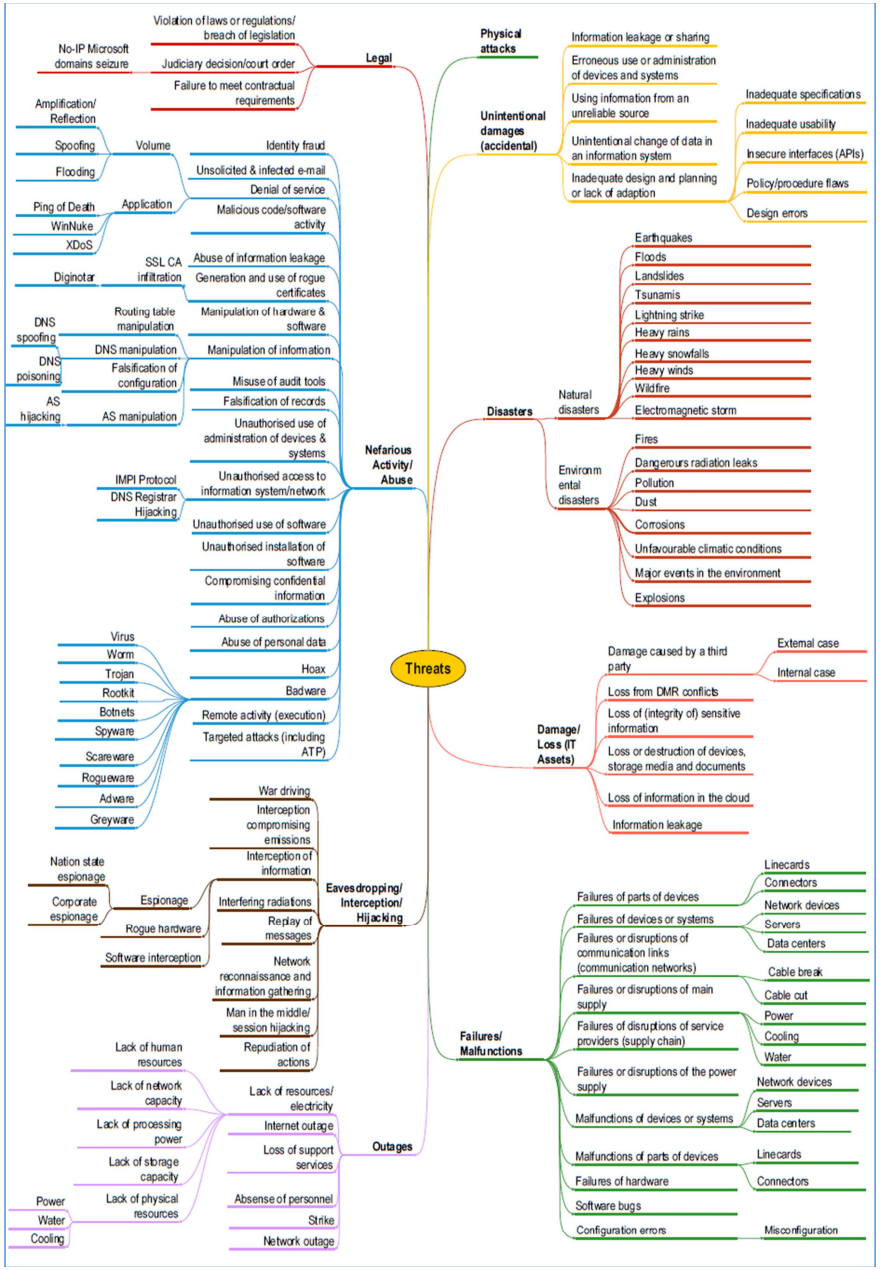
ENISA Threat Taxonomy

A tool for structuring threat information

INITIAL VERSION
1.0
JANUARY 2016

www.enisa.europa.eu

European Union Agency For Network And Information Security



Cyber security: NIS Directive

"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. [...] Cyber-attacks know no borders and no one is immune. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks."

European Commission President Jean-Claude Juncker, State of the Union Address, 13 September 2017

Resilience, Deterrence and Defence: Building strong cybersecurity in Europe

DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 6 de julio de 2016

relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

REGLAMENTO DE EJECUCIÓN (UE) 2018/151 DE LA COMISIÓN

de 30 de enero de 2018

por el que se establecen normas para la aplicación de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo en lo que respecta a la especificación de los elementos que han de tener en cuenta los proveedores de servicios digitales para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información, así como de los parámetros para determinar si un incidente tiene un impacto significativo

Action Areas / Answers

ACTION:

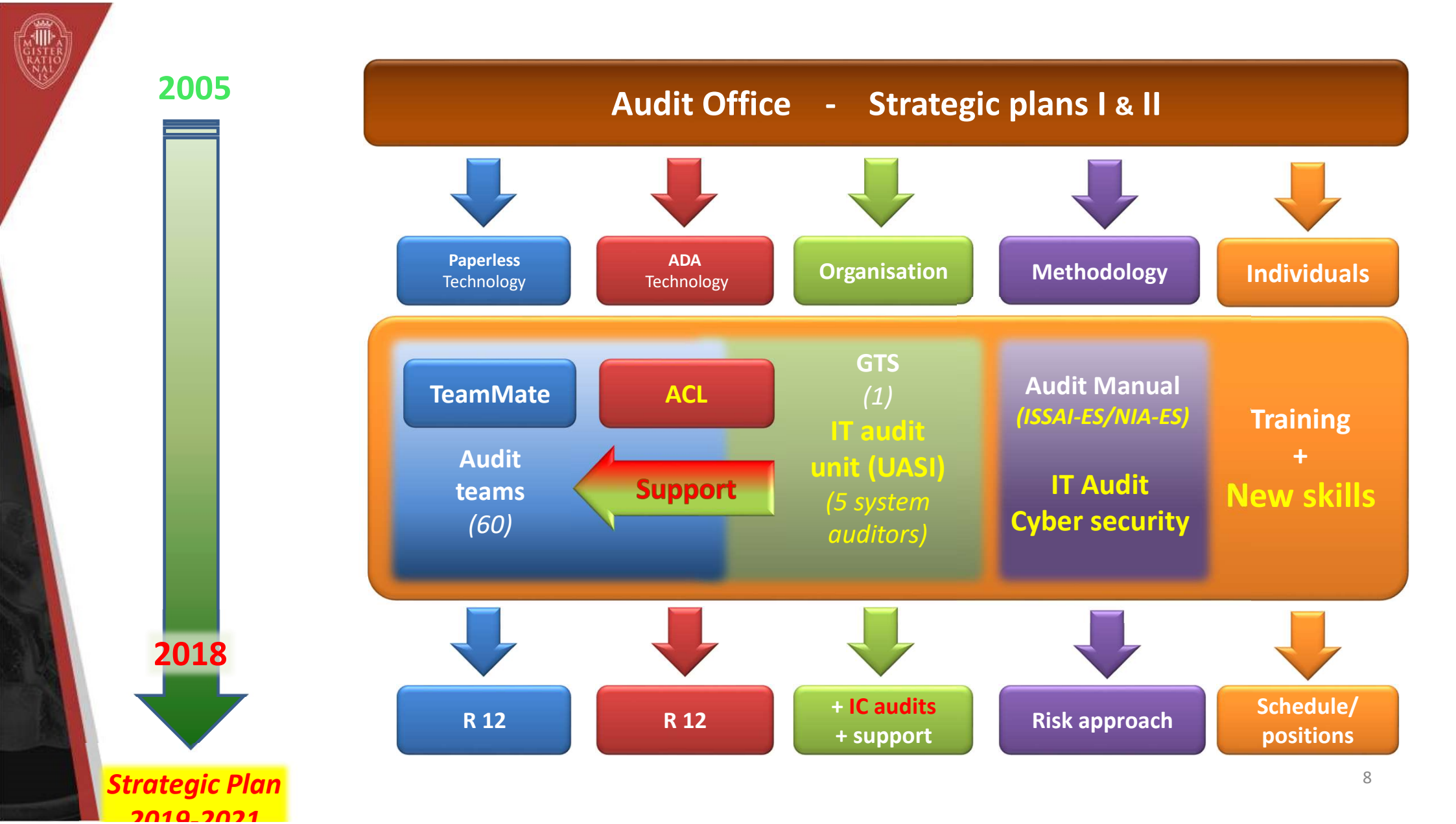
- Technical standards (ISA+ISSAI)
- Guidelines (GPF-OCEX)
- Training of current staff
- New technological skills
- Integrated teams
- Cyber security
- Techniques for digital analysis
- Visualization techniques
- Cognitive technologies (AI)
- IT auditing

Process reengineering

*"The challenges of the immediate future (disruptive technology changes, among others) require a **proactive response** from auditors."*

"Transformation will also require new areas of knowledge as well as indispensable introduction of intelligent systems in processes (Big Data analytics, predictive programmes and cyber security solutions)."

Daniel Faura
10/10/2016


2005
2018
Strategic Plan
2019-2021
Audit Office - Strategic plans I & II
Paperless Technology
ADA Technology
Organisation
Methodology
Individuals
TeamMate
ACL
Audit teams (60)
Support
GTS (1) IT audit unit (UASI) (5 system auditors)
Audit Manual (ISSAI-ES/NIA-ES)
IT Audit
Cyber security
Training + New skills
R 12
R 12
+ IC audits + support
Risk approach
Schedule/ positions

New audit guides (ASOCEX)

ISSAI 5300

INTOSAI

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5300: Directrices de auditoría de tecnologías de la Información

Referencia: ISSAI 5300 Directrices sobre auditoría de TI, aprobada en el XXII INCOSAI, en diciembre de 2016

Directrices sobre Auditoría de TI

IAS 315

Guía práctica de fiscalización de los OCEX

GPF-OCEX 1316: El conocimiento requerido del control interno de la entidad

ANEXO 1: Análisis del control interno en un entorno informatizado

(Manual de procedimientos de fiscalización de regularidad del Tribunal de Cuentas, apartado 5.3)

La revisión de
la actividad fi

MANUAL DE LA IDI Y DEL WGITA SOBRE AUDITORÍA DE TI PARA LAS ENTIDADES FISCALIZADORAS SUPERIORES

IAS 500

Guía práctica de fiscalización de los OCEX

GPF-OCEX 1500: Evidencia de auditoría

Anexo 2 Consideraciones sobre la evidencia electrónica de auditoría

"Emerging technology, and the challenges it brings to organizations and industries, presents many possibilities for the accountancy profession.

*Over the coming years, we are going to need to **adapt to** technological disruption, harness artificial intelligence, and provide **guidance** on cybersecurity".*

Olivia Kirley,
IFAC President

23/8/2016

New audit guides (ASOCEX)

Guía práctica de fiscalización de los OCEX Draft

GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica

Refe[illegible]

Guía práctica de fiscalización de los OCEX Draft

GPF-OCEX 5340: Los controles de aplicación: qué son y cómo revisarlos

Referencia: ISSAI-ES 5300, GPF-OCEX 5000 y GPF-OCEX 1315

Borrador elabo

Guía práctica de fiscalización de los OCEX Draft

GPF-OCEX 5370 Guía para la realización de pruebas de datos

Referencia:

Borrador de 01,

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa

Referencia: GPF-OCEX 1315, 1500 y 5300

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 27/11/2017

Guía práctica de fiscalización de los OCEX Draft

GPF-OCEX 5313 Revisión básica de ciberseguridad

Referencia: GPF-OCEX 5311, Esquema Nacional de Seguridad, CIS Controls IS Audit/Assurance Program de ISACA, CIS Controls.

New skills for public auditors

Staff and teams specialising in:

- IT audit.
- Data Analytics, Big Data and Cloud analysis.
- Tools for data analysis and visualization.
- Cyber security.

Auditors in general:

- Should have a high level of technological know-how / technological expertise, deeper than the currently existing.
- Training actions for the current practitioners and future professionals addressed to the new needs should be established.

*"**A new type of audit requires a new type of auditor**.*

It will continue to be substantial that auditors have a sound understanding of the essentials of auditing.

But a wide range of advanced knowledge, including the use of analysis tools will be required ."

Thomas Davenport

2016

E-government and electronic evidence

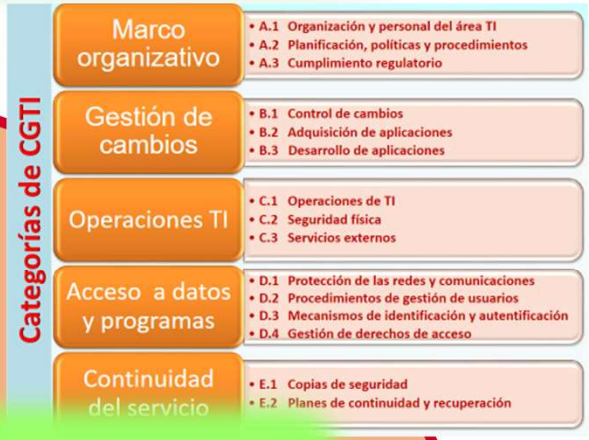
The information and data circulated, stored or processed in an information system must meet a number of characteristics (availability, authenticity, integrity, and confidentiality) to be ensured by security controls,
as requested by the Directive on Cyber security.

External auditors should review the internal controls designed and implemented in information systems to ensure that the data used as source of evidence meet such characteristics.

Cyber security: New Practical Audit Guide GPF-OCEX 5311

enisa

CIS Critical Security Controls



Guía práctica de fiscalización de los OCEX

GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa

Referencia: GPF-OCEX 1315, 1500 y 5300

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 27/11/2017

CCN Centro Criptológico Nacional

The purpose of this guide is to serve as an introduction to the challenge that cyber security presents in the activity performed by RAI auditors, raise awareness of its importance and set subsequent lines of development of a practical audit guide for RAIs (GPF-OCEX).

Main approaches of a cyber security audit

- Perform a **cyber security audit** which consists in a thorough analysis of the issue in a given agency/entity.

  This could be similar to a security audit required by the ENS or an audit that is aligned with ISACA methodology.

  Such a work involves very intense dedication of specialized staff both for the auditor and the audited body.

- The review of aspects directly linked to the significant areas audited when performing a **financial audit**.

  It will consist of the revision of the **ITGC** relates solely to the significant areas of the audited body for the purposes of the financial audit. **>>>> Practical Audit Guide for RAIs (GPF-OCEX 5330)**

- **The review of a set of basic cyber security controls**.

  It will enable to have an overall view of the situation of the audited entity and does not require the allocation of excessive specialised resources either from external auditor or from the audited body. **>>>> Practical Audit Guide for RAIs (GPF-OCEX 5313)**

MANUAL DE FISCALIZACIÓN 2018

Revisión CGTI	2850		
Revisión CGTI nivel básico	2857		
Revisión CGTI nivel básico. Cuestionario	2857.1		
Revisión CGTI nivel medio	2858		
Revisión CGTI nivel medio. Formulario	2858.1		
Revisión CGTI nivel alto	2859		
Revisión CGTI nivel alto. Cuestionario	2859.1		
Guía de fiscalización de área de gastos de personal	2861		
Documentar la comprensión del proceso de gestión de personal-nóminas	2861.1		
Guía de fiscalización del área de compras, gastos y proveedores	2862		

OCEX

GPF-OCEX 5330

GPF-OCEX 5330

ITGC

Organisational framework	•A.1 IT organisation and staff •A.2 Strategy •A.3 Policies and procedures •A.3 Regulatory compliance
Change management	• B.1 Acquisition of IT applications and systems • B.2 In-house development of IT applications • B.3 Change control
IT operations	• **C.1 Hardware and software inventory** C.5 Physical safety • C.2 Control procedures in operation C.6 Outsources services • **C.3 Incident management** **C.7 Secure configurations** • C.4 Antivirus **C.8 Audit Log monitoring**
Access to data and programmes	• D.1 Networks and communications protection • D.2 User management procedures • D.3 Identification arrangements and authentication mechanisms • **D.4 Controlled use of administrative privileges**
Service continuity	• E.1 Data backups • E.2 Continuity and recovery plans

Cyber security audit

CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Cyber security audit tests

Example CIS 4, Controlled use of administrative privileges

- Verify that there is a procedure ensuring that Administrator privileges are restricted to those cases where it is necessary and that administrator accounts are used only when necessary
- Verify if the activities of system administrators and users is recorded and reviewed.
- Review the lists of users with privileged access and check if the number of users is appropriate. Verify that the access is appropriate on the basis of the functions of the post.

Objectives of cyber security basic review

- Verify that the audited entities have a degree of resilience against cyber threats appropriate to the services they provide
- Improve the effectiveness of controls for cyber security in the audited entities

Information System Security: legal requirement for the Audit Office

DIARI OFICIAL
DE LA GENERALITAT VALENCIANA

Legislación consolidada

Última revisión 13.12.2017

Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura

Artículo 7. Función fiscalizadora

El ejercicio de la función fiscalizadora la realizará la Sindicatura de Comptes por los siguientes medios:

..

c) Para el desarrollo de sus funciones, la Sindicatura de Comptes podrá utilizar todos los medios adecuados para la consecución de sus objetivos, incluidos los de carácter informático y la contratación de expertos. El Consejo también podrá contratar con empresas consultoras o de auditoría para el cumplimiento de su programa anual de actuación.

Artículo 11. Medios de información para el ejercicio de la función fiscalizadora y consecuencias derivadas de la obstrucción al ejercicio de la actividad fiscalizadora

Uno. En el desarrollo de su función fiscalizadora, la Sindicatura de Comptes está facultada para:

a) Acceder a todos los expedientes y documentos de cualquier clase relativos a la gestión del sector público valenciano, incluyendo las bases de datos electrónicas en las que se archiven, así como para pedir, a los que estén sometidos a su control, cuantos escritos, informes o aclaraciones orales considere necesarios.

..

c) Efectuar las comprobaciones que considere oportunas en relación con los activos, pasivos, transacciones, procesos, control interno, etcétera.

d) Verificar la seguridad y fiabilidad de los sistemas informáticos que soportan la información económico-financiera, contable y de gestión.


M A
GISTER
RATIO
NAL
IS
Thank you!
Moltes gràcies!