NIS IMPLEMENTATION & CHALLENGES

CSC webinar – 11/06/2020

dns belgium

.be .vlaanderen .brussels

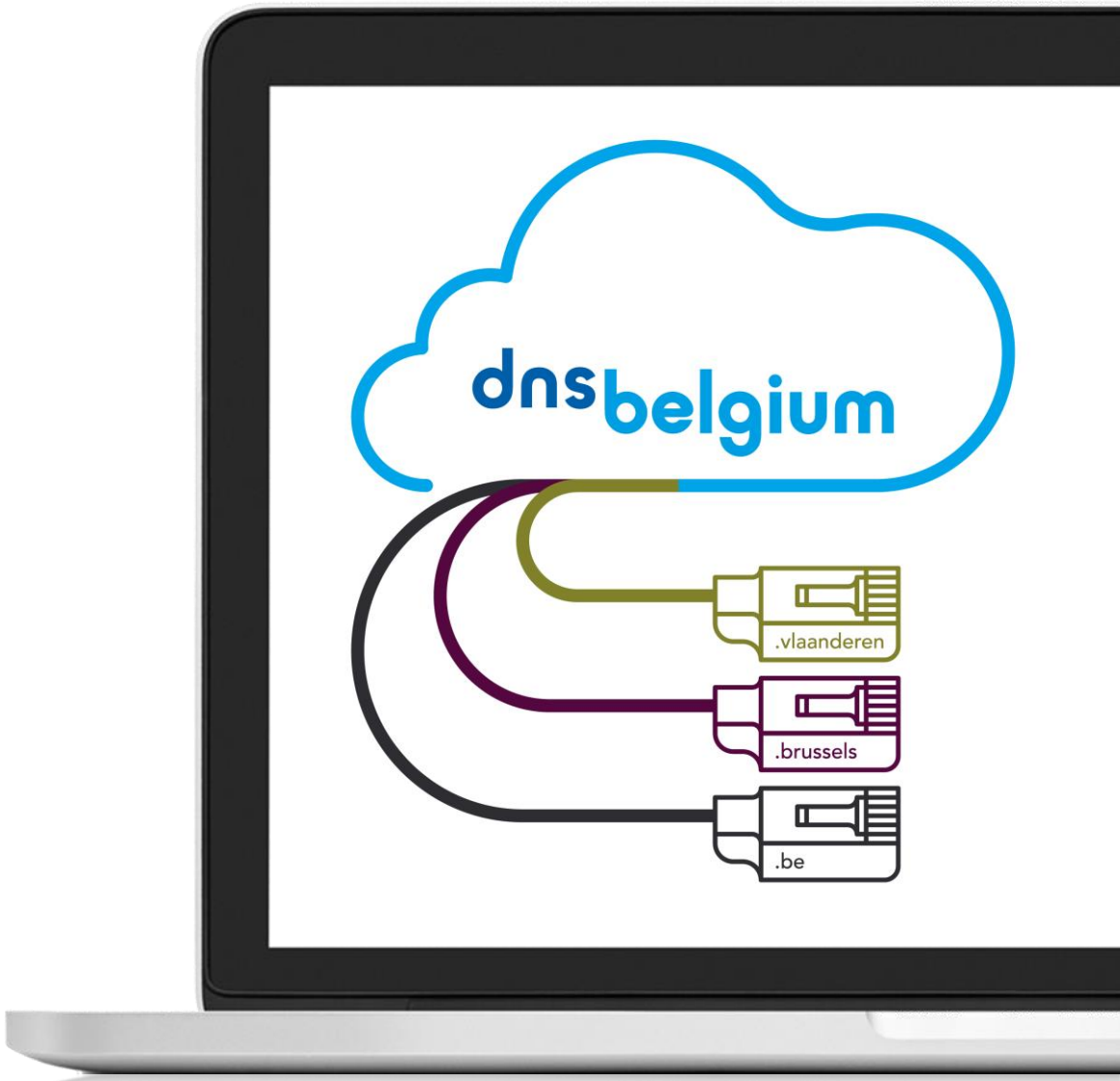
#0

INTRODUCING DNS BELGIUM

WHO WE ARE

Not-for profit organisation

Top Level Domain registry



ORGANISATION

Founding members

.AGORIA

BELTUG
Be Connected

ISPA

Effective members

be commerce GUARANTEED

fe web
federatie van webbedrijven

"B:A/M! BELGIAN ASSOCIATION OF MARKETING

comeos
for commerce and services

bereas

CORE TASKS

Registry database administration

Authoritative DNS operation

Lookup services (WHOIS/RDAP)

KEY FIGURES

≈ 35
Employees

20.000
New registrations per month

Domain names

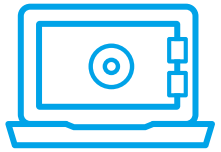
+1,65m .be
8.100 .brussels
6.500 .vlaanderen

400
Registrars

+7m €
Income

STRATEGIC OBJECTIVES

Operational excellence



Cyber security

Sustainability in its broad definition

Internal security

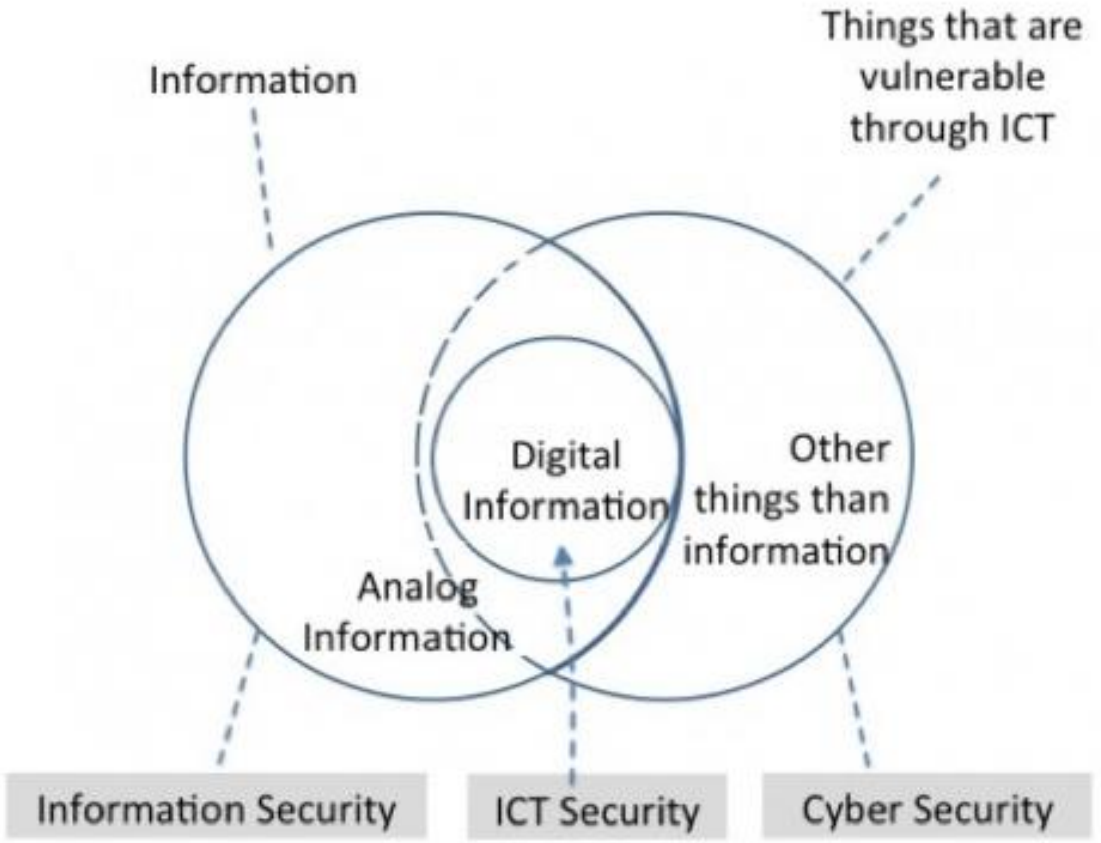
Legal compliance

State of the art corporate governance

#1

CONTEXT AKA ISO/IEC 27001 CHAPTER 4

INFORMATION SECURITY VERSUS CYBERSECURITY



Source:
https://www.ntnu.edu/ccis/

BEFORE 2016

- Very mature technical baseline but no management “framework”
- Implicit risk management
- No dedicated security officer
- Legal initiatives in the field of cybersecurity ?

- 01/2015 -> Start “ISO 27001” project

ANNEX II OF THE NIS DIRECTIVE

7. Digital Infrastructure		— IXPs
		— DNS service providers
		— TLD name registries

That's us

EU CYBERSECURITY ACT

- As a priority focus for future mandatory schemes: the sectors listed in Annex II of the NIS Directive (**which includes TLD registries)**

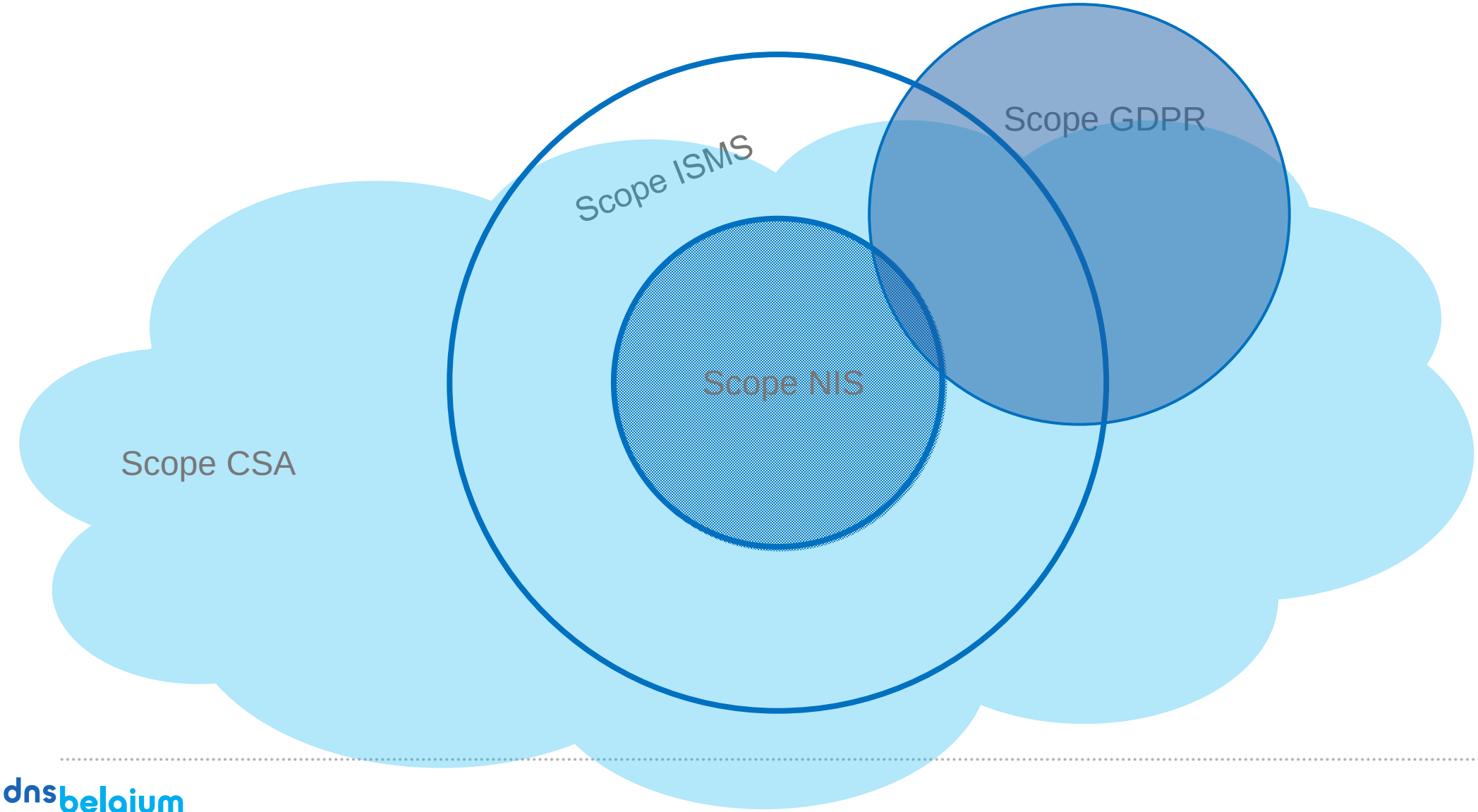
RELATIONSHIP WITH THE NIS DIRECTIVE

- EU Cybersecurity Act & NIS Directive are both part of the EU Cybersecurity Package
- They focus on complementary activities to drive greater cybersecurity resilience across the EU
- The NIS Directive emphasises cybersecurity incident preparedness and cooperative response planning and management
- The Cybersecurity Certification Framework focuses on cybersecurity certification schemes to ensure actors like service providers take reasonable cybersecurity measures upfront in their ICT products, services, and processes (‘security by design’)

#Challenge 1

SCOPING

SCOPE DRIFT?



NIS 2.0?

European Parliament

LEGISLATIVE TRAIN 05.2020

2 A EUROPE FIT FOR THE DIGITAL AGE

REVIEW OF THE DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS / BEFORE 2021-1

[DEPARTURES]

CONTENT

On 29 January 2020, the European Commission's new work programme was published. Under the second priority - 'A Europe fit for the digital age', the Commission announced its intention to launch a review of the Directive on security of network and information systems (NIS Directive), in order to 'further strengthen overall cybersecurity in the Union'. According to the work programme, the review should be adopted in the last quarter of 2020.

The current Directive on security of network and information systems entered into force in August 2016. Member States had to transpose it into their national laws by 9 May 2018. The directive lays down requirements regarding national cybersecurity capabilities of Member States; rules for their cross-border cooperation; and requirements regarding national supervision of operators of essential services and key digital service providers.

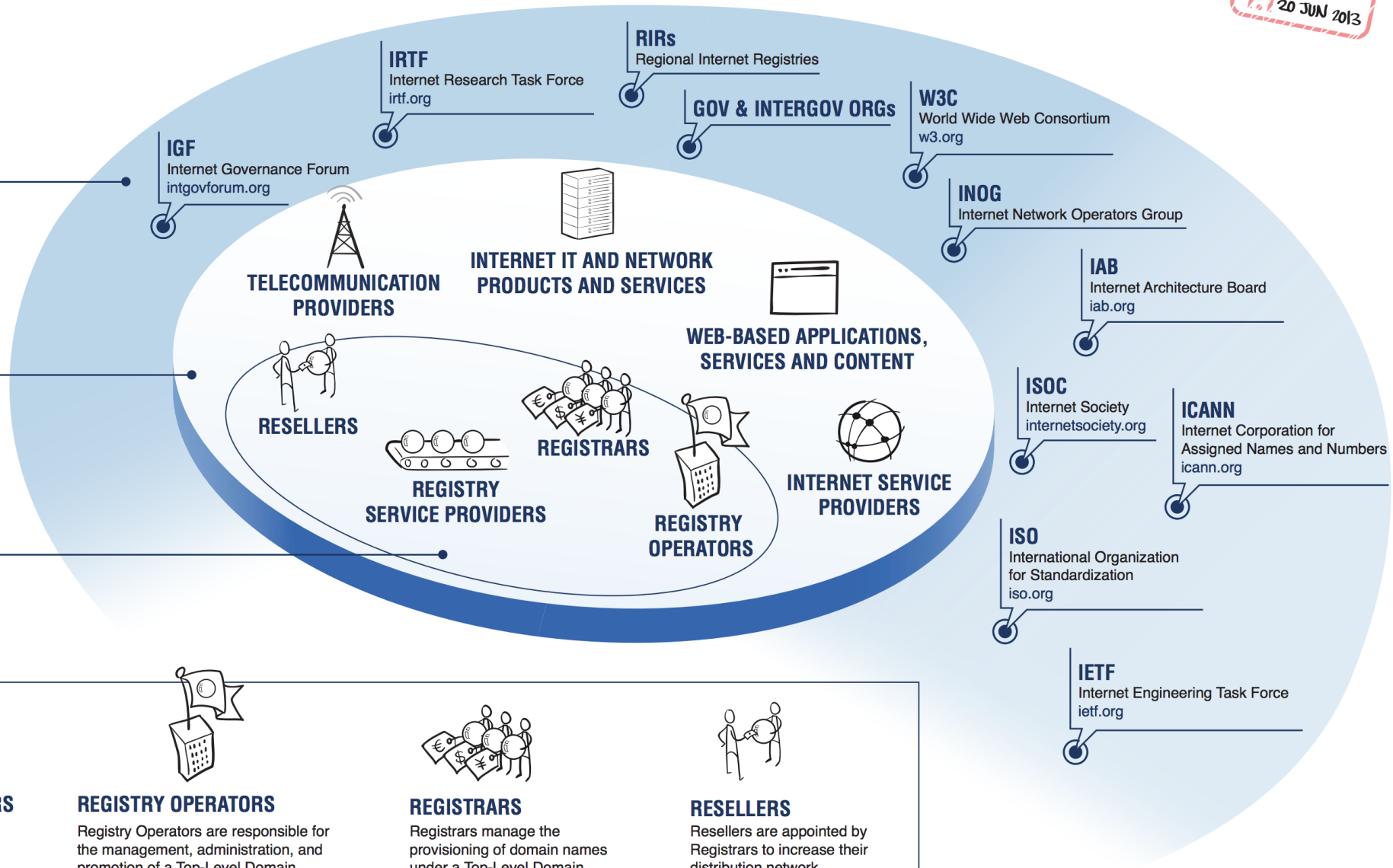
Source: https://www.europarl.europa.eu

THE DOMAIN NAME INDUSTRY

ECOSYSTEM

Source:
https://www.icann.org

VERSION 1.1 20 JUN 2013



REGISTRY SERVICE PROVIDERS

Registry Service Providers manage the technical operations in support of Registry Operators.

REGISTRY OPERATORS

Registry Operators are responsible for the management, administration, and promotion of a Top-Level Domain.

REGISTRARS

Registrars manage the provisioning of domain names under a Top-Level Domain.

RESELLERS

Resellers are appointed by Registrars to increase their distribution network.

SHARING AND CARING WITHIN

- Security Working Group since 2011
- ISO/IEC 27001 implementation workshops
- GDPR & NIS experience sharing
- S3G project for EU CSA
- …

And also TECH, R&D, Legal, Admin, Marketing working groups

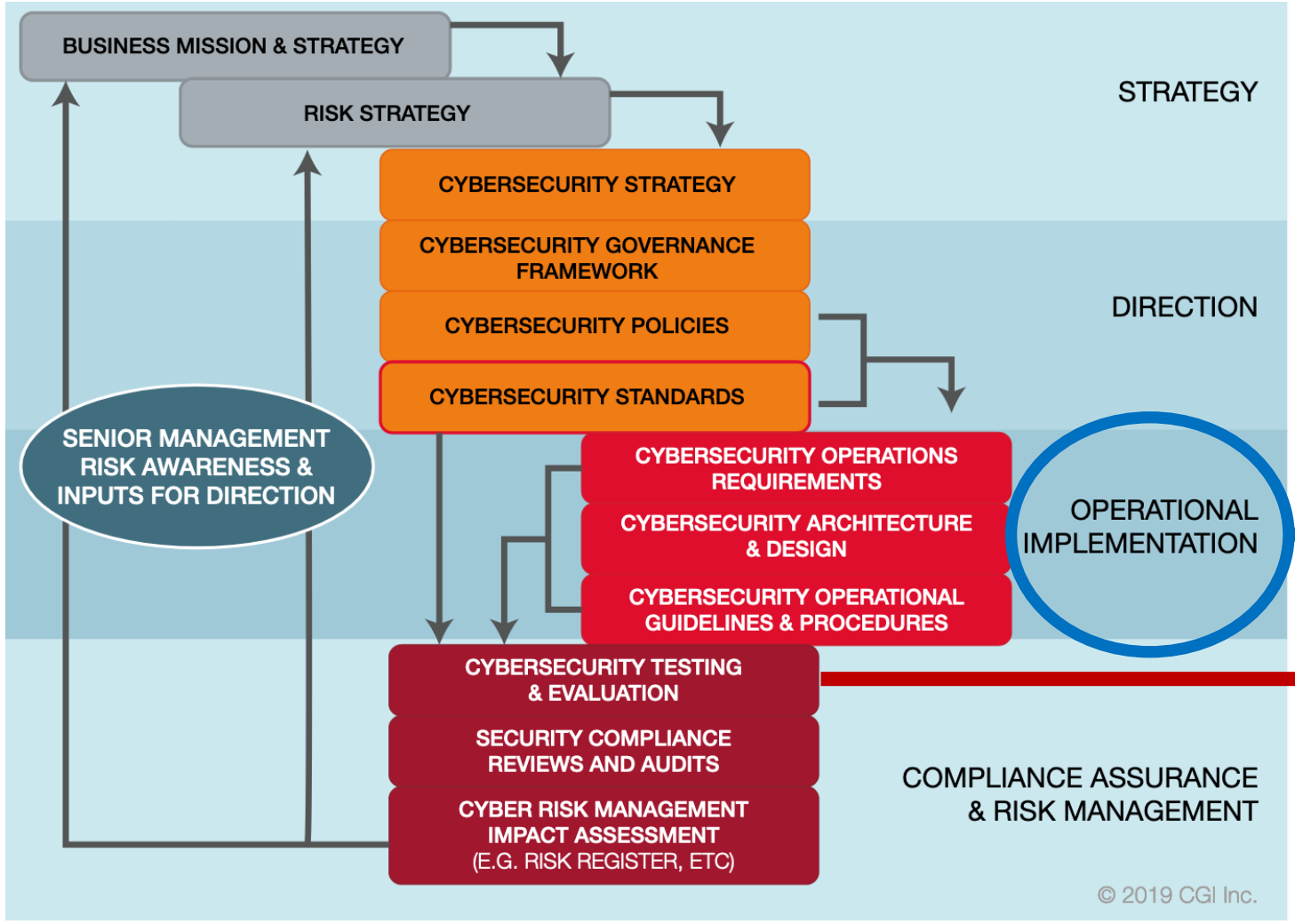
Together, its full members **manage 50%** of all **country code domain name registrations worldwide,** representing **more than 75 million registrations.**

Around **87%** of European ccTLDs **are either already certified** or **undergoing the process of cybersecurity certification** under the international Information Security Management System (ISMS) standards, such as ISO/IEC 27001.

#2

THE POWER OF THE SoA

THE GLOBAL PICTURE

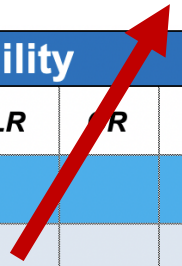


SoA, MIND MAPPING FOR THE CISO

- Statement of Applicability
- What controls are applied via which policies & procedures
- Why these controls are implemented
- At least Annex A controls are considered/evaluated
- But can be extended (but who does this?)
  - ISO/IEC 27017
  - ISO/IEC 27701
  - …

SoA IN PRACTICE

NIS consequences



Risk Assessment Result

ISMS-0104 Statement of Applicability

Section	Information security control	Applicable	Justification	LR	CR	BR	RA	Implementation / Reference
A5	**Information security policies**							
A5.1	**Management direction for information security**							
A5.1.1	Policies for information security	Y	Policies are documented, approved and communicated to ensure that DNS Belgium maintains an effective ISMS.	X		X	X	Corporate ISMS space ISMS-0101 ISMS Management ISMS-0501 Overarching information security policy
A5.1.2	Review of the policies for information security	Y	Information security policies are subject to scheduled reviews to ensure their suitability, adequacy and effectiveness.	X		X	X	ISMS-0101 ISMS Management ISMS-0502 Information security policy review guidelines
A6	**Organisation of information security**							
A6.1	**Internal organisation**							
A6.1.1	Information security roles and responsibilities	Y	To ensure the ISMS is operating within DNS Belgium, information security roles and responsibilities have been defined and communicated.			X	X	ISMS-0101 ISMS Management ISMS-0606 Organisation structure RACI matrix Information security responsibilities in job function profiles
A6.1.2	Segregation of duties	Y	Information security roles and responsibilities have been defined and communicated to reduce risks related to conflicting duties.			X	X	ISMS-0606 Organisation structure RACI matrix ISMS-0607 Segregation of duties policy
A6.1.3	Contact with authorities	Y	DNS Belgium maintains contact with relevant authorities to support information security incident management and the business continuity and contingency planning process.	X		X	X	ISMS-0101 ISMS Management ISMS-0608 Contact with authorities and special interest groups guidelines ISMS-1306 Crisis communications plan ISMS-1601 Information security incident management policy Contact list wiki page
A6.1.4	Contact with special interest groups	Y	To share and exchange information about new technologies, products, threats or vulnerabilities.			X	X	ISMS-0101 ISMS Management ISMS-0608 Contact with authorities and special interest groups guidelines ISMS-1304 Communications manual Contact list wiki page
A6.1.5	Information security in project management	Y	To identify information security risks -in as early as possible stage- related to new and existing projects regardless of the type of the project.			X	X	ISMS-0604 Information security in project management policy

dns belgium

A STANDARD FOR MANAGERS

- ISO/IEC 27001 is a management standard
- How to implement, operate & improve your ISMS
- Limited/restricted set of controls and controls “as is”
- Security policy translates, clarifies, and communicates the management position on security -> **high-level** security principles
- Security policy acts as a bridge between management objectives and specific **security requirements**

#Challenge 2

HOW TO MONITOR EFFECTIVENESS

CHAPTER 9: PERFORMANCE EVALUATION

Nonconformity source	Examples
Business requirements	Availability issues (KPI's/SLA's) Business Continuity Management reviews
Security requirements	Policy reviews Security baseline analysis
Legal, regulatory and contractual requirements	Vendor management Legal assessments
Contact with special interest groups	Feedback from interested parties Industry standard best practices
Risk management processes	Risk assessment output Gap analysis
Information security incidents	Knowledge gained from analysing and resolving incidents Log files, network flows and monitoring alerts
Internal and external audits	Review meetings Audit reports
Management reviews	Review meetings Information security objectives monitoring
Technical security audits	Results from penetration testing Results from vulnerability scanning
ISMS evaluation and document reviews	Outcome from ISMS review cycles Internal security forums
...	

#3

NO STANDARD STANDARD

NIS LAW ARTICLE 20

- The OES shall take **appropriate** and **proportionate** technical and organisational measures to manage the risks that threaten the security of networks and information systems on which its essential services depend

❖What is “appropriate”?

❖What is “proportionate”?

} A risk-based business decission

❖How to audit technical measures?

NIS LAW ARTICLE 20

- The OES shall take appropriate and proportionate technical and organisational measures to manage the risks …

  => Organisational measures = ISMS = ISO/IEC 27001

  => **Technical** measures = ISO/IEC 27002, 27017, 27018, 27032, … ? PCI DSS, …

- These measures shall ensure a level of physical and logical security appropriate to the **existing risks**, taking into account **the state of knowledge**

  => ISO/IEC 27005, ISO 31000, …

- The operator shall also take appropriate measures to prevent or limit the impact of incidents …, with a view to ensuring the continuity of these services

  => NIST cybersecurity framework; ISO 22301

A FOUNDATION TO CREATE YOUR OWN BASELINE

- Management standard
- Technical standard
- Best practice

Source: https://www.enisa.europa.eu

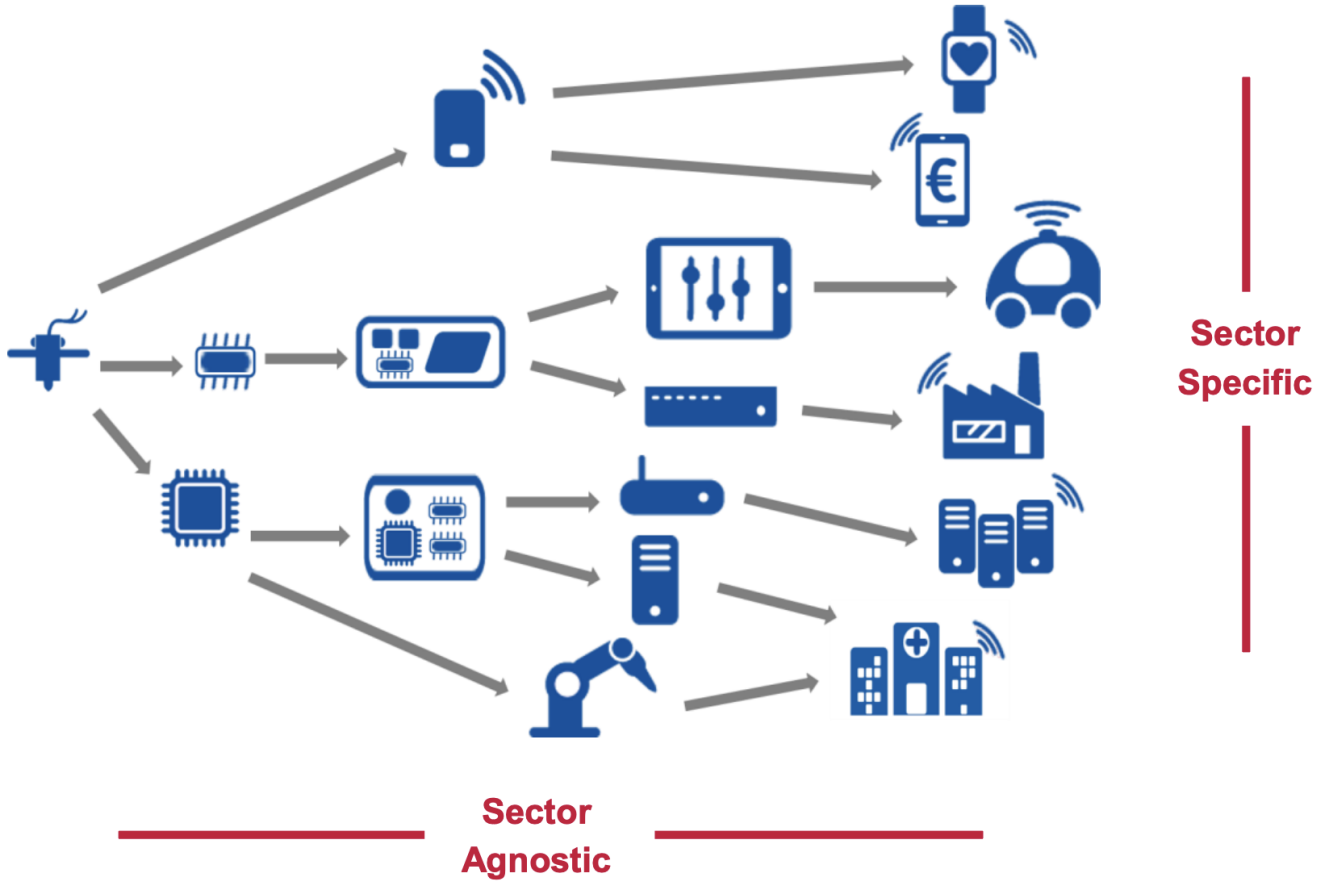
SECTOR	STANDARDS	GOOD PRACTICES
Digital Infrastructure	• ISO/IEC 27011:2008 Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	• Technical guidance on the security measures for Telcos in Article 13a, ENISA • Best Practices – IX-F

Table 17: International standards and good practices specific to the Digital Infrastructures sector

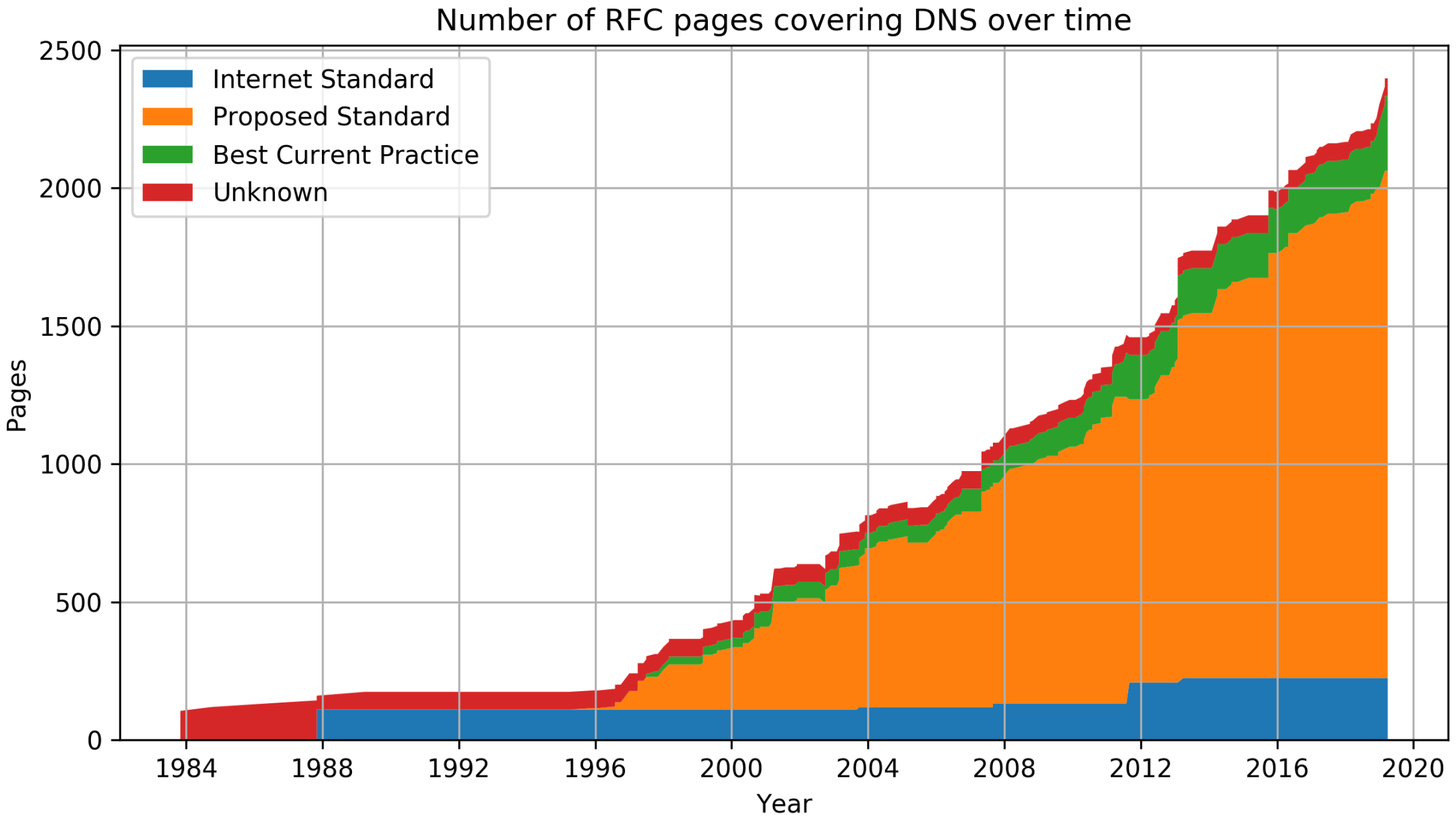
#Challenge 3

SECTOR-SPECIFIC

HORIZONTAL VERSUS VERTICAL



Source:
https://www.enisa.europa.eu


Number of RFC pages covering DNS over time
Internet Standard
Proposed Standard
Best Current Practice
Unknown
Pages
2500
2000
1500
1000
500
0
1984
1988
1992
1996
2000
2004
2008
2012
2016
2020
Year

BEST PRACTICES

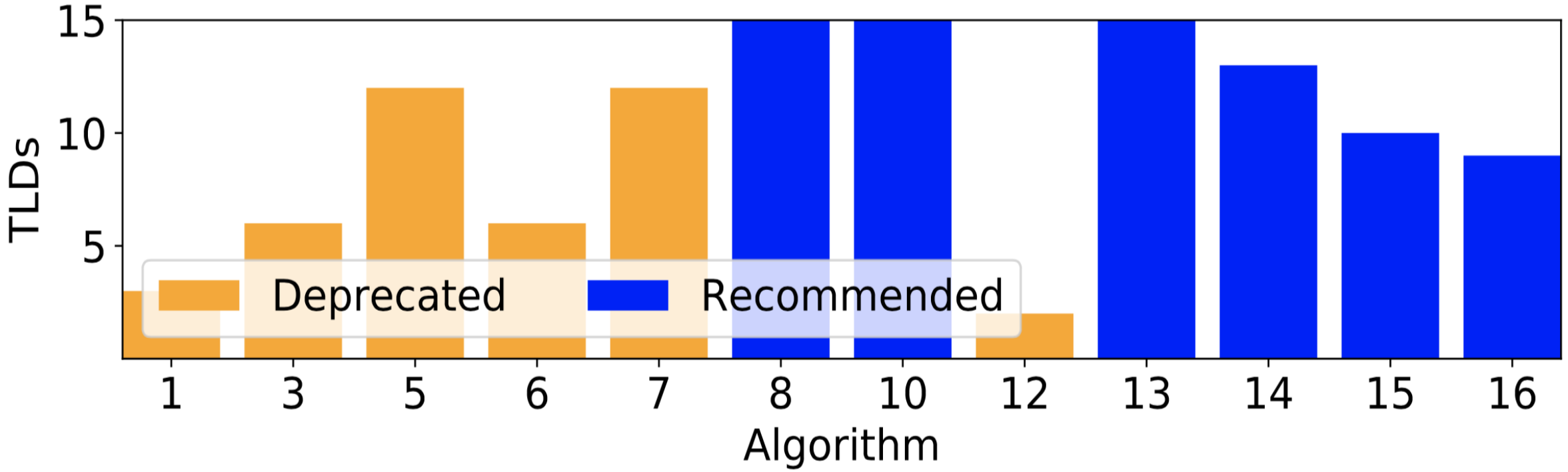
3. Algorithm Selection

3.1. DNSKEY Algorithms

The following table lists the implementation recommendations for DNSKEY algorithms [DNSKEY-IANA].

Number	Mnemonics	DNSSEC Signing	DNSSEC Validation
1	RSAMD5	MUST NOT	MUST NOT
3	DSA	MUST NOT	MUST NOT
5	RSASHA1	NOT RECOMMENDED	MUST
6	DSA-NSEC3-SHA1	MUST NOT	MUST NOT
7	RSASHA1-NSEC3-SHA1	NOT RECOMMENDED	MUST
8	RSASHA256	MUST	MUST
10	RSASHA512	NOT RECOMMENDED	MUST
12	ECC-GOST	MUST NOT	MAY
13	ECDSAP256SHA256	MUST	MUST
14	ECDSAP384SHA384	MAY	RECOMMENDED
15	ED25519	RECOMMENDED	RECOMMENDED
16	ED448	MAY	RECOMMENDED

REALITY CHECK



#4

FILLING THE GAPS

LEGAL FRAMEWORK

- GDPR -> NIS -> EU CSA

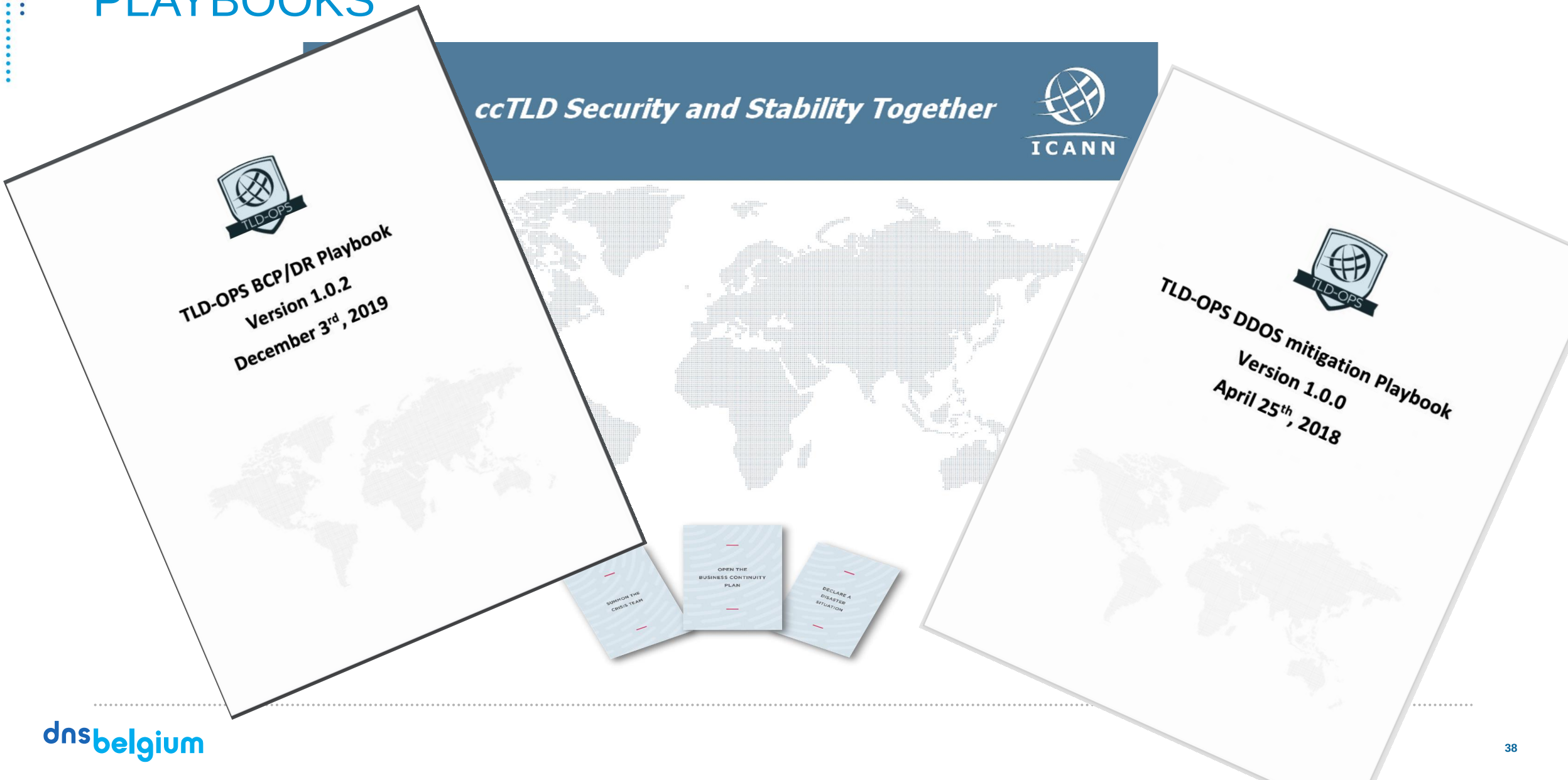
Product	Service	Relevant legislation		
.ccTLD	authoritative DNS service		NIS	CSA
	registration service	GDPR	NIS	*CSA*
	lookup service	GDPR		*CSA*

TABLE 1: Mapping products and services on legislation

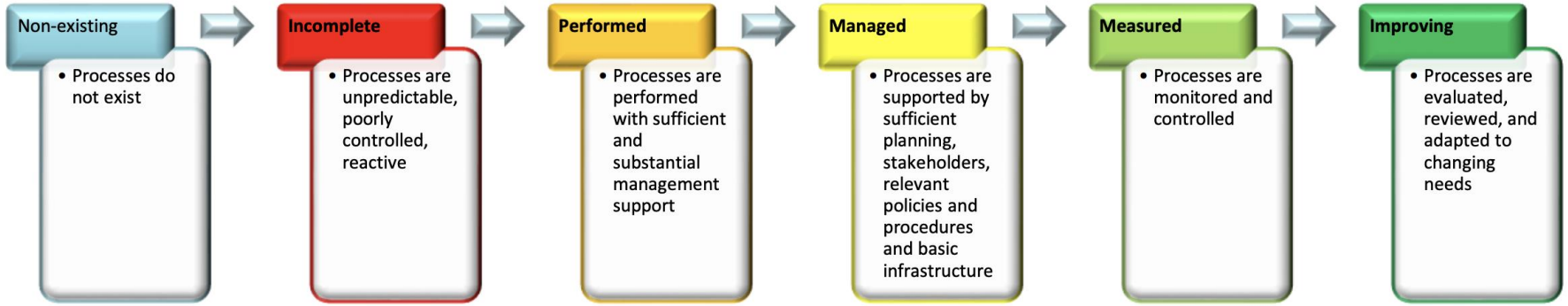
Legislation	ccTLD implementation						Main object
GDPR	ISO/IEC 27001	ISO/IEC 27002	ISO/IEC 27018	**ISO/IEC 27701**	…		Customer
NIS	ISO/IEC 27001	ISO/IEC 27002	ISO 22301	…			Network and information systems
CSA	Certification scheme (incl. technical standards)						Consumer

TABLE 2: Mapping legislation on standards and best practices

PLAYBOOKS


TLD-OPS
TLD-OPS BCP/DR Playbook
Version 1.0.2
December 3rd, 2019
ccTLD Security and Stability Together
ICANN
SUMMON THE CRISIS TEAM
OPEN THE BUSINESS CONTINUITY PLAN
DECLARE A DISASTER SITUATION
TLD-OPS
TLD-OPS DDOS mitigation Playbook
Version 1.0.0
April 25th, 2018

CM-SMM



Category	Sub-Category
Establish	Information security strategy
	Governance and compliance
	Risk management
	Workforce management
	Asset management
	Managing the supply chain
Prevent	Change management
	Configuration and automation management
	Secure engineering and development
	Secure operations
	Identity and access management
	Awareness and training
	Information protection
Detect	Undertake logging and monitoring
	Threat and vulnerability management
	Auditing
	Detect information security events
Respond	Escalate information security events and declare incidents
	Response planning
	Respond to information security incidents
Recover	Continuity management
	Communications

Baseline (ML3)

CM-SMM

ID	Level	Description	Reached
2.1		**Change management**	**3**
	ML1		
	ML1	Activities and procedures associated with change management such as change request submission and impact assessment are completed in at least an ad hoc manner.	y
	ML2		
	ML2	Significant changes that affect information security are identified and recorded.	y
	ML2	Significant changes are subject to risk assessments, and the associated risks (and benefits) are communicated to management before being implemented.	y
	ML2	Changes to assets are tested prior to being deployed, whenever possible.	y
	ML3		
	ML3	Change management practices address the full life cycle of assets (i.e. acquisition, deployment, operation, retirement and disposal).	y
	ML3	Adequate resources (people, funding and tools) are provided to support change management activities.	y
	ML3	A formal change management process with assigned stakeholders' responsibilities that includes documented procedures is in place.	y
	ML3	A formal approval procedure for proposed changes is in place. Changes are assessed to meet applicable security requirements.	y
	ML3	Change details are communicated to all relevant stakeholders.	y
	ML3	Changes are prioritised and planned.	y
	ML3	An emergency change process is established to enable the prompt and controlled implementation of changes needed to resolve an incident.	y
	ML3	Fall-back procedures for aborting and recovering from unsuccessful changes are developed.	y
	ML4		
	ML4	Changes to assets are monitored to validate the fact that they meet the strategic aims and objectives, including information security (e.g. being validated by a project committee or business owner, meeting functional or non-functional business requirements, etc.).	y
	ML4	Change results are reviewed to validate their effectiveness and the extent to which they meet the expectations of the relevant stakeholders (feedback process).	n
	ML4	Change management activities are periodically reviewed to ensure their conformance with policy and to validate their effectiveness.	y
	ML5		
	ML5	The change management process contains an improvement track based on the outcome of the periodical change review cycles and the monitoring effort specified under ML4.	n
	ML5	The change management process itself is periodically re-appraised to capture and adapt to changes in the information security risk environment.	n

#5

TECHNICAL MEASURES

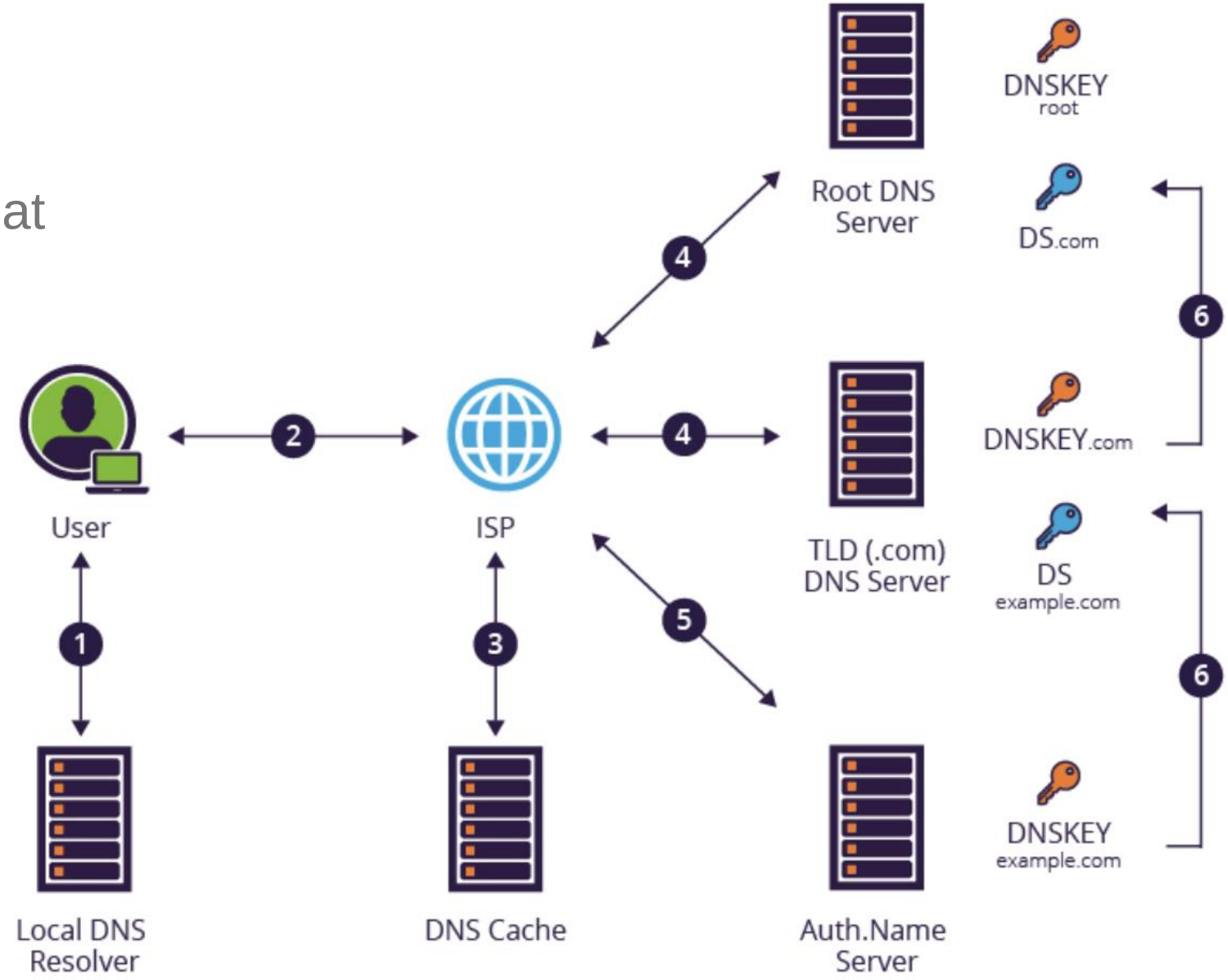
WHAT'S IN THE TOOLBOX?

- DNSSEC
- Domain Guard
- Domain Shield
- Local/global anycast

DNSSEC

- How can we be sure that the public keys are not tampered with?
- Solution:
  store a hash of the DNSKEY record at the parent, in a DS record

  = trust anchors



Source: imperva.com

#Challenge 4

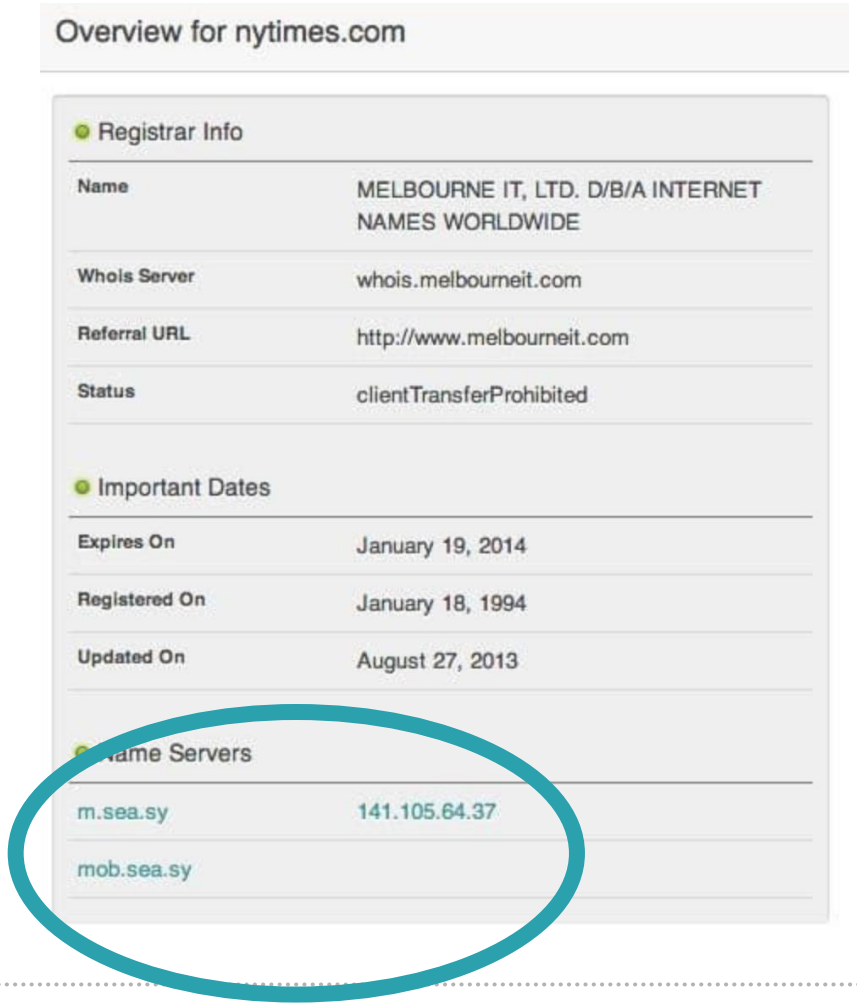
USE IT OR LOSE IT (*)

CHICKEN AND EGG

- Core infrastructure of DNS has been equipped with DNSSEC support
  - July 2010: root signed
  - Aug 2010: be zone signed
  - Oct 2010: first registrars started signing domains
- Caching recursive name servers need to enable DNSSEC **validation**
- Registrants/registrars need to **sign** the DNS zones associated with these domains using DNSSEC

DNS HIJACKING – FACEBOOK vs NY TIMES

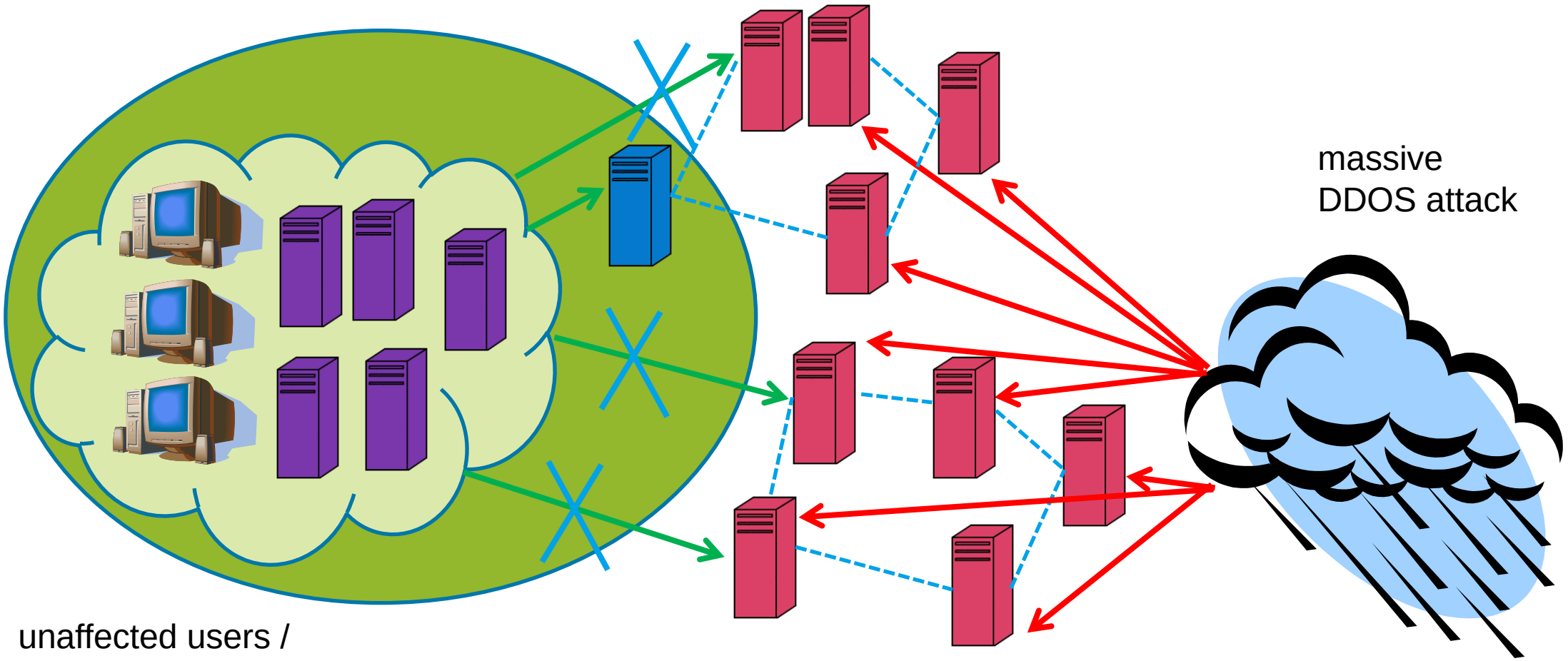
```
Domain Name: facebook.com
Registry Domain ID:
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2013-06-06T04:00:37-0700
Creation Date: 2010-04-01T11:56:37-0700
Registrar Registration Expiration Date: 2020-03-29T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: compliance@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited
Domain Status: clientTransferProhibited
Domain Status: clientDeleteProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Facebook, Inc.
Registrant Street: Syria,
Registrant City: Damascus
Registrant State/Province: SY
Registrant Postal Code: 94025
Registrant Country: SY
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax: +1.6505434800
Registrant Fax Ext:
Registrant Email: syrian.es.sy@gmail.com
```



DDOS DEFENSE: ANYCAST DNS

- In anycast, one IP address can apply to many servers
- Anycast DNS means that any one of a number of DNS servers can respond to DNS queries
- Typically the one that is geographically closest will provide the response (path-length; BGP)

DDOS PROTECTION: ANYCAST@ISP



unaffected users /
caching name servers@ISP

#6

ISMS IN DAILY LIFE

#Challenge 5

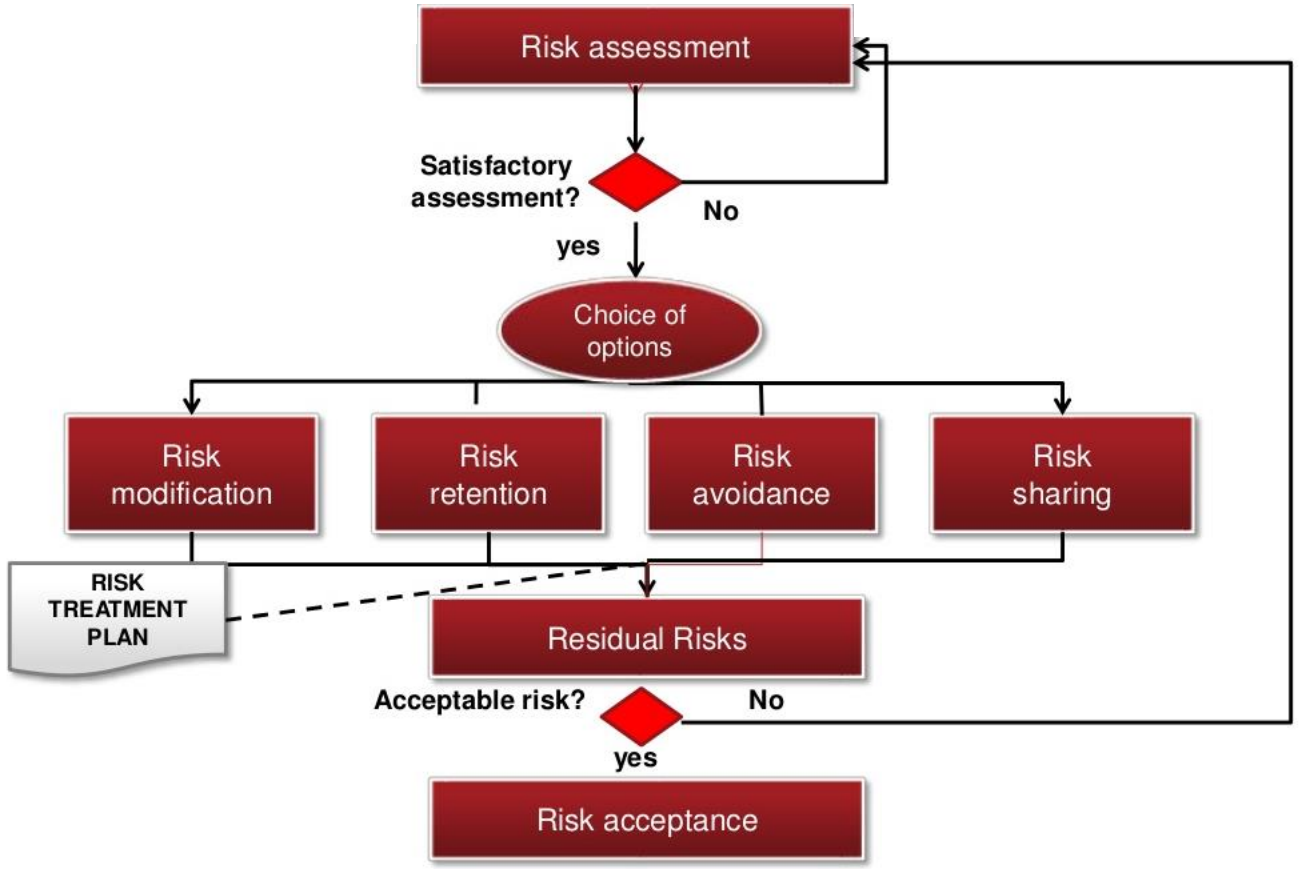
HOW TO KEEP IT ALIVE?

AWARENESS

- Repeat - repeat – repeat
- ISMS content reviews by relevant staff
- Both internal & external
  - Campaigns
  - Projects
  - Cyber security challenges
  - …

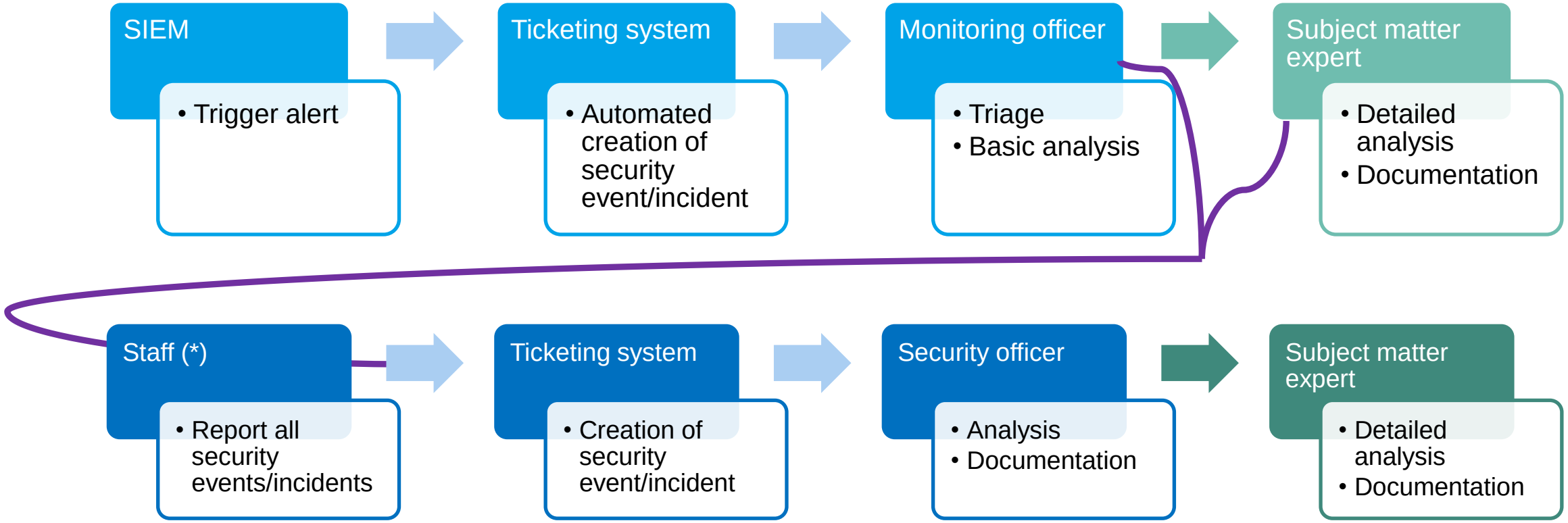
RISK MANAGEMENT

- Based on ISO/IEC 27005
- ⇔ Corporate risk mgmt

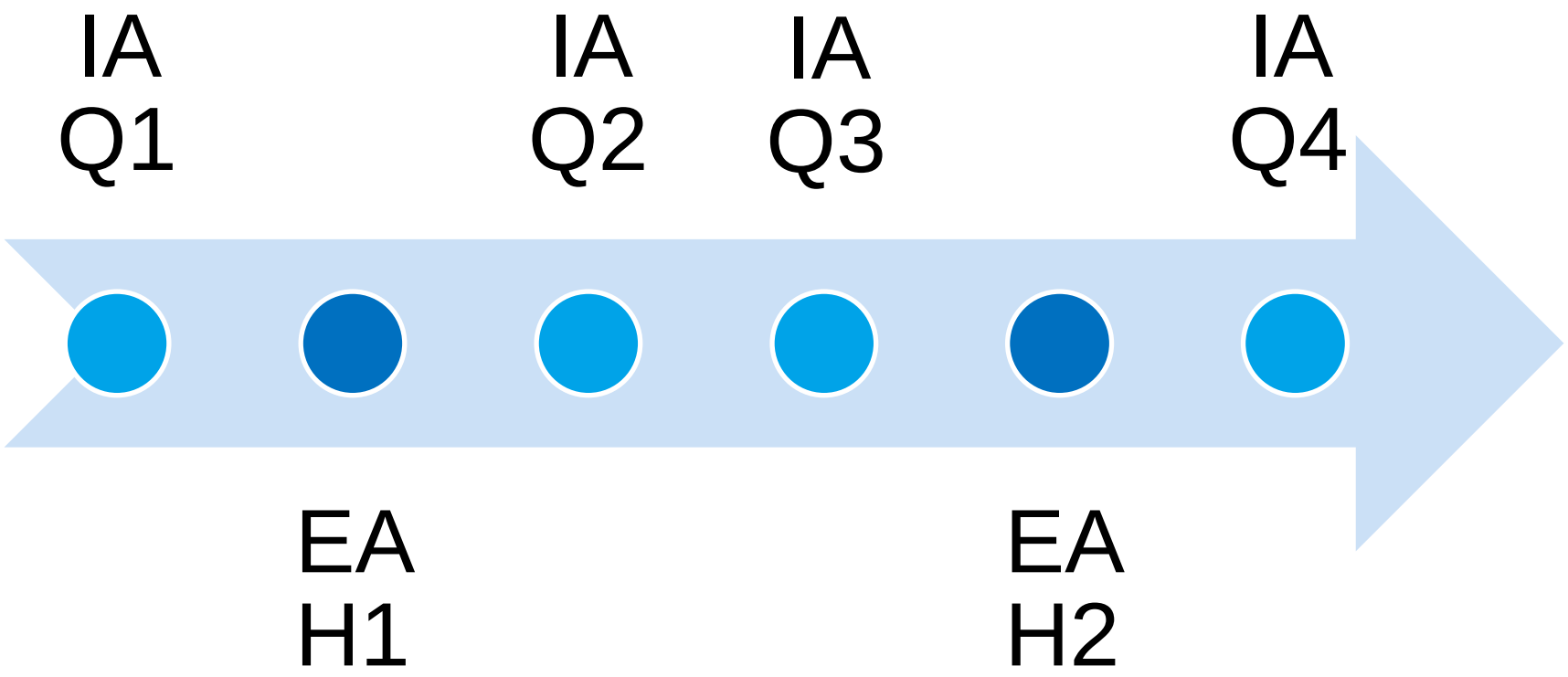


- Security risk assessments incorporated in project mgmt flow
- Risk treatment incorporated in agile organisation

REPORTING INCIDENTS



AUDITS



dnsbelgium