FOSS

ANALYTICS BEYOND MEASURE

ISO27002 – THOUGHTS ON IMPLEMENTATION & USE

ANALYTICS BEYOND MEASURE

AGENDA

Kristian Kreiner

- Information Security & Compliance specialist
- Member of DS/S-441
- Background in IT, Risk & Compliance

ISO27001 - IMPLEMENTATION PROJECT (27002 AS A GUIDE)

- *WHY WERE WE DOING IT*
- *HOW WERE WE DOING IT*
- *HOW DID IT GO*

HOW WE ADD VALUE

FOSS

RAW MATERIAL
Payment, segregation and quality control of raw material

PROCESSING
Improved predictability and control of manufacturing processes

FINISHED GOODS
Safe products and compliance with regulatory requirements

On-farm

Receiving points

At-line/In-line production

Quality Control Laboratories

Finished products

INFORMATION MANAGEMENT NETWORK

DATA GENERATION

CONTROL & AUTOMATION

DATA INTELLIGENCE

ANALYTICS BEYOND MEASURE

A VERSATILE RANGE OF SOLUTIONS

Digital Services

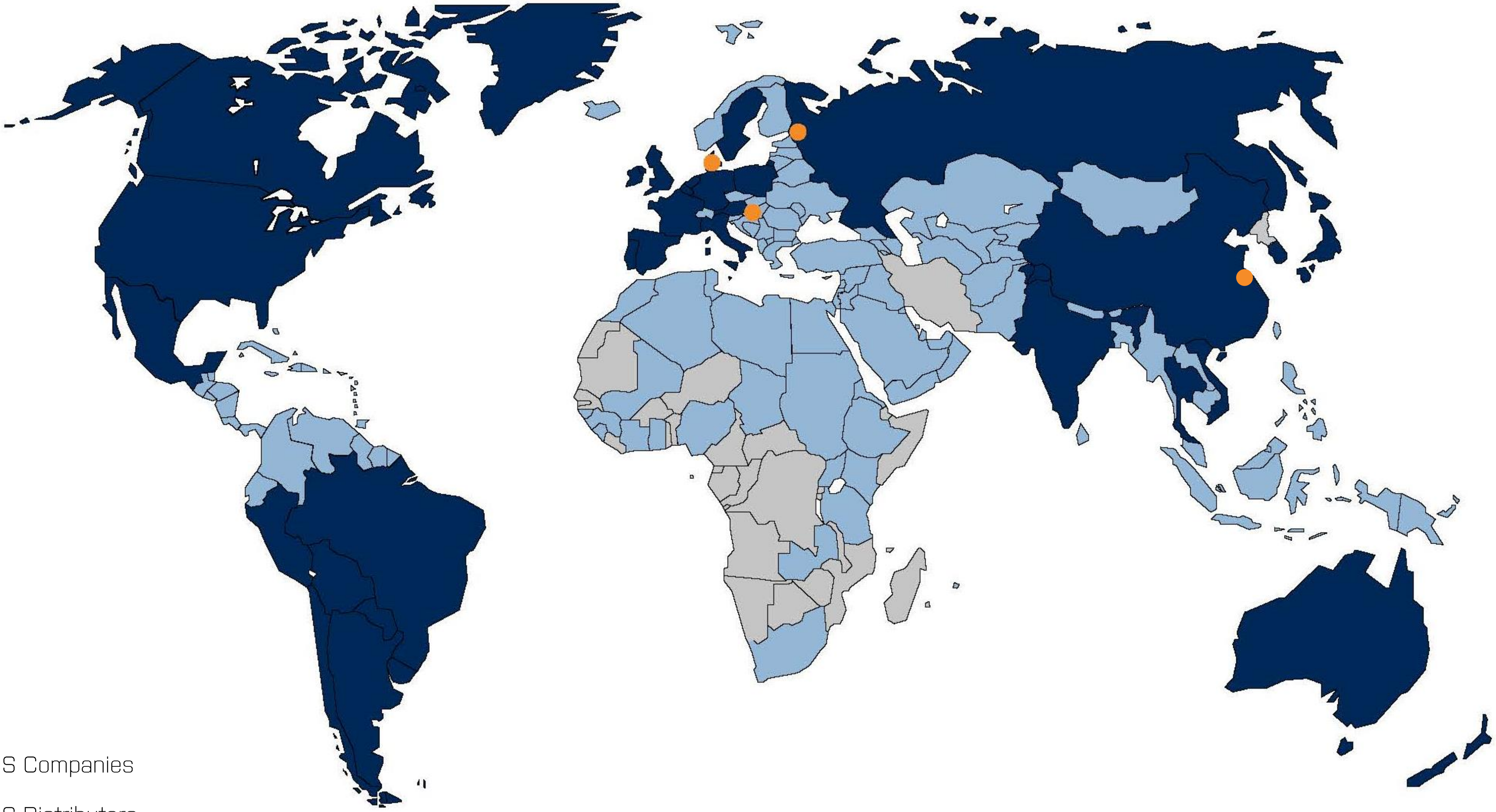
> 50 Benchtop/laboratory solutions

> 10 Process solutions

ANALYTICS BEYOND MEASURE

GLOBAL PRESENCE

FOSS



■ FOSS Companies

🟦 FOSS Distributors

🟧 FOSS RDM Centres

ANALYTICS BEYOND MEASURE

INDUSTRY LEADING SOLUTIONS
FOR INDUSTRY LEADING CUSTOMERS

FOSS

RAW MILK TESTING

- mpr
- valacta
- NML national milk laboratories
- eurofins
- Qlip kwaliteitsborging in agrifood

DAIRY

- Fonterra
- GROUPE LACTALIS
- Nestlé
- DANONE
- glanbia
- KRAFT
- FrieslandCampina
- Arla

GRAIN, MILLING & OILS

- Barilla
- CBH GROUP
- ADM
- DCOOP
- SGS
- LDC. Louis Dreyfus Company

WINE

- EST. 1883 CONCHA Y TORO
- CHATEAU LATOUR
- DOMINIO DE PINGUS
- VAL D'OCA
- ANTINORI
- indevin New Zealand
- Hochschule Geisenheim University

MEAT

- Tyson
- VION FOOD GROUP
- OSI
- JBS
- Cargill

FEED & FORAGE

- Cargill
- inVivo
- nutreco
- EVONIK INDUSTRIES
- CPF
- ADISSEO A Bluestar Company Adding Difference

OTHER INDUSTRIES

- Olam
- Cargill
- HERSHEY'S
- Mondelēz International
- raízen
- MARS

LABORATORIES

- eurofins
- SGS
- MERIEUX NutriSciences
- AGROLAB GROUP

ANALYTICS BEYOND MEASURE

WHY WERE WE DOING IT....

Hackers are very smart !

&

We need security ☺

WHY WERE WE DOING IT….
WHAT OUR CUSTOMER ASKED OF US

FOSS

Customer List:

- Abbot
- Cargill
- Fonterra
- Danone
- Tyson Foods
- EBOS
- Schreiber
- …….

COBIT 5 AN ISACA® FRAMEWORK

FedRAMP

HIPAA Health Insurance Portability and Accountability Act

NIST

CSA cloud security alliance®

Information Security Management ISO 27001 Certified

PCI DSS COMPLIANT

ISAE 3000

AICPA

Information Security Management ISO 27001 Certified

Evaluation

- Risk based approach
- Control mapping
- Customer recognition
- Customer demand
- GDPR
- ISO 9001
- Digital business

Information Security Area
Application & Interface Security
Audit Assurance & Compliance
Business Continuity Management & Operational Resilience
Change Control & Configuration Management
Data Security & Information Lifecycle Management
Datacenter Security
Encryption & Key Management
Governance and Risk Management
Human Resources
Identity & Access Management
Infrastructure & Virtualization Security
Interoperability & Portability
Mobile Security
Security Incident Management, E-Discovery, & Cloud Forensics
Supply Chain Management, Transparency, and Accountability
Threat and Vulnerability Management

WHY WERE WE DOING IT….
ISO 27001 CERTIFICATION BENEFITS

Prove our information security commitment to FOSS current and future clients and partners

Reduced compliance burden for our organization

Reduce cost by lowering number & impact of risks and incidents

Increase security of important company assets

Helps to optimize organisational processes

CERTIFIED ISO 9001 CERTIFIED

GDPR

HOW WERE WE DOING IT…?
INITIAL RISKS – ISO27002 AN EARLY CONSIDERATION

FOSS

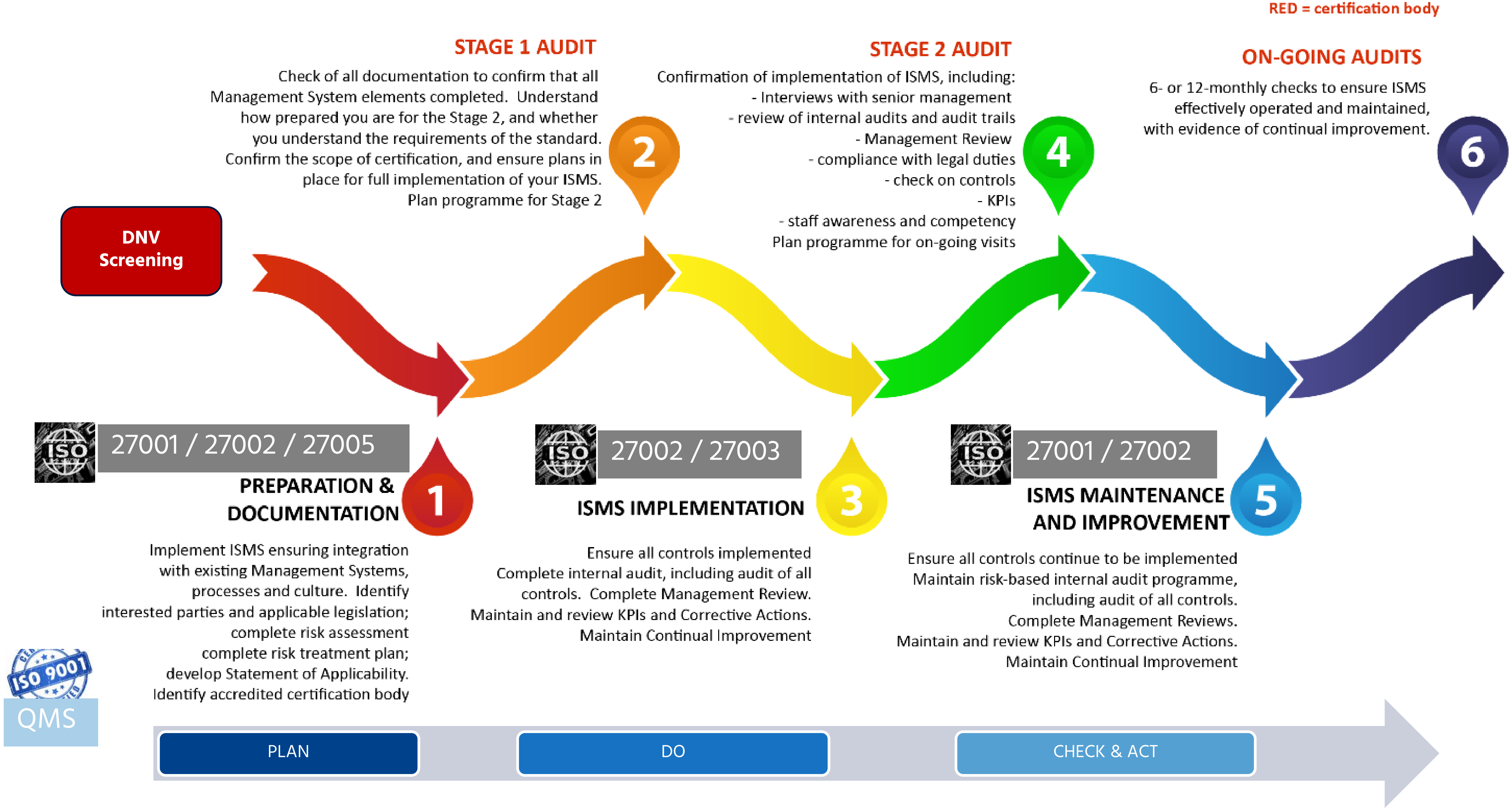
Description of Risk / Issue	Effect	Likelihood	Impact	Action taken to handle/mitigate risk
ISMS scope too big / implementation timeframe too short	ISMS not ready for certification on agreed date	HIGH	HIGH	• 1st stage audit + internal audit to assess ISMS readiness before the final certification audit • Limiting the scope • **ISO implementation managed as a project (Use 27002/3 as a guide)**
Large number of projects / enhancements necessary to obtain certification	High amount of work and resources needed, harder to achieve certification	HIGH	MEDIUM	• Prioritize project / enhancements based on risk assessment • Focus top priority • Consult & review security & technology roadmaps
Lack support in the organization needed to implement necessary changes	ISMS not functioning correctly, limited benefits from the ISMS implementation	MEDIUM	HIGH	• Engagement of other departments in scope of a project • General training & learning
Insufficient ISO 27001 knowledge among people working on the project	ISMS implemented incorrectly	MEDIUM	MEDIUM	• Additional ISO 27001 trainings
Performing activities that incur unnecessary costs and waste time	Loss of time/money, missing project deadline	MEDIUM	MEDIUM	• Additional ISO 27001 trainings • **ISO implementation managed as a project (Use 27002/3 as a guide)**
Selection of too many and/or too expensive controls	Lost of time/money	MEDIUM	LOW	• Some ISO training already scheduled, more to come • People with necessary knowledge appointed to the project • **Use ISO27002/SoA as Control Gap tool**

ANALYTICS BEYOND MEASURE

HOW WERE WE DOING IT…?

FOSS

ANALYTICS BEYOND MEASURE



RED = certification body

DNV Screening

27001 / 27002 / 27005

PREPARATION & DOCUMENTATION

Implement ISMS ensuring integration with existing Management Systems, processes and culture. Identify interested parties and applicable legislation; complete risk assessment complete risk treatment plan; develop Statement of Applicability. Identify accredited certification body

STAGE 1 AUDIT

Check of all documentation to confirm that all Management System elements completed. Understand how prepared you are for the Stage 2, and whether you understand the requirements of the standard. Confirm the scope of certification, and ensure plans in place for full implementation of your ISMS.
Plan programme for Stage 2

27002 / 27003

ISMS IMPLEMENTATION

Ensure all controls implemented
Complete internal audit, including audit of all controls. Complete Management Review.
Maintain and review KPIs and Corrective Actions.
Maintain Continual Improvement

STAGE 2 AUDIT

Confirmation of implementation of ISMS, including:
- Interviews with senior management
- review of internal audits and audit trails
- Management Review
- compliance with legal duties
- check on controls
- KPIs
- staff awareness and competency

Plan programme for on-going visits

27001 / 27002

ISMS MAINTENANCE AND IMPROVEMENT

Ensure all controls continue to be implemented
Maintain risk-based internal audit programme, including audit of all controls.
Complete Management Reviews.
Maintain and review KPIs and Corrective Actions.
Maintain Continual Improvement

ON-GOING AUDITS

6- or 12-monthly checks to ensure ISMS effectively operated and maintained, with evidence of continual improvement.

QMS

PLAN

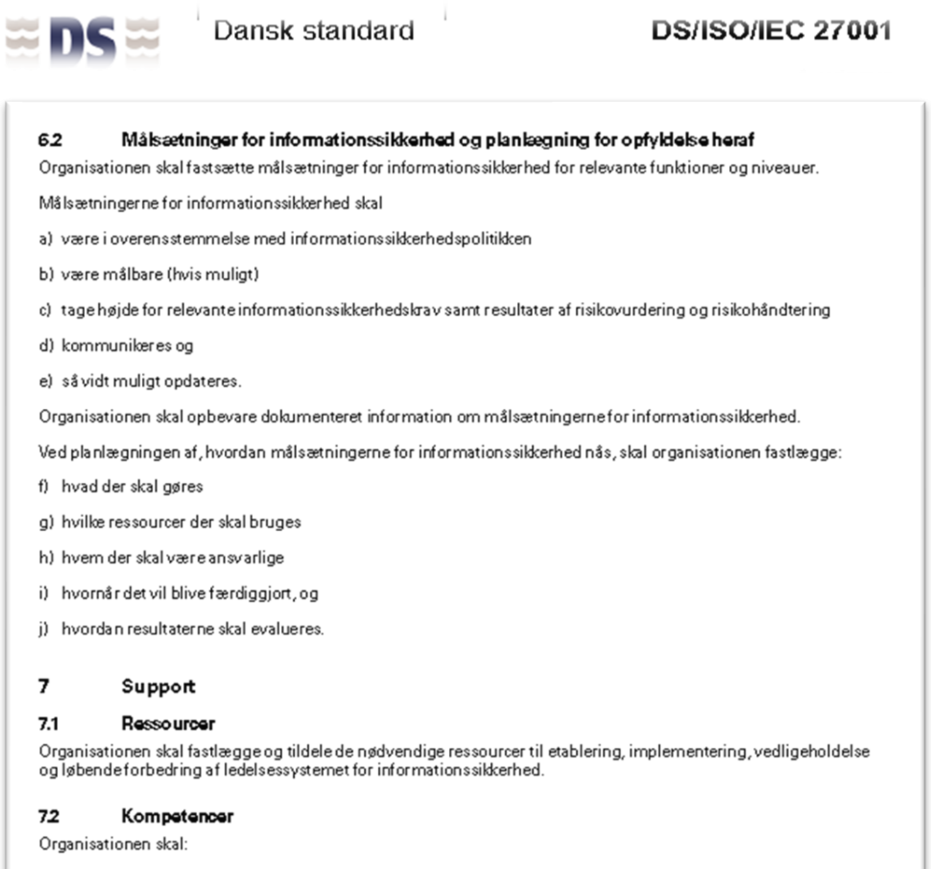
DO

CHECK & ACT

HOW WERE WE DOING IT…?
ISO 27001 IN PRACTISE

Requirements Implementation

- **Chapter**
  - **Sub section**
- **Requirements**



DS | Dansk standard | DS/ISO/IEC 27001

6.2 Målsætninger for informationssikkerhed og planlægning for opfyldelse heraf

Organisationen skal fastsætte målsætninger for informationssikkerhed for relevante funktioner og niveauer.

Målsætningerne for informationssikkerhed skal

a) være i overensstemmelse med informationssikkerhedspolitikken

b) være målbare (hvis muligt)

c) tage højde for relevante informationssikkerhedskrav samt resultater af risikovurdering og risikohåndtering

d) kommunikeres og

e) så vidt muligt opdateres.

Organisationen skal opbevare dokumenteret information om målsætningerne for informationssikkerhed.

Ved planlægningen af, hvordan målsætningerne for informationssikkerhed nås, skal organisationen fastlægge:

f) hvad der skal gøres

g) hvilke ressourcer der skal bruges

h) hvem der skal være ansvarlige

i) hvornår det vil blive færdiggjort, og

j) hvordan resultaterne skal evalueres.

7 Support

7.1 Ressourcer

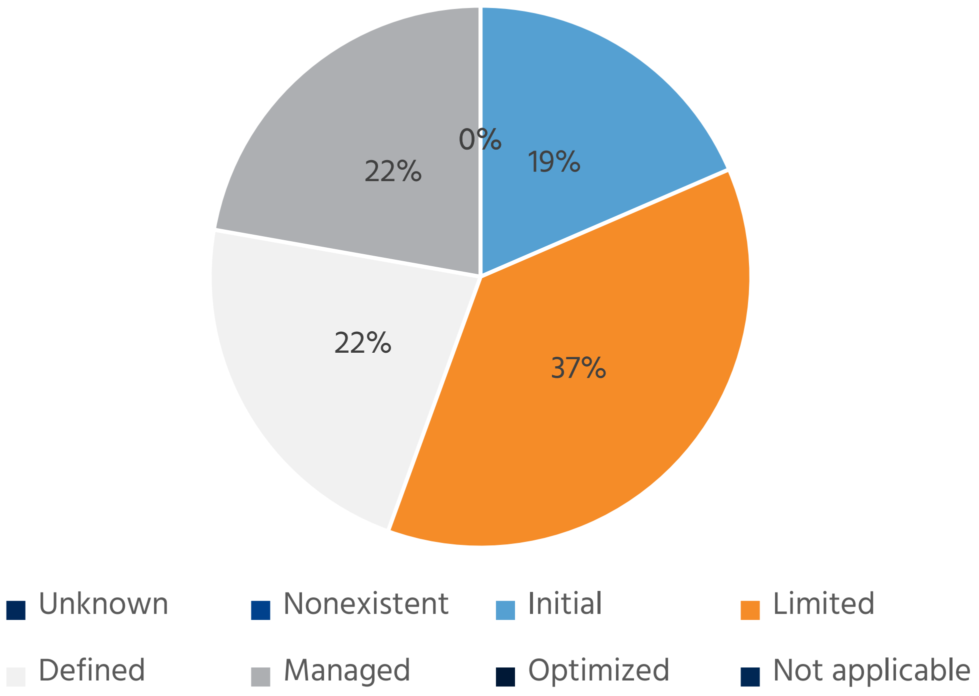
Organisationen skal fastlægge og tildele de nødvendige ressourcer til etablering, implementering, vedligeholdelse og løbende forbedring af ledelsessystemet for informationssikkerhed.

7.2 Kompetencer

Organisationen skal:

Requirements Implementation Status

Proportion of ISMS requirements



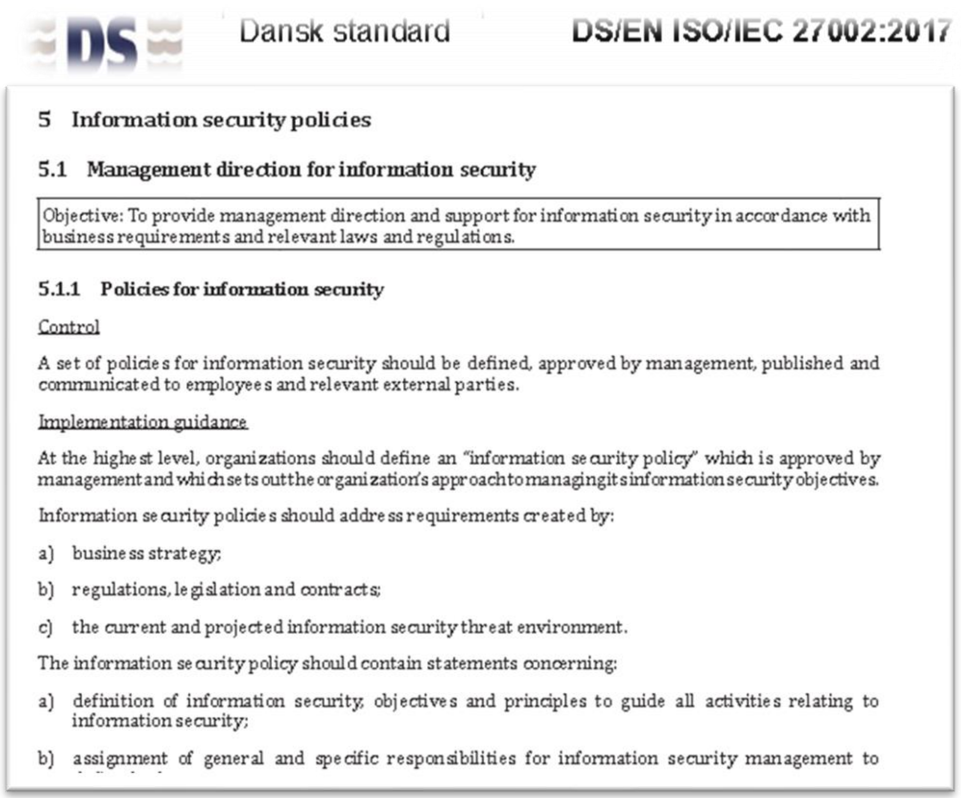
ANALYTICS BEYOND MEASURE

HOW WERE WE DOING IT…?
ISO 27002 IN PRACTISE

FOSS

Control Implementation

- **Control**
- **Implementation Guidance**
- **Other information**



DS Dansk standard DS/EN ISO/IEC 27002:2017

5 Information security policies

5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.

Information security policies should address requirements created by:

a) business strategy;

b) regulations, legislation and contracts;

c) the current and projected information security threat environment.

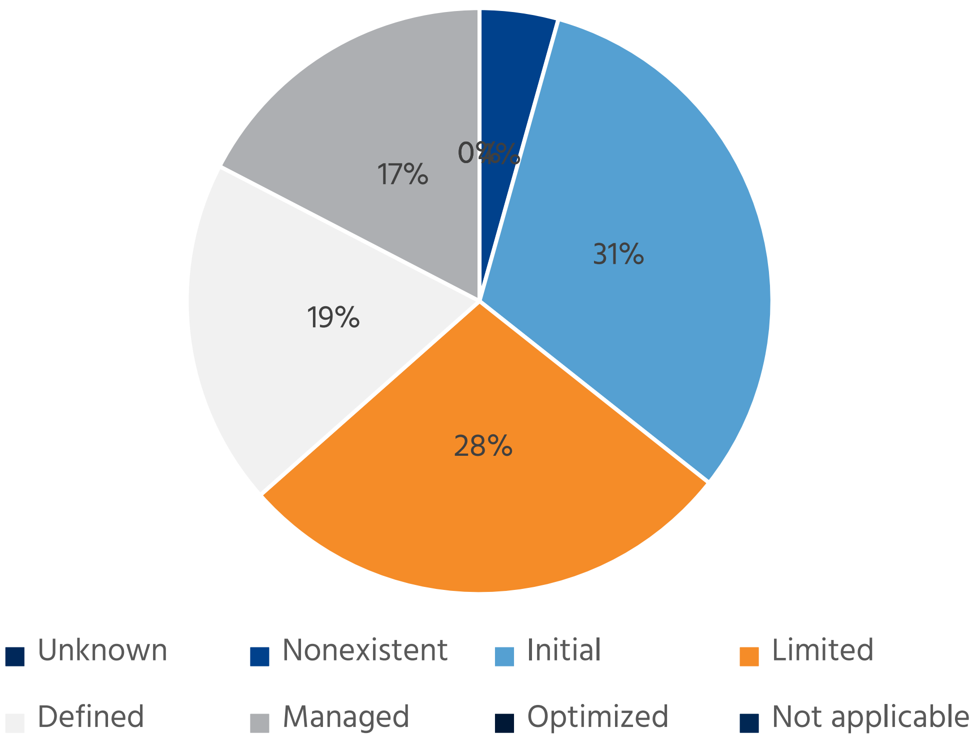
The information security policy should contain statements concerning:

a) definition of information security, objectives and principles to guide all activities relating to information security;

b) assignment of general and specific responsibilities for information security management to

Control Implementation Status

Proportion of information security controls

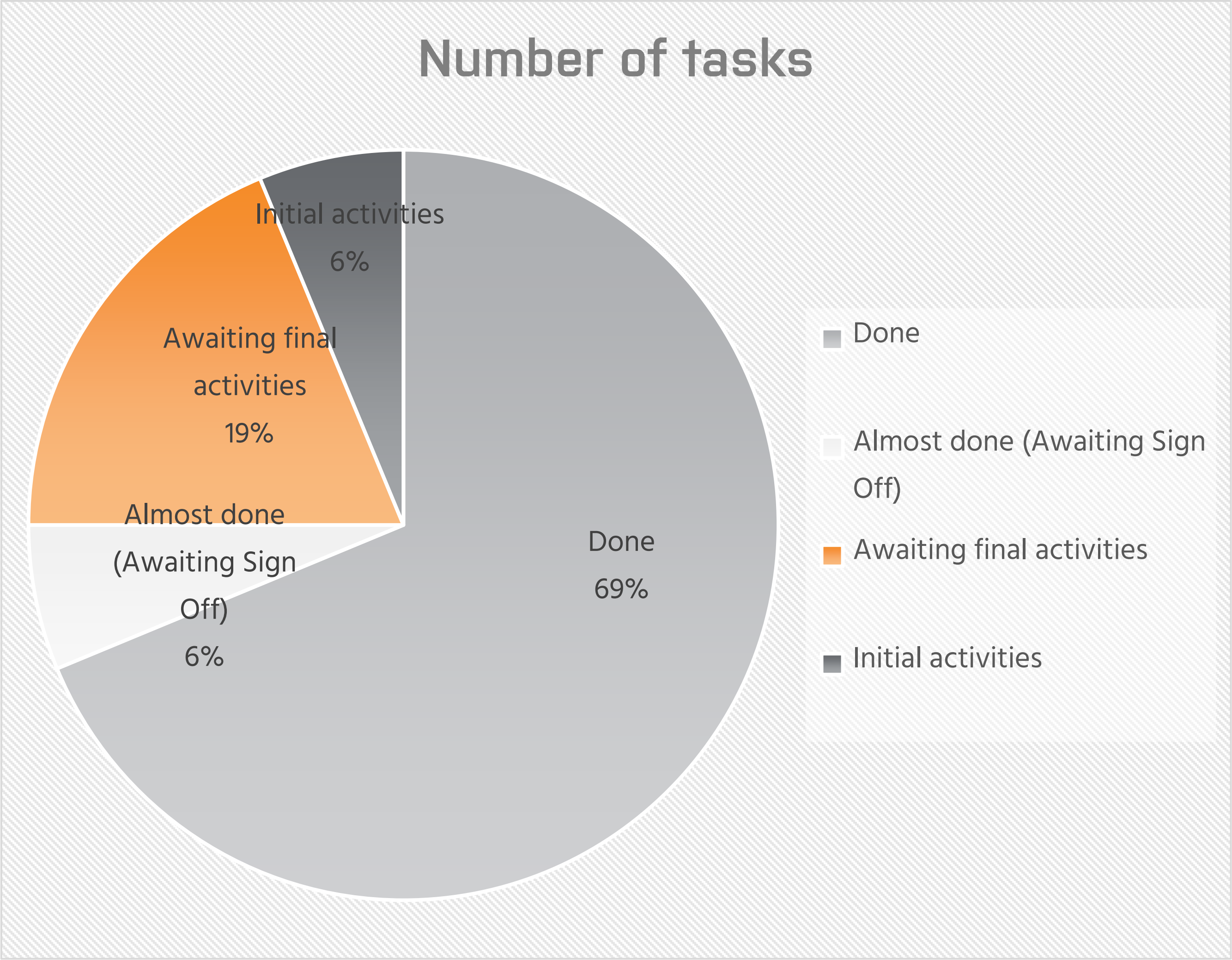


ANALYTICS BEYOND MEASURE

HOW WERE WE DOING IT...?

FOSS

TASK REPORTING SAMPLE – PHASE 01 – PLAN (ESTABLISH ISMS)



Almost Done

Review & complete Inventory and ownership of assets document	99%
Review & complete Supplier IS Questionnaire (light) document	99%

Awaiting Final Activities

Review & complete Physical and Environmental Security document	75%
Management Reviews	75%
Review & complete Performance Evaluation Procedure document	75%
Review & complete Supplier Information Security Procedure document	75%
Review & complete Secure Development Policy document	60%
Review & complete Information Security Incidents document	50%

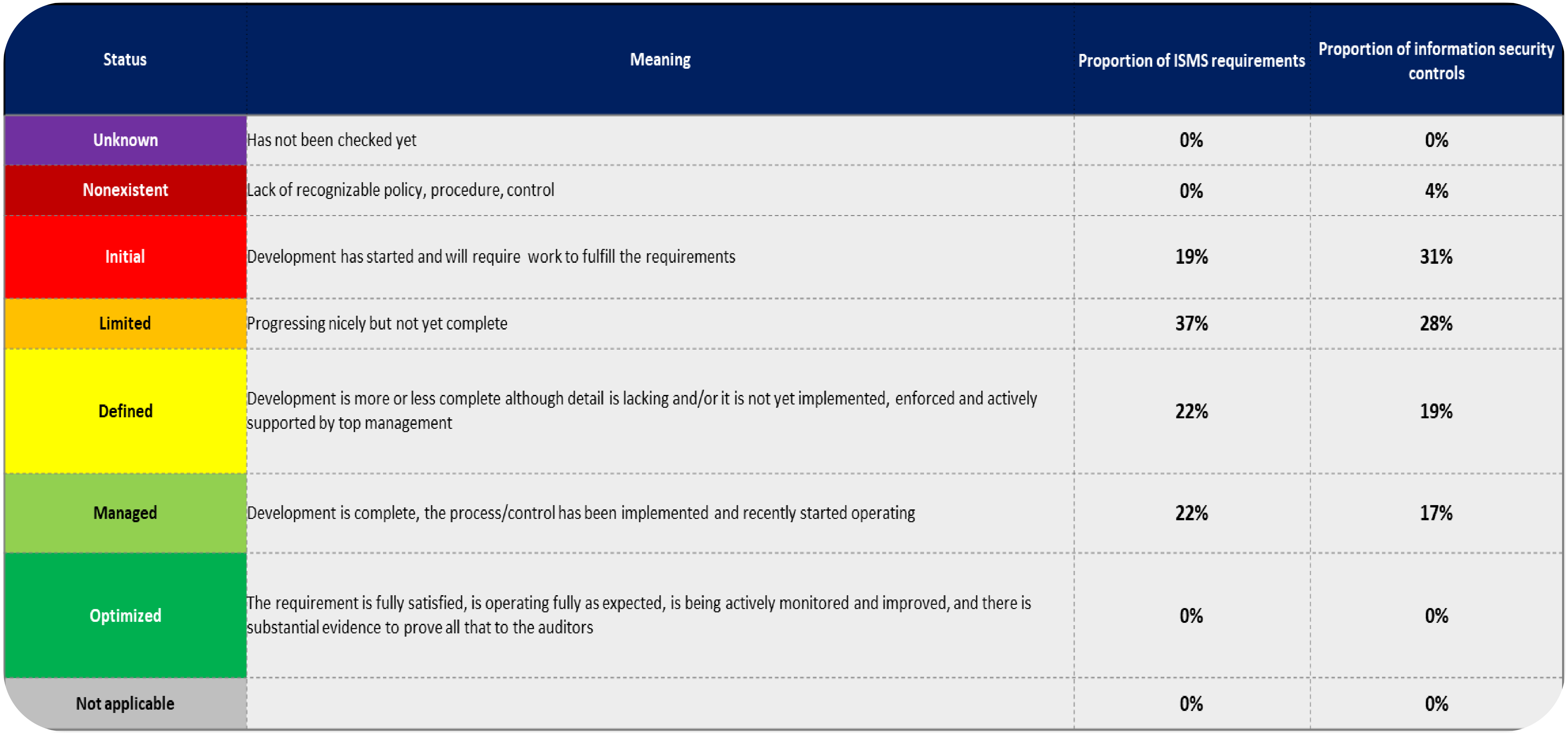
Initial Activities

Review & complete Information Security Classification document	15%
Review & complete Information Security Continuity Plan document	10%

ANALYTICS BEYOND MEASURE

HOW WERE WE DOING IT…?
CONTROL/REQUIREMENTS GAP MONITORING

FOSS



Status	Meaning	Proportion of ISMS requirements	Proportion of information security controls
Unknown	Has not been checked yet	0%	0%
Nonexistent	Lack of recognizable policy, procedure, control	0%	4%
Initial	Development has started and will require work to fulfill the requirements	19%	31%
Limited	Progressing nicely but not yet complete	37%	28%
Defined	Development is more or less complete although detail is lacking and/or it is not yet implemented, enforced and actively supported by top management	22%	19%
Managed	Development is complete, the process/control has been implemented and recently started operating	22%	17%
Optimized	The requirement is fully satisfied, is operating fully as expected, is being actively monitored and improved, and there is substantial evidence to prove all that to the auditors	0%	0%
Not applicable		0%	0%

ANALYTICS BEYOND MEASURE

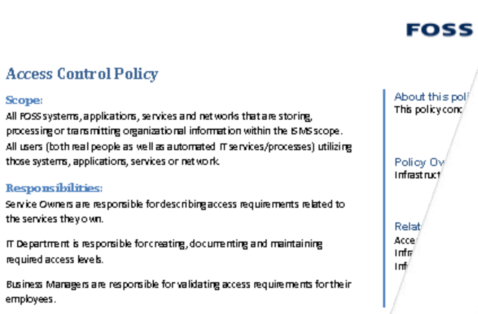
HOW DID IT GO

FOSS

TECHNLOGY POTENTIAL @ FOSS

- 🟩 Implemented
- ● Under consideration
- 🟥 No solution
- ○ Needs priority

Network Security
Network Firewall
Network Monitoring/Forensics
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application
WAF & App
Vul
Managed Security Serv
Risk & Compliance
Industrial / IoT Security
Fra


FOSS

Access Control Policy

Scope:

All FOSS systems, applications, services and networks that are storing, processing or transmitting organizational information within the ISMS scope. All users (both real people as well as automated IT services/processes) utilizing those systems, applications, services or network.

Responsibilities:

Service Owners are responsible for describing access requirements related to the services they own.

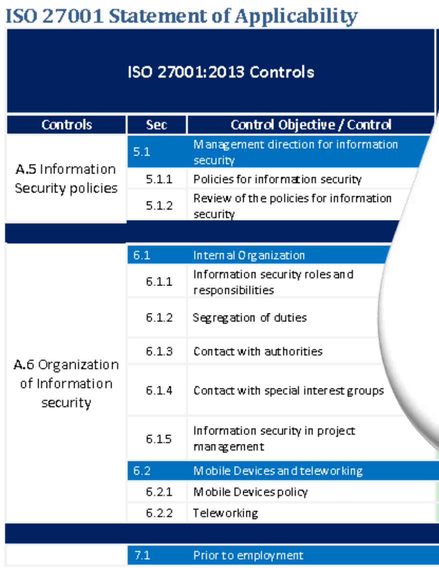
IT Department is responsible for creating, documenting and maintaining required access levels.

Business Managers are responsible for validating access requirements for their employees.

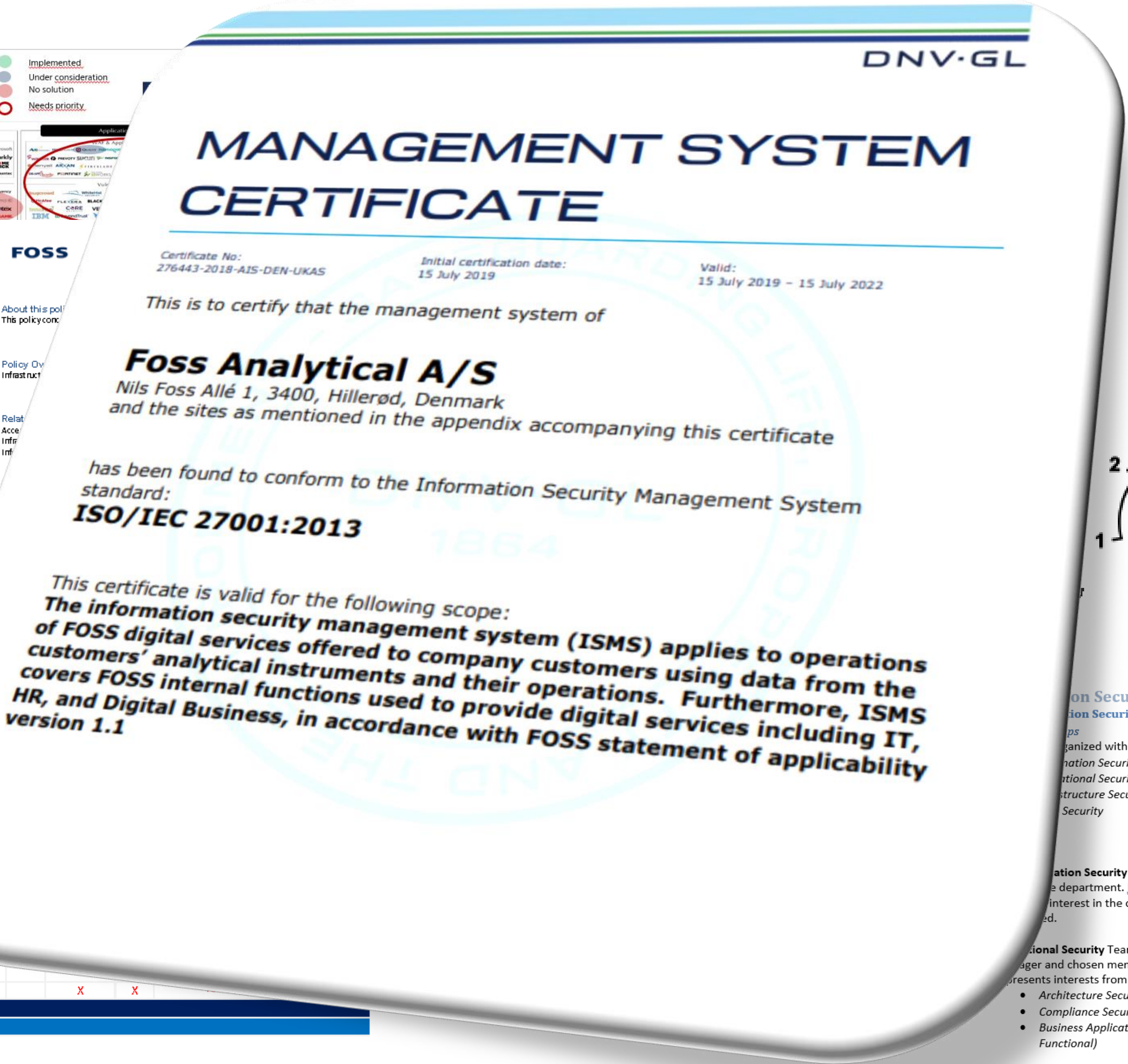
About this pol
This policy conc

Policy Ov
Infrastruct

Relat
Acce
Infr
Inf


ISO 27001 Statement of Applicability

ISO 27001:2013 Controls			cluded				
Controls	Sec	Control Objective / Control					
A.5 Information Security policies	5.1	Management direction for information security					
	5.1.1	Policies for information security					
	5.1.2	Review of the policies for information security					
A.6 Organization of Information security	6.1	Internal Organization					
	6.1.1	Information security roles and responsibilities					
	6.1.2	Segregation of duties					
	6.1.3	Contact with authorities					
	6.1.4	Contact with special interest groups					
	6.1.5	Information security in project management					
	6.2	Mobile Devices and teleworking					
	6.2.1	Mobile Devices policy	Yes				
	6.2.2	Teleworking	Yes			X	X
	7.1	Prior to employment					


DNV·GL

MANAGEMENT SYSTEM CERTIFICATE

Certificate No:
276443-2018-AIS-DEN-UKAS

Initial certification date:
15 July 2019

Valid:
15 July 2019 – 15 July 2022

This is to certify that the management system of

Foss Analytical A/S

Nils Foss Allé 1, 3400, Hillerød, Denmark
and the sites as mentioned in the appendix accompanying this certificate

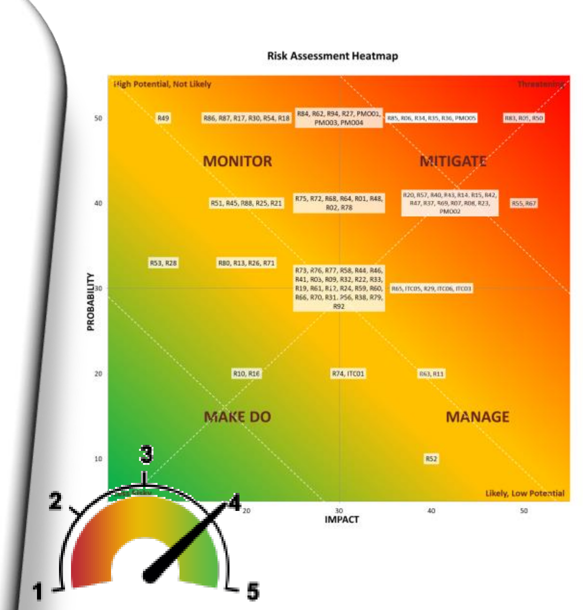
has been found to conform to the Information Security Management System standard:

ISO/IEC 27001:2013

This certificate is valid for the following scope:

The information security management system (ISMS) applies to operations of FOSS digital services offered to company customers using data from the customers' analytical instruments and their operations. Furthermore, ISMS covers FOSS internal functions used to provide digital services including IT, HR, and Digital Business, in accordance with FOSS statement of applicability version 1.1

FOSS


Risk Assessment Heatmap

ANALYTICS BEYOND MEASURE

r

DEGREE OF
CONTROL

High

FOSS

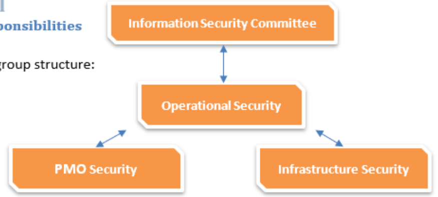
on Security Manual

ion Security Roles & Responsibilities

ps

ganized within the following group structure:

- nation Security Committee
- tional Security
- structure Security
- Security



ation Security Committee (ISC) is made up of the VP of Global IT and chosen members of the e department. Furthermore SVP of Finance, SVP of Digital Business and SVP of R&D, represents interest in the committee. Other members of the business are invited to the Committee meetings ed.

ional Security Team is made up of the VP of Global IT, the Head of PMO Security, Infrastructure ager and chosen members of the Compliance department. Furthermore, the following Security Roles presents interests from the organization:

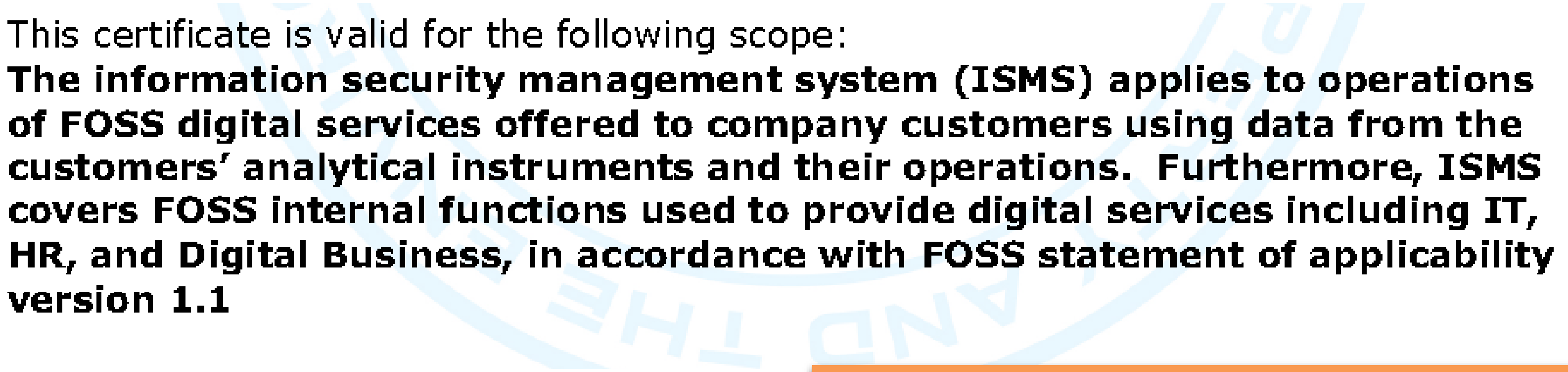
- *Architecture Security*
- *Compliance Security*
- *Business Applications Security (Technical & Functional)*
- *Infrastructure Security (Hard & Soft)*
- *Support Security*
- *Digital Business Security*

Infrastructure Security Team is made of the Infrastructure Manager, Hard and Soft Infrastructure Security Managers.

HOW DID IT GO

SCOPE, AUDIT AND ALL THE REST

SCOPE



This certificate is valid for the following scope:
The information security management system (ISMS) applies to operations of FOSS digital services offered to company customers using data from the customers' analytical instruments and their operations. Furthermore, ISMS covers FOSS internal functions used to provide digital services including IT, HR, and Digital Business, in accordance with FOSS statement of applicability version 1.1

AUDIT

Certified July 2019
2 Maintenance audits
Focus areas helps improvement

"Living It " vs. Initial certification.....

LESSONS LEARNED

Early Corporate Management engagement is key
Use ISO27002 as inspiration and a tool
Design the project as you would live it (PDCA & ISO2003)
Tailor the scope to specific needs and goals
Compliance a growing factor in sales process
Integrated Risk Management essential

ANALYTICS BEYOND MEASURE

FOSS

THANK YOU

ANALYTICS BEYOND MEASURE