Logicom Solutions

Welcome to Cybersecurity for Critical Infrastructures webinar. The presenters are in a practice session. The webinar will start at 11!

Logicom Solutions

We will start in 5 minutes!
For any technical issue, please use the Chat
For your questions, please use the Q&A!

Agenda

- Cybersecurity Strategy of the Republic of Cyprus – Covering Critical Information Infrastructures
  George Michaelides, Commissioner of Communications

- Key provisions of the NIS Directive and compliance to Cyprus legislation for CIIs
  Costas Efthymiou, Technical Officer, Digital Security Authority

- HOW TOs – Achieving Compliance by Critical Infrastructures against the Security Measures defined in the Law
  Charis Florides, Senior Business Consultant, Logicom Solutions

- Q&A- Discussion

3 Business Units

Sales & Business Development, Accounting, Operations

- Business Solutions and Services
- Technology Solutions and Services
- Business Consulting Services

ISO Certified

ISO 9001 — Quality Management System

ISO 27001 — Information Security Management System

3 Countries of coverage

Partnerships

With industry leaders such as:

Gold Microsoft Partner

Cisco Partner Gold Certified

DELL EMC

accenture

400+ Customers

...and growing

Logicom Solutions

$37+ m

Revenue 2019

Values

- Uncompromising **integrity**
- Commercial **agility**
- Operational **efficiency**
- Service **quality**
- People **development**

~ 100 Employees

Serving Customers in the following industries:

Government, Utilities, Banking, Telecommunications, Insurance, Retail, Energy, Education, Shipping

Digital Security Authority (DSA)

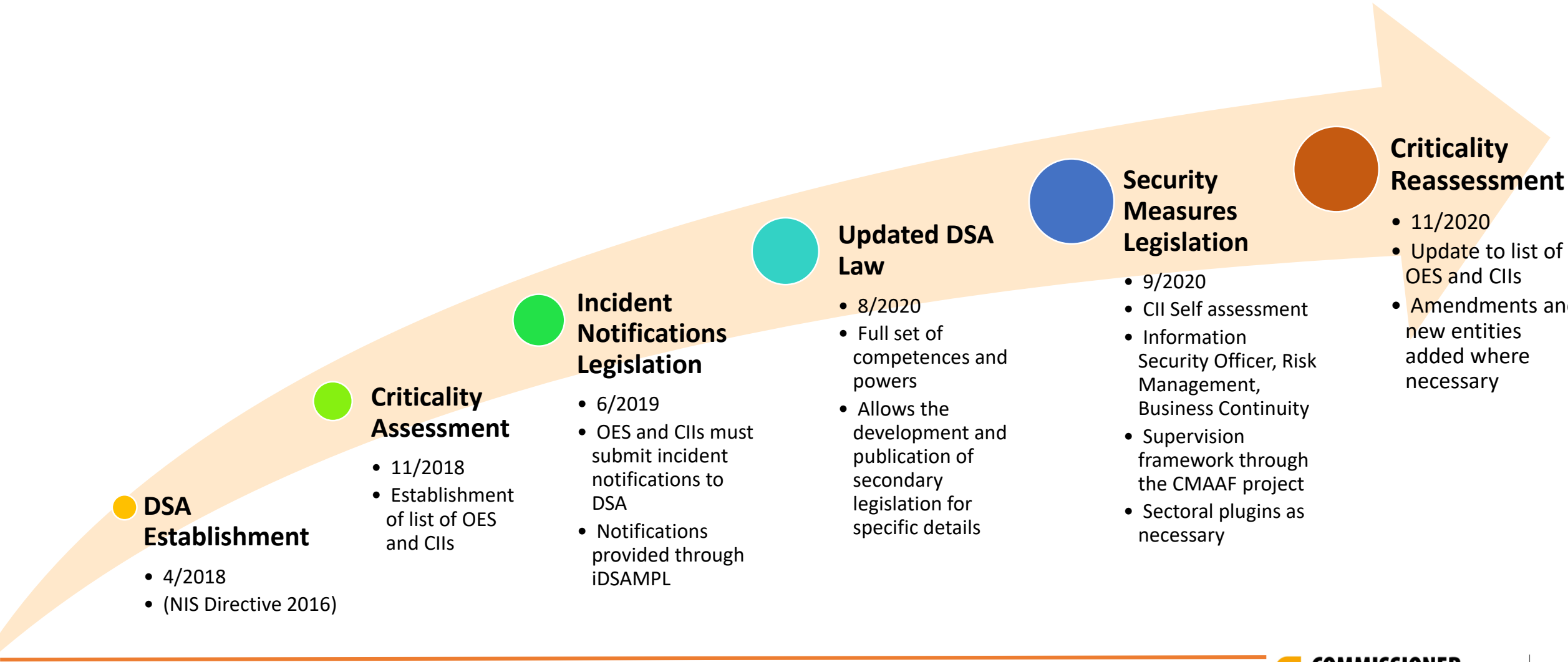
Implementation of the NIS Directive in Cyprus

George Michaelides, Commissioner of Communications
Digital Security Authority
https://dsa.cy | https://csirt.cy

Nicosia, 15 December 2020

COMMISSIONER OF COMMUNICATIONS | Digital Security Authority

NIS Directive in Cyprus – Timeline so far



DSA Establishment

- 4/2018
- (NIS Directive 2016)

Criticality Assessment

- 11/2018
- Establishment of list of OES and CIIs

Incident Notifications Legislation

- 6/2019
- OES and CIIs must submit incident notifications to DSA
- Notifications provided through iDSAMPL

Updated DSA Law

- 8/2020
- Full set of competences and powers
- Allows the development and publication of secondary legislation for specific details

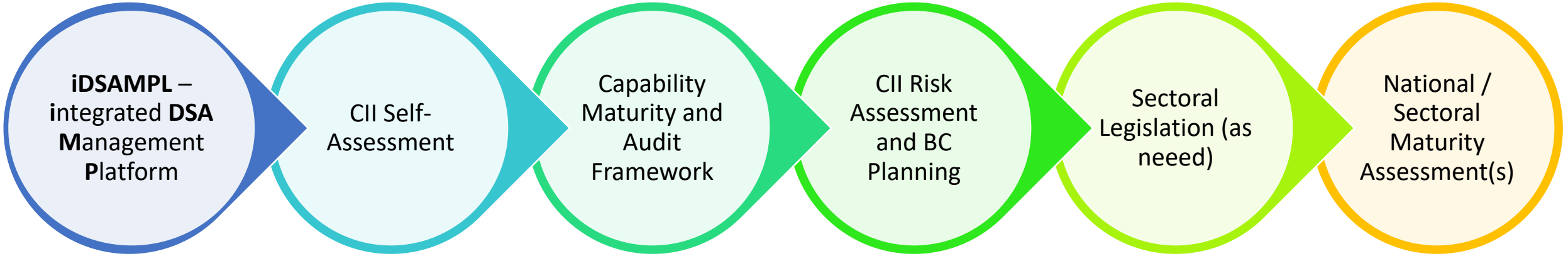
Security Measures Legislation

- 9/2020
- CII Self assessment
- Information Security Officer, Risk Management, Business Continuity
- Supervision framework through the CMAAF project
- Sectoral plugins as necessary

Criticality Reassessment

- 11/2020
- Update to list of OES and CIIs
- Amendments and new entities added where necessary

NIS Directive in Cyprus – Planned Actions 2021



A new platform that has been developed by DSA to manage and handle interactions with OES and CIIs. Modular structure, which entities will access via a web interface.

CII operators are asked to perform a simple self-assessment of their security posture as it relates to the DSA security measures framework.

Development of a capability maturity and audit framework, to specify how the security measures implementation will be supervised in Cyprus (including audit service accreditation).

CII operators must perform a first risk assessment and business continuity planning activity, as specified in the relevant legislation, with submission of appropriate documentary evidence to DSA.

The DSA is closely following relevant European updates and participates in a range of NIS working groups. Sectoral security measures will be specified as and when needs arise (e.g. energy, 5G, health, etc.).

The DSA is planning to perform a series of maturity assessments at the sectoral and/or national levels, to gauge current capability levels and to guide future strategic actions.

Thank you

Questions?

Digital Security Authority (DSA)

Implementation of the NIS Directive in Cyprus

OES / CIIs Compliance Overview

Costas Efthymiou, Technical Officer
Digital Security Authority
https://dsa.cy | https://csirt.cy

Nicosia, 15 December 2020

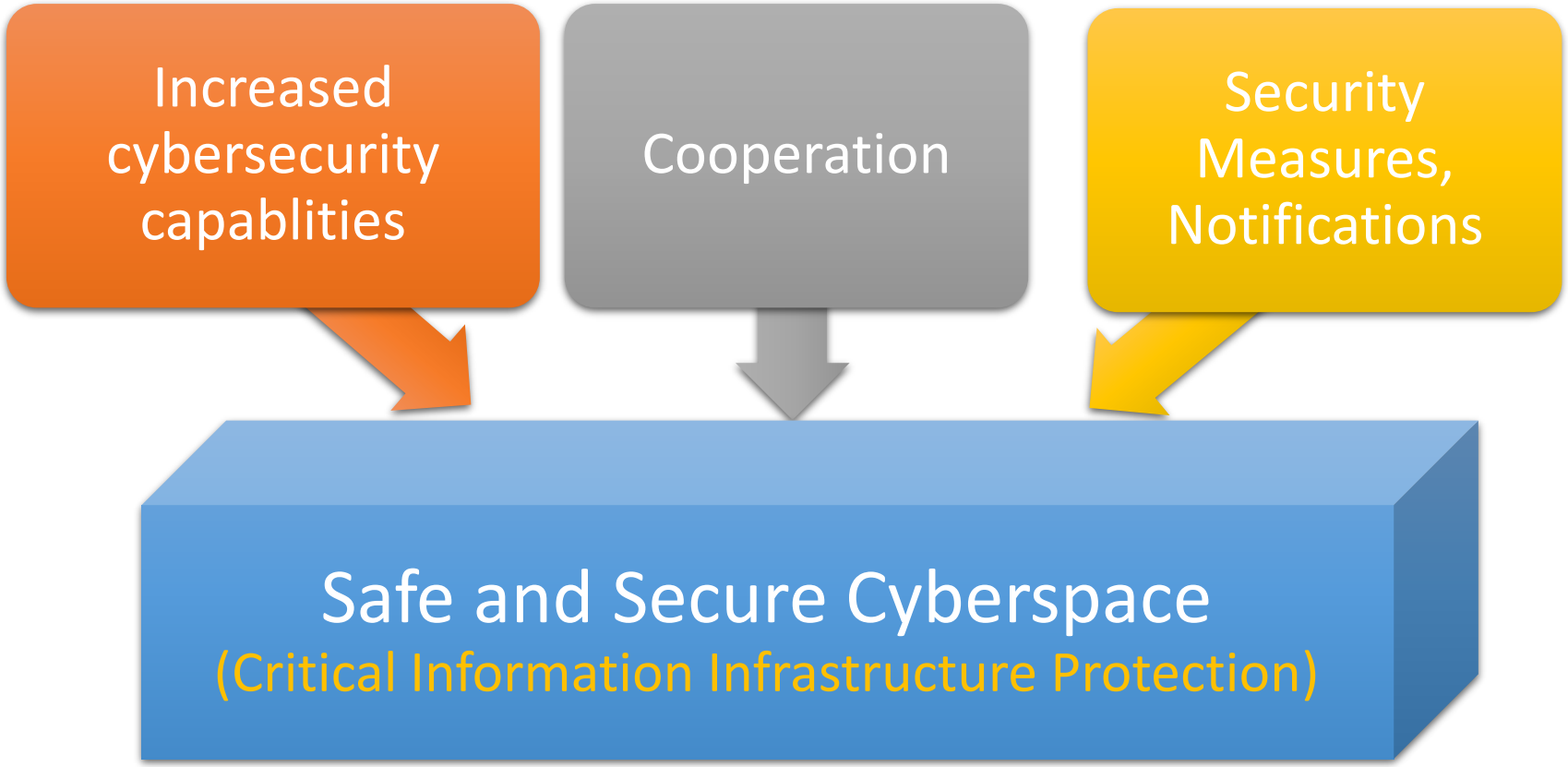
COMMISSIONER OF COMMUNICATIONS | Digital Security Authority

DSA – Who are we?

- Digital Security Authority
  - under supervision of the Commissioner of Communications
- Implementation of the EU NIS Directive in Cyprus
  - It is the Single Point of Contact, the National Competent Authority (for all NIS sectors + electronic communications) and it incorporates the National CSIRT
  - Critical Information Infrastructure Protection
- Coordination of the Implementation of the National Cybersecurity Strategy
  - Cybersecurity/NIS, Cybercrime, Cyberdefence, Related External Affairs
- National Cybersecurity Certification Authority
  - Implementation of the European Cybersecurity Certification Framework in Cyprus

Components of National Cybersecurity Capability

NIS Directive – Main Provisions



Attainment of a satisfactory minimum level of cybersecurity in all critical information infrastructures in Cyprus

DSA Structure

Commissioner of Communications / Deputy Commissioner

DSA Director

Regulation, Strategy and Supervision Team	
- Cybersecurity Strategy	- Audits and supervision
- National Level Cyber Risk Assessment	- Crisis Management
- CII Designation	- Coordination
- Security measures	- Communication
- Incident notifications	- Cooperation
	- Awareness

National CSIRT-CY	
- Alerts and Warnings	- Communication
- Incident Handling	- Cooperation
- Vulnerability Handling	- Awareness
- Artefact Handling	
- Forensic Analysis	
- Crisis Management	

Stakeholders

- Operators of Essential Services (OES)
  - Entities that are defined according to the NIS Directive (energy, transport, health, water, banking/financial, etc.)
- Critical Information Infrastructures (CIIs)
  - Entities that operate other information infrastructures that are considered critical in Cyprus, but are not OES (e.g. sewerage, some governmental services)
- Electronic Communications Providers (ECPs)
  - Entities that operate networks and/or electronic communications services, and are registered at OCECPR
- Digital Service Providers (DSPs)
  - Online search engines, online marketplaces, cloud computing services






DSA in a nutshell

National Cybersecurity Strategy

National Collaboration

Cyber Crisis Management

Operational Coordination

Digital Security Authority

CSIRT-CY

Security Requirements

Incident Reporting

Supervision

European Cybersecurity Strategy

International Collaboration

Cooperation Group

CSIRT Network

OSCE

enisa

EUROPEAN COMMISSION

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Operators of Essential Services (~60)
Energy, Drinking Water, Transport, Health, Banking, Financial, Digital Infrastructure

Digital Service Providers (<20)
Cloud Computing Services, Online Marketplaces, Search Engines

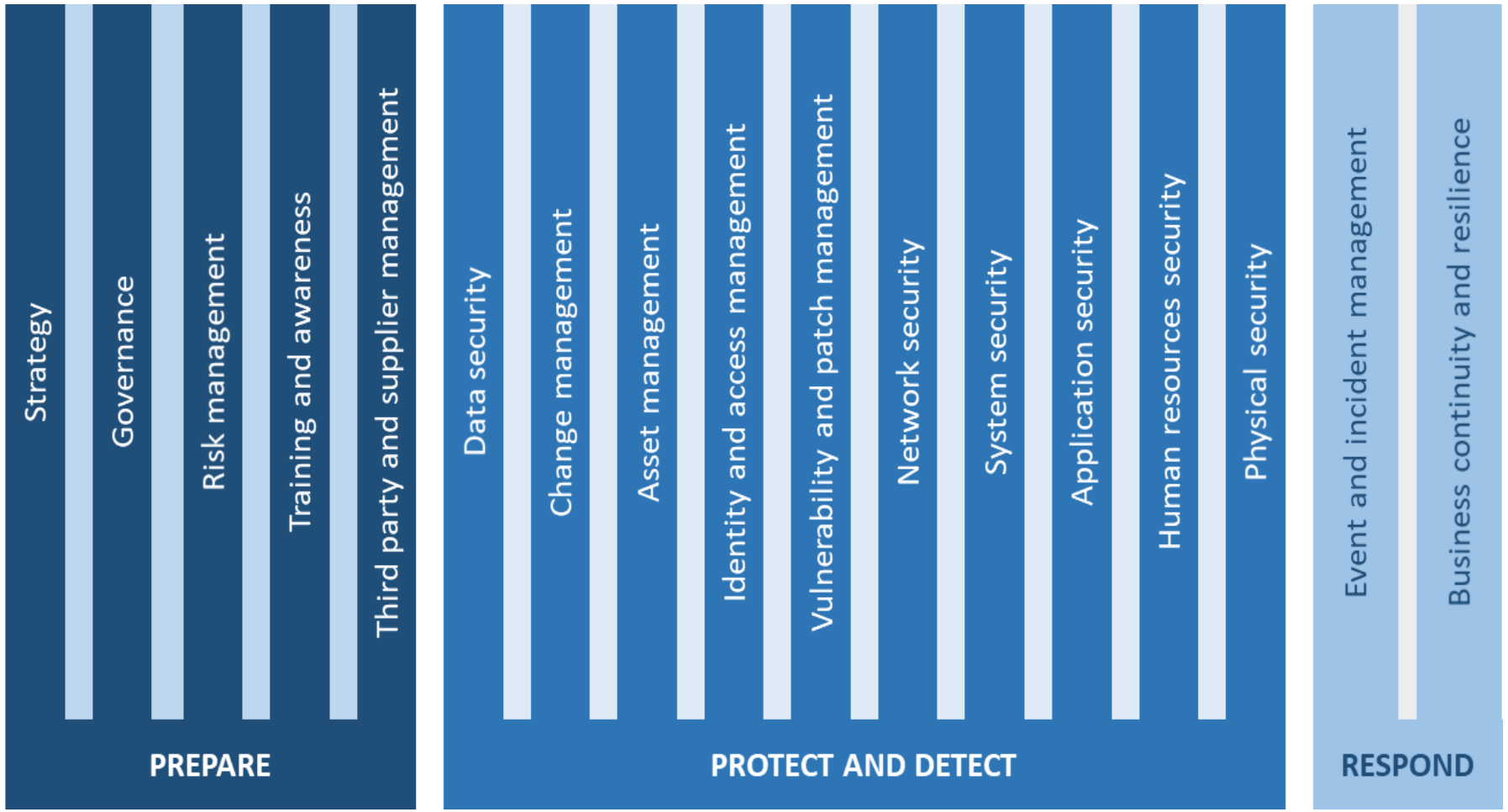
Security Measures Requirements

Prevent Risks	• Organisational measures that are appropriate and proportionate to the risk
Ensure NIS	• The measures should ensure a level of NIS appropriate to the risks
Handle Incidents	• The measures should prevent and minimise the impact of incidents on the IT systems used to provide the services

Security Measures – DSA Principles

- Based on current international standards, best practices and guidelines
  - including NIS Cooperation Group requirements
- Horizontal approach
  - Additional sectorial requirements will follow in the future, where needs arise
- Security Posture based on defined risk management processes
  - Security Strategy, Risk Reporting and Business Continuity
- Full spectrum
  - Activities include Preparation, Protection and Detection, Response and Recovery
- Control Framework
  - Definitions and mapping to relevant ISO/IEC and NIST standards, as well as coverage of NIS Cooperation Group Work Stream documents

Security Measures - Controls



PREPARE - Ensure OES and CIIs are taking into account information security risk in day-to-day operations and ensure top-level management commitment to address security threats, vulnerabilities and risks

PROTECT AND DETECT - Ensure OES and CIIs establish, implement and maintain adequate information security measures appropriate to their risk exposure. Adoption of preventive, detective and reactive measures from a technological, administrative and physical perspective

RESPOND - Ensure OES and CIIs are able to respond to information security events and incidents that could affect the confidentiality, integrity, availability or authenticity of information. Adoption of operational resilience and business continuity and disaster recovery measures, as well as restoration to normal operations

Security Measures - Compliance Timeline

Incident Notification – High-Level Requirements

Operators of Essential Services / CIIs	• Incidents having a significant impact on the continuity of the essential services they provide
Digital Services Providers	• Incidents having a substantial impact on the provision of a service

Incident Notification - Process

Incident

- Check notification thresholds
- Mandatory or voluntary notification

Initial Notification

- Basic incident and impact Information (within 6 hours)
- Request for assistance from CSIRT-CY (if necessary)

Intermediate Notification

- Additional information as the incident develops (optional)
- Can be used to update information for long incidents

Final Notification

- Final (analysed, accurate) incident report, with action plan
- Within 15 days of incident resolution and services restored

Legislative References – CY and EU

- **DSA Legislation**
  - Law 89(I)/2020 on Network and Information Systems Security - https://dsa.cy/wp-content/uploads/DSA-Law-89-I-2020.pdf
  - Decision 389/2020 on Security Measures for Operators of Essential Services and Critical Information Infrastructure Operators - https://dsa.cy/wp-content/uploads/Decision-389-2020.pdf
  - Decision 218/2019 on Incident Notification - https://dsa.cy/wp-content/uploads/Decision-218-2019.pdf
  - Security legislation for electronic communications - https://dsa.cy/el/legislation/ec-security-legislation/
- **NIS Directive**
  - Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union - https://eur-lex.europa.eu/eli/dir/2016/1148/oj
  - Commission Implementing Regulation (EU) 2018/151 laying down rules for application of Directive (EU) 2016/1148 as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.026.01.0048.01.ENG
- **EU Cybersecurity Act**
  - Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act)
  - https://eur-lex.europa.eu/eli/reg/2019/881/oj
- **DSA (upcoming legislation)**
  - Relevant public consultations - https://dsa.cy/el/category/public-consultations/

Thank you

Questions?

Contact Information

- Digital Security Authority, Cyprus
  - NIS Competent Authority
  - Single Point of Contact (NIS)
  - Includes National CSIRT-CY
  - Coordinator of National Cybersecurity Strategy
  - Electronic Communications Security Supervision
  - National Cybersecurity Certification Authority
- **Costas Efthymiou**
  - Technical Officer at the DSA
  - costas.efthymiou@ocecpr.org.cy
  - +357 22693169
- https://dsa.cy/en


Logicom
Solutions
HOW TOS
ACHIEVING COMPLIANCE BY CRITICAL INFRASTRUCTURES
AGAINST THE SECURITY MEASURES DEFINED IN THE LAW

The First Cybersecurity Legislation Passed by the European Union

It aims to achieve a high common standard of network and information security across all EU Member States.

August 2016

- The Directive is adopted and taken into effect by EU.
- EU Member States have 21 months to integrate its requirements into their own national laws

April 2018

- Cyprus formulates the Digital Security Authority which is responsible for the enforcement of the NIS Directive.

August 2020

- The law for the enforcement of the NIS directive is taken into effect.

Ο ΠΕΡΙ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΝΟΜΟΣ ΤΟΥ 2020

Logicom Solutions

What is the NIS directive?

Europe needs to safeguard against cyberattacks

The aim of the NIS Directive is to ensure a high common level of cybersecurity across the EU.

The Commission recognised that cybersecurity incidents are increasing in frequency and magnitude, and becoming more complex and cross–border in nature.

The NIS Directive is a key component of the overall strategy to prevent and respond to cyber disruptions and attacks.

What members states should do

Assign a national single point of contact on security of networks and information systems	A CSIRT responsible for handling risks and incidents
Network and Information Security strategy	A national competent authority to monitor the application of the NIS Directive

Logicom Solutions

What is the role of National Digital Security Authority?

Supervisory, Advisory, Coordinating, Monitoring, Enhancing

DIGITAL SECURITY AUTHORITY

SUPERVISORY ROLE for the different stakeholders

INCIDENT MANAGEMENT for Cybersecurity events

Acts as a **SINGLE POINT OF CONTACT** between other states for cybersecurity issues

Ensure that Critical Infrastructures in Cyprus are taking the appropriate **CYBERSECURITY CONTROLS** to protect their data, systems, operations.

COORDINATION OF LOCAL AUTHORITIES for responding to Cybersecurity incidents and alignment with the **National Cybersecurity Strategy**

IMPOSE ADMINISTRATIVE FINES on any person / entity that violates the provisions of this law

Validates the **effectiveness of the national CSIRT**

Ensures **that Cis are communicating on time any incidents**.

Coordinates with **DATA PRIVACY COMMISSIONER**

Acts as a **CYBERSECURITY ADVISOR** for national authorities and government officials

NIS DIRECTIVE CYPRUS

Logicom Solutions

Which industries are being affected?

Energy, Transport, Health, Banking, Digital Service Providers

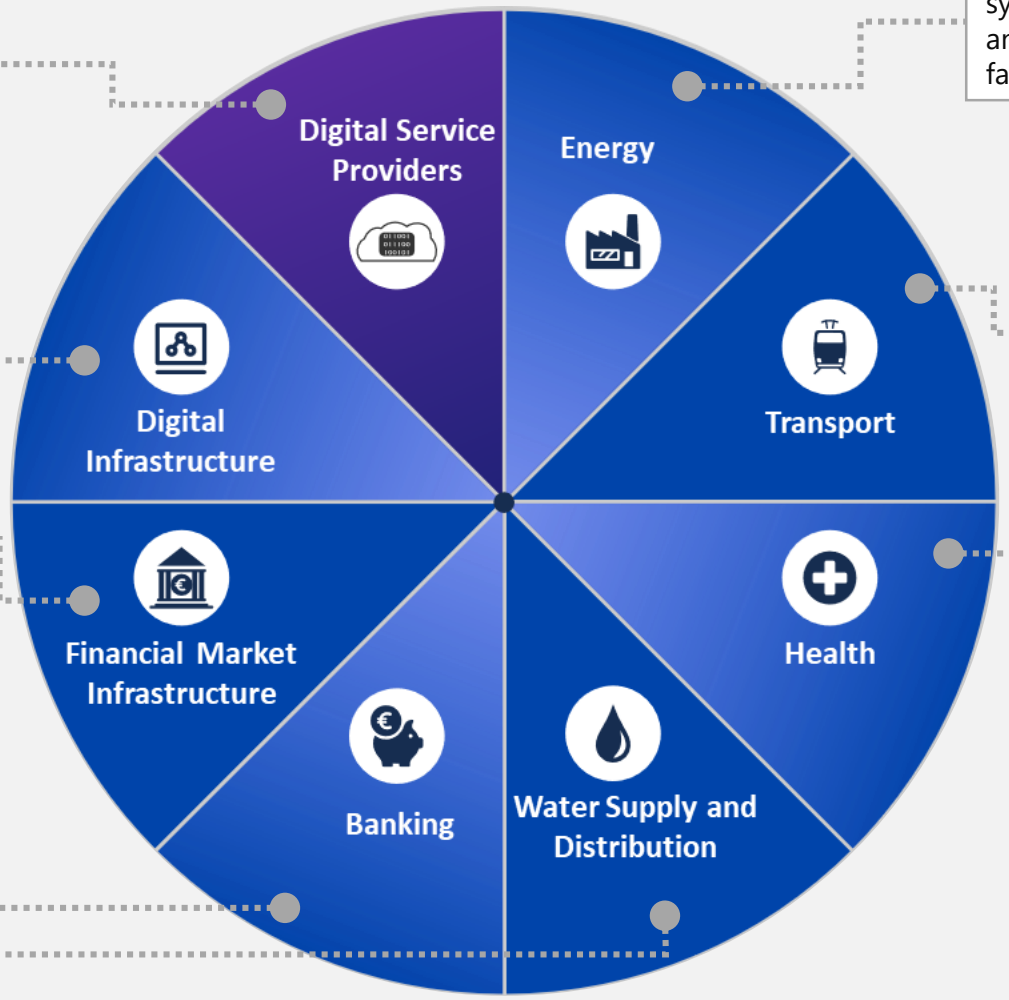
Cloud service providers, Search Engines, Online Market Places

Internet exchange points, top level domain name registries, and domain name system service providers

Stock exchanges and central counterparties

Credit institutions in accordance with the Capital Requirements Regulation

Entities in the drinking water supply and distribution sector



Electricity/gas suppliers and distribution system operators, transmission system operators, storage system operators, LNG operators, and operators of oil and natural gas production, refining and treatment facilities

Air and maritime carriers, traffic management control operators, airports, railways, road traffic management control and intelligent transport system operators

Healthcare providers (including hospitals and private clinics)

NIS

DIRECTIVE CYPRUS

Logicom Solutions

What are the requirements?

12 areas that CI needs to cover

CISO OFFICE

1. GOVERNANCE & RISK ASSESSMENT
2. ASSET MANAGEMENT
3. SYSTEM AND APPLICATIONS
4. IDENTITY ACCESS CONTROL
5. NETWORK PROTECTION
6. DATA SECURITY
7. VULNERABILITY MANAGEMENT
8. BUSINESS CONTINUITY
9. THIRD PARTIES & SUPPLY CHAIN
10. HR SECURITY
11. PHYSICAL CONTROLS
12. INCIDENT RESPONSE

Logicom Solutions

#	PHASE	SECURITY MEASURES SECTION	1 GOVERNANCE & RISK ASSESSMENT	2 ASSET MANAGEMENT	3 SYSTEM AND APPLICATIONS	4 IDENTITY ACCESS CONTROL	5 NETWORK PROTECTION	6 DATA SECURITY	7 VULNERABILITY MANAGEMENT	8 BUSINESS CONTINUITY	9 THIRD PARTIES & SUPPLY CHAIN	10 HR SECURITY	11 PHYSICAL CONTROLS	12 INCIDENT RESPONSE	
1	**PREPARE**	Strategy	•												✓
2	**PREPARE**	Governance	•												✓
3	**PREPARE**	Risk management	•												✓
4	**PREPARE**	Training and awareness										•			✓
5	**PREPARE**	Third party and supplier management									•				✓
6	**PROTECT AND DETECT**	Data security						•							✓
7	**PROTECT AND DETECT**	Change management	•												✓
8	**PROTECT AND DETECT**	Asset management		•											✓
9	**PROTECT AND DETECT**	Identity and access management				•									✓
10	**PROTECT AND DETECT**	Vulnerability and Patch Management							•						✓
11	**PROTECT AND DETECT**	Network security					•								✓
12	**PROTECT AND DETECT**	System security			•										✓
13	**PROTECT AND DETECT**	Application security			•										✓
14	**PROTECT AND DETECT**	Human resources security										•			✓
15	**PROTECT AND DETECT**	Physical security											•		✓
16	**RESPOND**	Event and incident management												•	✓
17	**RESPOND**	Business continuity and resilience								•					✓

Some details on the requirements of each area

Critical Infrastructures are expected to have the following controls

1 GOVERNANCE & RISK ASSESSMENT

- Information Security Strategy
- Information Security Policy Framework
- Roles & Responsibilities
- Compliance with standards / regulations
- Risk Assessment
- Change Management Processes

2 ASSET MANAGEMENT

- Asset Inventory and Ownership
- Asset Lifecycle
- Asset Monitoring
- Availability Monitoring
- Capacity Monitoring

3 SYSTEM & APPLICATION PROTECTION

- Anti-Malware Protection controls
- Configuration and Hardening Guides
- Remote Access and MDM
- Updates and Patch Management
- Development environments

Logicom Solutions

Some details on the requirements of each area

Critical Infrastructures are expected to have the following controls

4 IDENTITY ACCESS CONTROL

- Authentication Mechanisms
- Access Rights of users
- Privileged Users Management
- Strong Authentication Controls (MFA)
- Credentials Management
- Traceability and audit trail

5 NETWORK PROTECTION

- Network Segmentation
- Denial of Service Protection
- Network Access Controls
- High Availability of network
- Intrusion Prevention Mechanisms
- Encryption

6 DATA SECURITY

- Data Lifecycle
- Data Classification
- Data Leakage Prevention
- Data Transfer Controls
- Data Backups and Restoration

Some details on the requirements of each area

Critical Infrastructures are expected to have the following controls

7 VULNERABILITY MANAGEMENT

- Vulnerability Scanning
- Penetration Testing
- Documentation and prioritization
- Remediation and patching
- Management involvement / decisions
- Validation of fixes

8 BUSINESS CONTINUITY

- Business Impact Analysis
- Business Continuity Plan
- Disaster Recovery Plan
- Simulation of disaster events

9 THIRD PARTIES & SUPPLY CHAIN

- Due Diligence of third parties
- Enforcement of access control rules
- Monitoring of access / activities
- Regular vendor assessment

Logicom Solutions

Some details on the requirements of each area

Critical Infrastructures are expected to have the following controls

10 HR SECURITY

- Information Security Awareness Session
- Phishing Email Campaigns
- Employment Lifecycle and Monitoring
- Acceptable use and disciplinary actions
- Communication of Infosec Policies

11 PHYSICAL CONTROLS

- Environmental controls
- Perimeter controls
- Internal Controls
- Cabling and equipment protection

12 INCIDENT RESPONSE

- Technologies to detect
- Readiness to analyse and evaluate
- Incident notification / collaboration
- Controls to respond
- Post-incident activities

What if we do not comply?

What are the consequences in the event that we do not comply?

!

NATIONAL SECURITY

NATIONAL ECONOMY

SOCIAL WELLBEING

HEALTH AND SAFETY

ENVIRONMENT

Logicom Solutions

What if we do not comply?

What are the consequences in the event that we do not comply?

Failure to take appropriate and proportionate technical and organisational measures to manage the risks posed to the organization may also lead to administrative fines by DSA or be found as Criminally liable.

ADMINISTRATIVE FINES IMPOSED BY DSA

€200,000

for any infringement of the Cyprus NIS Law

€10,000

for each day the infringement persists

CRIMINAL LIABILITY

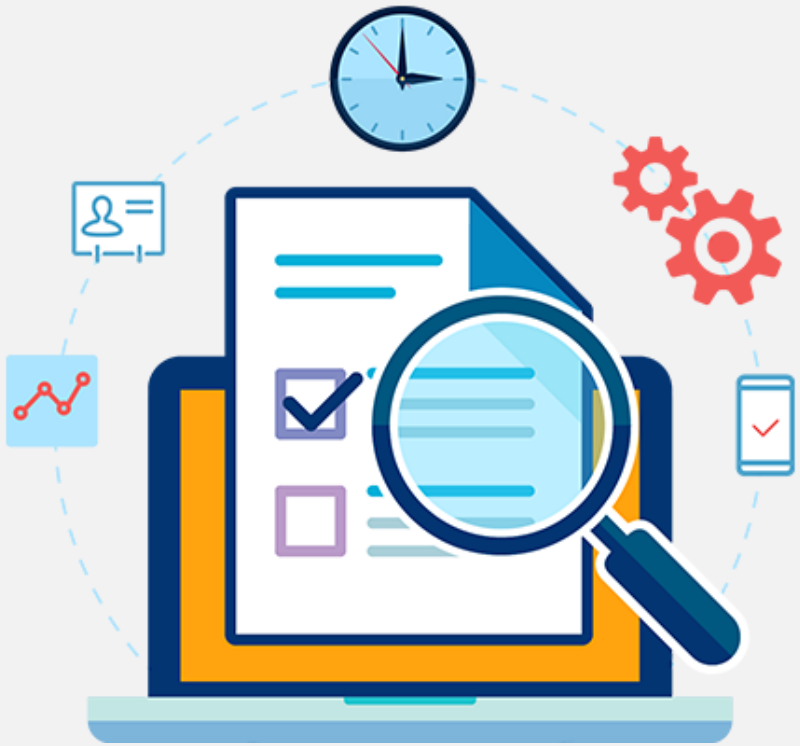
Imprisonment of up to **3 years**

and/or a fine of up to **€15,000**

Logicom Solutions

Main challenges and key risks

It is not just another cybersecurity project. Now is different.



Shortage of professionals with specifics skills and expertise in cyber risk management within Cyprus market.

NIS includes a substantial number of controls to be implemented, targeting organizations that are at a low maturity level in Cybersecurity.

The development / maintenance of NIS Controls requires experience in infosec governance along with strong technical knowledge.

Implementation of all controls can have a significant cost and minimum benefit if not implemented properly.

Implementation requires the involvement of multiple stakeholders from different layers of the organization and externals, which can include additional complexity.

Logicom Solutions

How we can help

A team of cybersecurity professionals can work with you on this

Information Security Management ISO 27001 Certified · CISSP® · OFFENSIVE security OSCP · CISA · OFFENSIVE security OSWP · OFFENSIVE security OSWE · ...

A highly qualified and certified Team of Information Security Professionals, with deep technical knowledge along with strong understanding of Business processes and needs, carrying valuable experience from projects across different industries. We have also certified our self's with ISO27001.

A strong team of professionals can support you in complying and safeguarding your operations, systems and data.

Our methodology works. We can work together to strategize, and achieve a significant progress in a relatively short period of time.

We are the only Cybersecurity Consulting team in Cyprus that combines a strong governance and technical knowledge.

Logicom Solutions

How we can help?

Europe needs to safeguard against cyberattacks

Our team follows a methodological approach, to provide assurance on your compliance journey.

70% compliance can be achieved in the first months of our work

We are offering a suite of technologies and services tailored for your environment through streamlined operations.

Logicom Solutions

OUR METHODOLOGY

We can drive you all the way

1 DISCOVERY

2 ASSESSMENT

Logicom Solutions

How we can help

What CIs should be aware before working on the security measures

VULNERABILITY ASSESSMENT

Discover → Review → Gap Assessment

SECURITY ARCHITECTURE REVIEW

Discover → Review → Gap Assessment

INFOSEC GOVERNACE REVIEW

Discover → Review → Gap Assessment

RISK ASSESSMENT

RISK TREATMENT PLAN

Logicom Solutions

OUR METHODOLOGY

We can drive you all the way

1 DISCOVERY

2 ASSESSMENT

3 ROADMAP

Logicom Solutions

OUR METHODOLOGY

We can drive you all the way

1	DISCOVERY
2	ASSESSMENT
3	ROADMAP

4	CISO as a Service
a	PLANNING
b	DESIGN
c	EXECUTE
d	TRACKING
e	REPORT
f	ADVISE

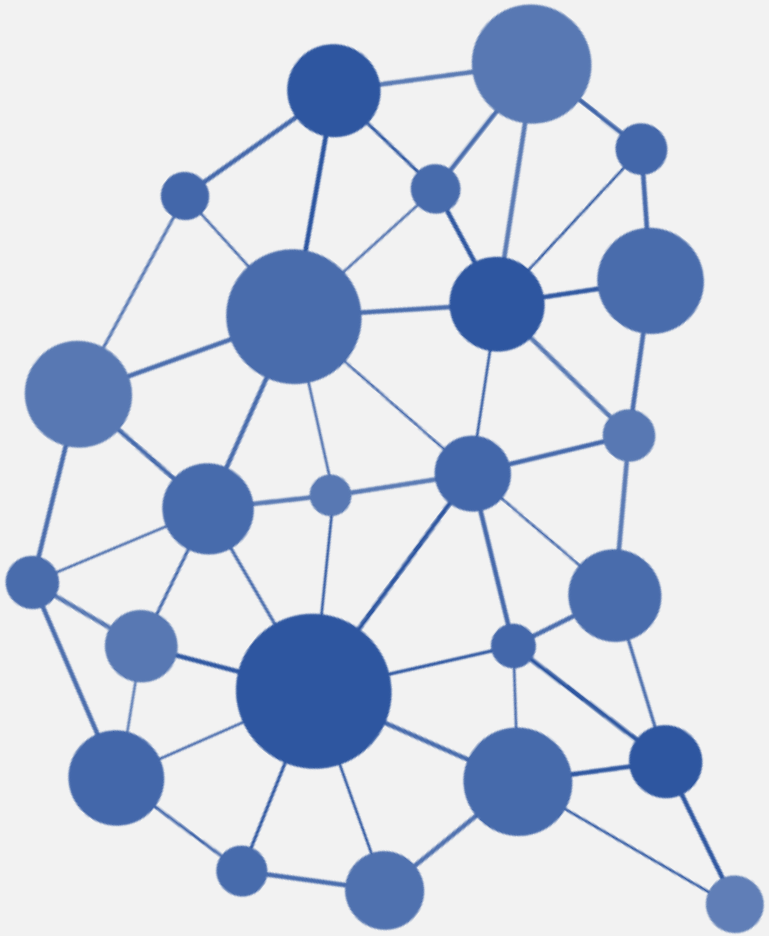
1 YEAR PERIOD

Logicom Solutions

How we can help

What is your current maturity level

We will assess the current maturity level of your organization for each of the 12 areas.



1 INITIAL	First very low level of policies, tending to be driven in an ad-hoc, uncontrolled, and reactive manner. On the fly implementations.
2 DEVELOPING	Adhoc policies, no well organized, in progress. A governance programme is being followed but is not established.
3 DEFINED	Policies exist, are communicated to all personell, are accessible and being followed by the employees.
4 MANAGED	Being regularly monitored, exceptions investigated, automation of tools, constant improvement.
5 OPTIMIZING	Processes have been refined to a very good level, automation and workflows implemented.

Where you stand now

The current maturity level on infosec to be estimated

1	INITIAL
2	DEVELOPING
3	DEFINED
4	MANAGED
5	OPTIMIZING

Where you can be in the next months

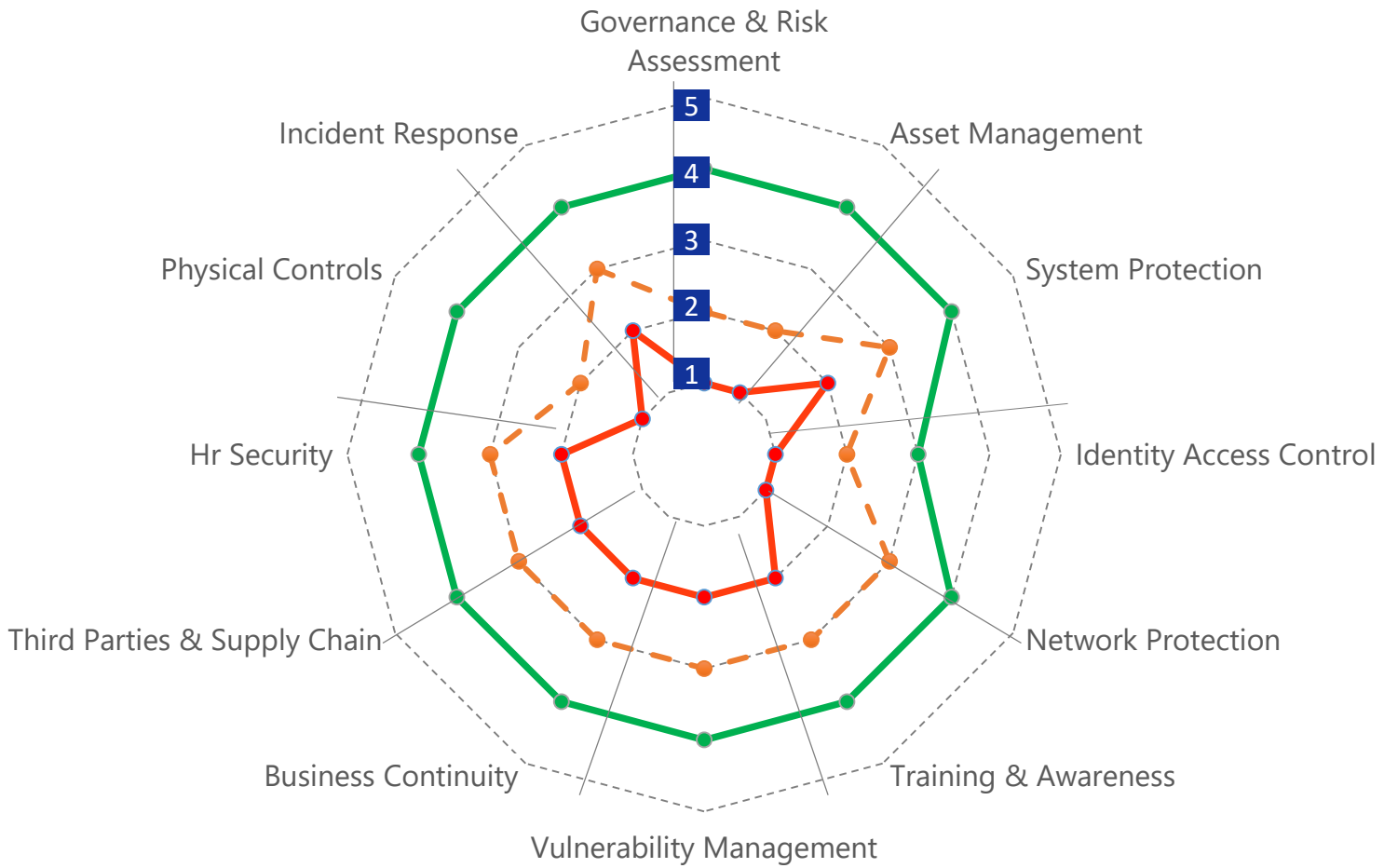
A forecast based on the strategic plan that will be proposed

1	INITIAL
2	DEVELOPING
3	DEFINED
4	MANAGED
5	OPTIMIZING

What is the target for the end of the year

A forecast based on the strategic plan that will be proposed

1	INITIAL
2	DEVELOPING
3	DEFINED
4	MANAGED
5	OPTIMIZING



Logicom Solutions

OUR METHODOLOGY

We can drive you all the way

1. DISCOVERY
2. ASSESSMENT
3. ROADMAP

4. CISO as a Service
   - a. PLANNING
   - b. DESIGN
   - c. EXECUTE
   - d. TRACKING
   - e. REPORT
   - f. ADVISE

\+ SOLUTIONS

1 YEAR PERIOD

MANAGED SECURITY SOLUTIONS CENTER

- Execution of Adversary Attack Simulation Services
- Cloud or On Premise Continuous Vulnerability Assessment
- Partnership 24x7 Monitoring Center (SOC)
- Utilising KnowBe4 Platform
- Ready to be launched in 2021.
- Partnership with Veracode

BUSINESS CONSULTING SERVICES

Logicom Solutions

CHARIS FLORIDES
CISSP, OSCP, MSc in InfoSec

Manager
Business Consulting Services
Logicom Solutions

Board Member
ISC2 Cyprus Chapter

email address
c.florides@logicom.net

Linkedin Profile
charis.florides

Logicom Solutions

For your questions, please use the Q&A!

Logicom Solutions

Thank you for your attention!

For more information, contact us at solutions@logicom.net