ODYSSEY
Impossible Challenges, Possible Solutions

# How to create an effective Information Security Program

Dimitris Mouzakitis - Senior Information Security Consultant

CISM, CRISC, ISO 27001 Auditor/ Lead Auditor

March 30th, 2017

# What is an Information Security Program?

An Information security program is the exercise of **designing and implementing** security practices to protect critical business processes and information assets across the organization.

# What is an Information Security Program?

Its objectives, among others, are to:

- Protect the organization and its information assets by keeping security at a **desired level**
- Manage risks by identifying assets, discovering threats and estimating the risk
- Provide direction for security by documenting security policies, procedures, etc.
- Plan and justify budgets and resources related to security
- Assess effectiveness of the implemented controls by using metrics and indicators.

# The Process for an Effective Information Security Program

## Vision Statement

Definition of the “**Desired State**” for security. This is the vision of what the strategy aims to achieve during a defined period.

# The Process for an Effective Information Security Program

## Business Strategy

The Information Security strategy is, on a great degree, influenced by the organization’s business strategy.

# The Process for an Effective Information Security Program

## Environmental Trends

Trends in the economic, business, market, regulatory, political and technology environments can have a great impact on the security risk facing the enterprise.

# The Process for an Effective Information Security Program

## Current-State Assessment

Assess the overall effectiveness and efficiency of security in the enterprise by performing:

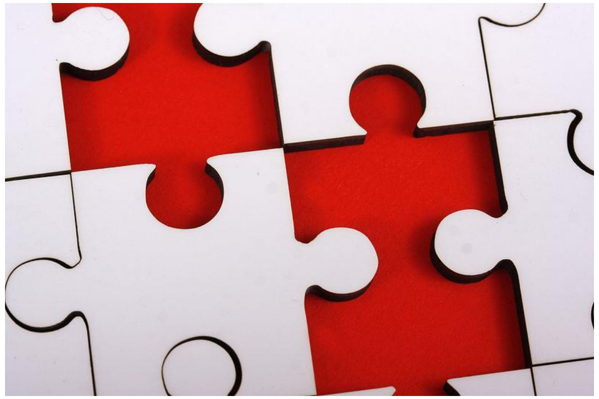
- Vulnerability assessments and penetration tests to assess the technical infrastructure
- Risk assessments to balance the investment on controls appropriate to the actual risks
- Internal and external audit results to assess the effectiveness of policy and controls compliance

and more

# The Process for an Effective Information Security Program

## Gap Analysis

Consists of mapping the current state against the vision statement, identifying the gaps between the two states in order to derive the actions and projects required to close these gaps.



# The Process for an Effective Information Security Program

## Prioritization

Almost no organization will have the resources required to execute on all of the identified projects and activities. Prioritization criteria include the following:

- The level of risk reduction potentially achieved by a given project/activity

- The resources (skills, staff and systems) required

- The financial cost

- The "time to value", the period between the initial investment and the point at which the project will start accruing value to the organization.

# The Process for an Effective Information Security Program

## Approval

The final step is to obtain executive approval and budget. The strategy shall be communicated using a written report and an executive presentation clearly describing the current state, the desired state, and how the projects with their respective phases and milestones will help to achieve the desired state.

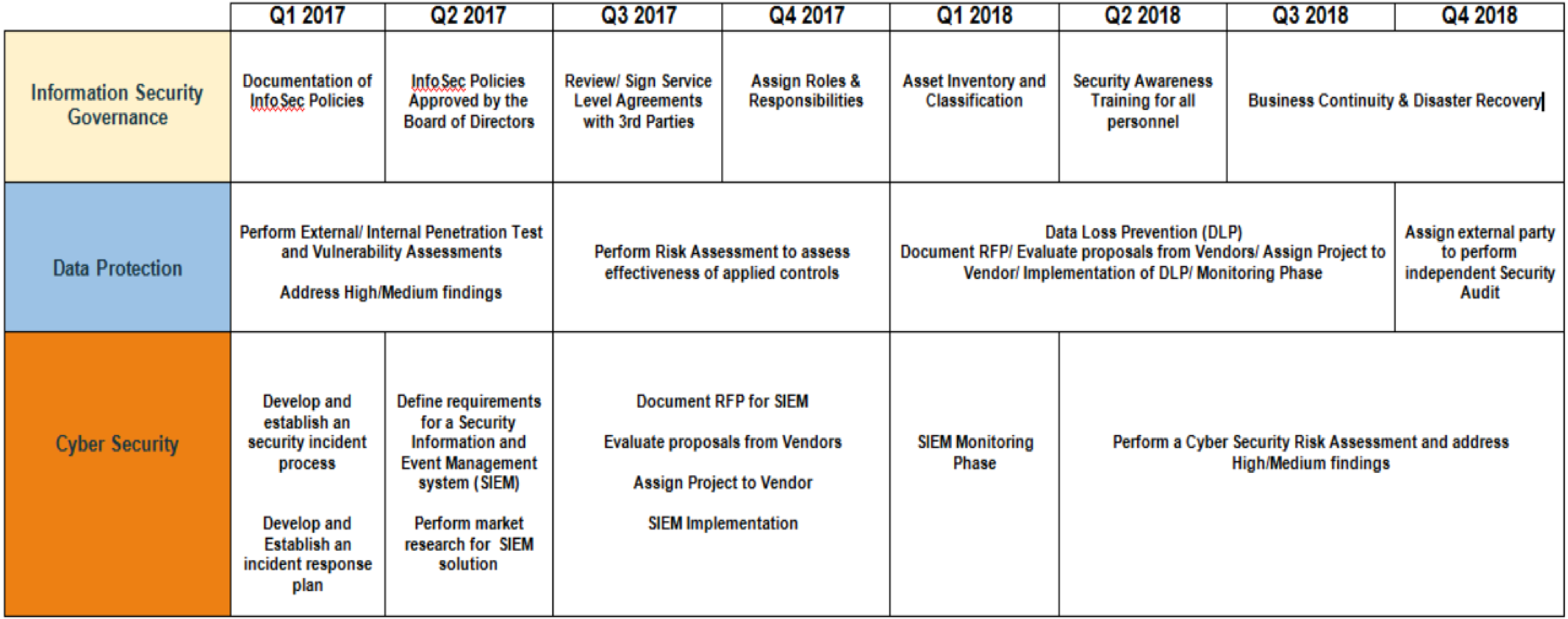
# The Process for an Effective Information Security Program

## Review & Reporting

A key part of maintaining support for the security program is effective and continuous review and reporting on the progress of the program.

Progress should be reported to the Upper Management on a quarterly basis.

# Example of an Information Security Program



| | Q1 2017 | Q2 2017 | Q3 2017 | Q4 2017 | Q1 2018 | Q2 2018 | Q3 2018 | Q4 2018 |
|---|---|---|---|---|---|---|---|---|
| Information Security Governance | Documentation of InfoSec Policies | InfoSec Policies Approved by the Board of Directors | Review/ Sign Service Level Agreements with 3rd Parties | Assign Roles & Responsibilities | Asset Inventory and Classification | Security Awareness Training for all personnel | Business Continuity & Disaster Recovery | |
| Data Protection | Perform External/ Internal Penetration Test and Vulnerability Assessments<br>Address High/Medium findings | | Perform Risk Assessment to assess effectiveness of applied controls | | Data Loss Prevention (DLP)<br>Document RFP/ Evaluate proposals from Vendors/ Assign Project to Vendor/ Implementation of DLP/ Monitoring Phase | | | Assign external party to perform independent Security Audit |
| Cyber Security | Develop and establish an security incident process<br>Develop and Establish an incident response plan | Define requirements for a Security Information and Event Management system (SIEM)<br>Perform market research for SIEM solution | Document RFP for SIEM<br>Evaluate proposals from Vendors<br>Assign Project to Vendor<br>SIEM Implementation | | SIEM Monitoring Phase | Perform a Cyber Security Risk Assessment and address High/Medium findings | | |

# THANK YOU

WWW.ODYSSEYCS.COM

ODYSSEY

ODYSSEY
Impossible Challenges, Possible Solutions

## HEADQUARTERS

**CYPRUS**
1 Lefkos Anastasiades str.,
2012 Strovolos, Nicosia
Tel.: +357 22463600
Fax: +357 22463563

## OFFICES

**GREECE | SERBIA | DUBAI | USA | SOUTH AFRICA**