


# Manage your Digital Risks with **ONE** Strategic Partner

**Advisory Services and beyond**



In **Gartner**  
Magic  
Quadrant.





## In the era of Digital Transformation, Digital Risks emerge faster than you can adapt.

Unequivocally, Digital Transformation presents organizations with rewarding opportunities. Equally clear is the fact that it creates an even greater dependency on an increasingly complex organizational IT ecosystem. Consequently, it brings the matter of Digital Risk Management and Information Security to a whole new criticality level; the Board's level.

As digital operations become the organization itself, managing Digital Risk and Information Security must be considered while business strategy and objectives are being formulated, not separately. Thus, they are the new hot issue to make it onto the Board's agenda.

To reap the benefits of Digital Transformation without sacrificing Information Security, you need **ONE** Strategic Partner with **ONE** Holistic Approach and a sole specialty in Cloud & Information Security to help you defend your digital ecosystem.

**Odyssey,**  
**ONE Strategic Partner to take you beyond**

# Discover

---

1

## Digital Transformation

---

3

Opportunities & Challenges of Digital Transformation.

2

## ONE Strategic Partner

---

6

Odyssey's Advisory Services holistic approach.

3

## Solutions & Services Pillars

---

8

Odyssey's five pillars.

4

## ClearSkies™ Threat & Vulnerability Management Platform

---

10

Deliver real-time visibility of organizations security posture.

5

## Ingredients of Success

---

11

The key ingredients for Digital Transformation Success.

6

## Address your Digital Risks

---

12

Digital Risks categories and focus areas.

7

## ONE Methodology

---

15

Understand our Cloud and Information Security methodology.

# Digital Transformation

---

## Managing the new Threat Landscape

---

The digital era is here, therefore Digital Transformation is no longer a choice for organizations, but rather the **ONLY** approach which will safeguard their very survival. Along with the business advantages it brings however, Digital Transformation further accelerates the rate by which the information-threat landscape expands, creating more and new lucrative opportunities for threat-actors.

To address this challenge, modern organizations are escalating the **“Digital Risk Management”** and **“Zero Trust”** discussion, pushing it beyond the confines of the internal Cloud and Information Security functions and onto the Board’s agenda.



A study by the Ponemon Institute reveals that the rush to achieve Digital Transformation increases the risks of a data breach by 72%, and cyberattack or threats to high-value assets by 65%.



## Opportunities & Challenges of Digital Transformation

---

As more and more organizations embark on their Digital Transformation journey to reach new levels of customer experience, deliver new products and services, optimize operations and their decision-making processes, reduce costs, and ultimately increase profit margins, they become increasingly reliant on technology and third-party technology providers/partners.

Along with the opportunities this transformation presents, it creates an entirely new playing field in which traditional Cloud & Information Security practices become irrelevant or less effective.

“To meet the challenges of the digital era, the Information Security function can no longer work from an approach where it has to be aligned with business strategy and objectives; Now, security needs to be considered while business strategy and objectives are being formulated.”

Therefore, as organizational digital boundaries blur, formulating a complex digital ecosystem where internal, cloud and external parties are practically indistinguishable, the question of “**who is to be trusted**” becomes abundantly clear - **No One**. The transition to the “**Zero Trust**” culture is no longer a discussion. It is fast becoming the new norm in Cloud & Information Security strategy for any organization.

Furthermore, the fast-track operational mode that is the end goal of Digital Transformation allows no time or room for mistakes and second guesses, including decisions pertaining to Cloud & Information Security. Evidently, “**Secure & Resilient by Design**” not only makes sense, but it is a critical success factor towards successful Digital Transformation.

Odyssey’s **Advisory Services** are specifically designed to help you adopt this new mindset and to reap the benefits of Digital Transformation without sacrificing Information Security nor having to invest heavily in maintaining your security posture.

Choosing this direction ensures successful Digital Transformation while it also demonstrates that the fiduciary responsibilities and obligations of your Board are truly exercised towards supporting an Information Security agenda that continuously aims at protecting and safeguarding the security, availability and integrity for your organization’s digital assets.

**“Secure & Resilient by Design” and “Zero Trust” - The cornerstones of Cloud & Information Management for the Digital Transformation era.**



Organizations now need to shift their Cloud & Information Security practices to cater to the “**Zero Trust**” and “**Secure & Resilient by Design**” mindset by appropriately **Re-Visiting and Re-Thinking their strategy.**

# Re-Visit & Re-Think your strategy

While you take the Digital Transformation leap towards capitalizing on your information assets, we go **beyond** traditional consulting practices to help you design security and resilience into your overall digital business strategy: “**Secure & Resilient by Design**”.

This strategy assists you, not only in addressing the critical questions towards making the right choices, but also in designing and implementing practices that enable you to efficiently and effectively manage the “**Operational Risk**” emanating from the fast-expanding information-threat landscape.



You need **ONE Strategic Partner** by your side, with a single focus and a sole specialty, to go beyond traditional consulting to help you design security and resilience into your overall digital business strategy.

*Eleftherios Antoniadou,  
CTO Odyssey*

# ONE Strategic Partner

## ONE Holistic Approach

Odyssey's **Advisory Services** provide a holistic 360° approach to Cloud & Information Security designed to effectively address the digital risks posed during and after your Digital Transformation journey. This approach, which not only complements, but also enhances your organization's Operational Information Security and Risk Management effort, **delivers the level**

**of assurance required to securely conduct your business in the digital era.**

Each of the five pillars, both separately or combined, can provide you with the solutions and services necessary to enable you to manage Digital Risk, including the ever-expanding information-threat landscape, in all operational aspects of your organization: **People, Process and Technology.**



Figure 1: Odyssey's 360° approach to Cloud & Information Security



## Advisory Services and beyond

For more than two decades, we have helped organizations of different sizes and industries globally to formulate and manage their Cloud & Information Security strategy.

We understand their challenges, are aware of the new horizons they explore, and have delved into the big questions emanating from their emerging needs. Digital Transformation is an **opportunity** of paramount importance for any modern organization. From an Information

Security standpoint, it is **also a monumental challenge**.

Therefore, remaining true to our longstanding **“Core Values”** and **“Principles”** of anticipating our clients’ needs and consistently offering them cutting-edge innovative solutions and services, we have adapted our **Advisory Services** to assist them in effectively managing Digital Risk, which is Information Risk in the Digital Transformation era.

We help you adopt the right practices that empower you to work smarter rather than harder.

Through the **“Secure & Resilient by Design”** approach, and in adopting the **“Zero Trust”** paradigm, we assist organizations in formulating their business and Information Security processes, controls and policies so that they can build security and resilience **into** their IT management processes, and not **on top of** them.

When you engage with our **Advisory Services**, you tap into the advantages offered by our 360° approach to Cloud & Information Security, as well as our foresight on how you can achieve your business goals by turning Digital Transformation into an opportunity rather than a necessary evil.



**“Secure & Resilient by Design”** ensures that procedures, controls and policies are built into the evolving IT ecosystem, enabling your organization to **continually Manage, Monitor, and Maintain your Information Risk posture**.



# Solutions & Services Pillars

---



## Managed Security Services (MSS)

---

Odyssey's **Managed Security Services (MSS)** are designed to serve as a remote extension of your security operations, essentially supporting you in maintaining your digital infrastructure in an optimal operational and effectiveness state, whether they are in the cloud and/or on-premises. Delivered via our homegrown award-winning ClearSkies™ Cloud SIEM platform, what sets our Managed Security Services (MSS) apart is the fact that they incorporate unique cutting-edge capabilities, including Human Intelligence, Advanced Analytics, Threat Intelligence and Security Automation & Orchestration.



## Governance, Risk & Compliance (GRC)

---

Odyssey's **Governance, Risk & Compliance (GRC)** services enable your organization to reliably achieve objectives, address uncertainty and act with integrity towards enhancing corporate performance and accountability. The outcome is the successful alignment of your organization's IT and business objectives, resulting in the effective management of risk while meeting and validating complex compliance requirements.



## Threat Risk Assessment Services by IthacaLabs™

---

Odyssey's **Threat Risk Assessment Services by IthacaLabs™** services help your organization Identify, Quantify and Prioritize Vulnerabilities and configuration Weaknesses found in your mission-critical systems, applications, IoT, network and security devices, whether in the cloud and/or on-premises. Through **Threat Risk Assessment Services by IthacaLabs™**, you are able to assess your organization's readiness, resilience, risk level and response capabilities in stopping, containing and mitigating targeted attacks.



## Cloud Security

Odyssey's **Cloud Security** services assist your organization into developing your migration strategy through your entire cloud transitioning journey in a manner that addresses risks inherently present in such a transition, while optimizing your total cost of ownership. Odyssey's cloud experts work closely with your key personnel to help you assess your readiness, design a migration plan, migrate your workloads, and maintain and manage your cloud infrastructure so that it is aligned with your business goals.



## Integrated Solutions

Odyssey's **Integrated Solutions** encompass leading state-of-the-art technologies, which along with our 20-year expertise and experience in the field, are tailor-made to enhance your organization's Information Security and Risk Management capabilities, irrespective of geographic dispersion or complexity, whether they involve on-premises and/or cloud environments. The end result is a secure, reliable, adaptable and scalable digital ecosystem, which not only meets, but surpasses your organization's risk mitigation goals.

## ONE Strategic Partner

who connects the dots and helps you see things you've never seen before.



# ClearSkies™ Threat & Vulnerability Management Platform

ClearSkies™ Threat and Vulnerability management platform help you “**Unlock the intelligence of your log & event Data**” comprised from Cloud SIEM, Active Defense, Endpoint Detection & Response (EDR), Identity & Access and Vulnerability Management and “Third-party data enrichment integration”, available to be procured at any time based on your needs and budget.

The Platform empowers organizations, as well as Managed Security Service Providers (MSSPs) to modernize their SOC capabilities by unlocking the intelligence of their data towards effectively managing digital risk while meeting compliance requirements. It does so by intelligently and swiftly associating threats with vulnerabilities, thus enabling an accelerated rate at which actual threats are identified and responded to.



## ClearSkies™ Cloud SIEM

Unravel Real-Time Visibility



### Active Defense

Lure and Trap  
Threat-Actors  
Post-Breach



### Endpoint

Detect &  
Respond to  
Malware &  
Insider Threats  
Before it is too  
Late



### Identity & Access

Stay on Top of  
your User Base



### Vulnerability Management

Focus on  
real threats &  
reduce false  
positives

## Third-Party Integrations

Extend the power of your SIEM with best-in-class SIEM integrations

Odyssey is included in 2021 **Gartner's Magic Quadrant** for ClearSkies™ Cloud SIEM.



# Ingredients of Success

Effectively managing digital risk is in itself a challenging process. The key to succeeding is a close cooperation between all stakeholders. Business, IT, Cloud and Information Security teams must work together and share the same understanding with regards to the desired objectives, ensuring that initiatives are **not overambitious**, **too disruptive** or simply **too long**.

To achieve the desired objectives, all stakeholders must be **engaged** from the beginning (**Engagement**), have a clear **vision** of what they are transforming and of the desired outcome (**Vision**), continuously receive and provide **feedback** into the transformation process (**Insight**), and take **ownership** of their part in it (**Ownership**) (Figure 2).

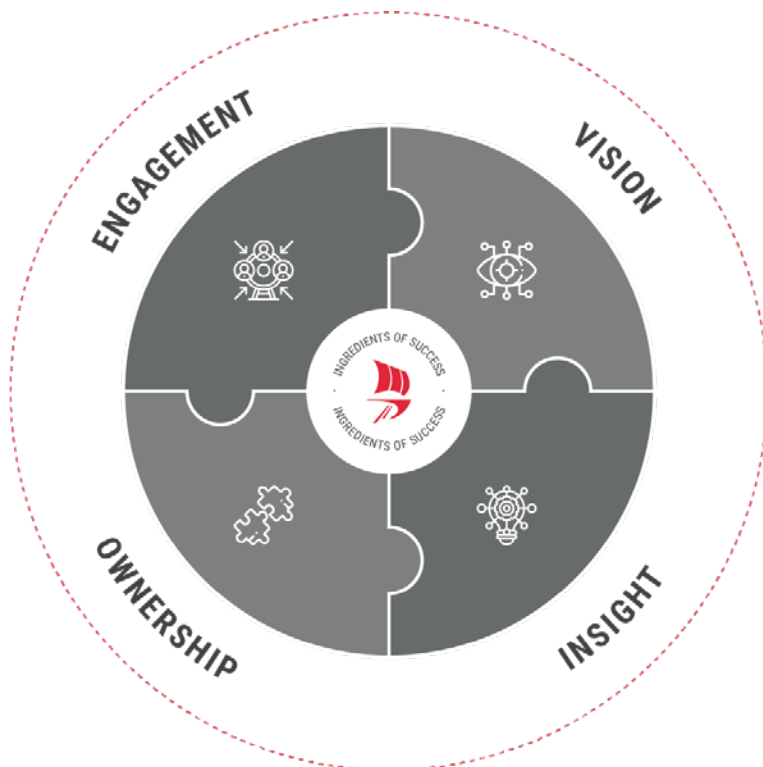


Figure 2: Engagement, Vision, Insight and Ownership

# Address your Digital Risks

While “**Digital Transformation**” is an opportunity of paramount importance for any modern organization, the increased complexity and dependency on the digital ecosystem results in a new and more complex set of “**Digital Risks**” that organizations need to address.

Digital Risks are divided into different categories and focus areas in supporting your organization’s “**Operational Risk**” management effort”:

## Digital Risks

- ✓ Cyber-Threats
- ✓ Insider Threats
- ✓ Third-Party Threats

## Focus Areas

- ✓ Data Governance & Privacy
- ✓ Business Continuity
- ✓ Resilience
- ✓ Compliance

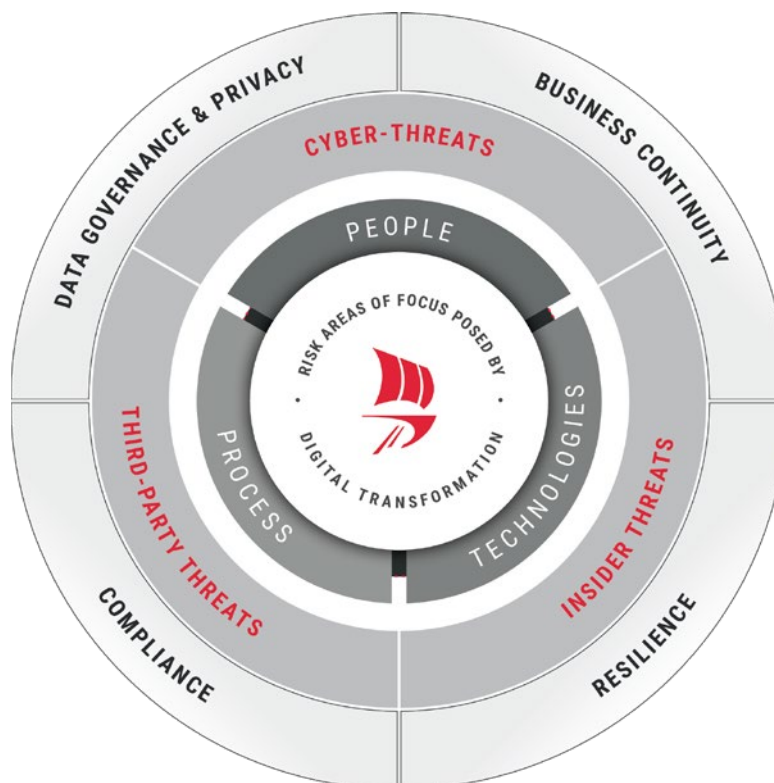


Figure 3: Digital Risk areas of focus



## Digital Risks

---

### Cyber-Threats

Cyber-Threats refer to the digital risks posed by targeted attacks circumventing organizational cyber defenses, leading to the compromise of sensitive/valuable data assets, as well as other attacks associated with service disruption, such as Denial-of-Service.

To minimize the impact of Cyber-Threats, the ongoing review and assessment of existing controls and processes is required. The outcome of this process will assist your organization in assessing the readiness, resilience, risk level and response capabilities to stop, contain and mitigate targeted cyberattacks towards protecting the digital ecosystem from unauthorized access/usage. The effective management of Cyber-Threats ensures the confidentiality, integrity and availability of your organizational digital ecosystem and digital assets.

### Insider Threats

Perhaps the hardest risk to address is the risk posed by staff, partners and any individuals with permanent or temporary access privileges to digital assets, who process, store and analyze sensitive/valuable information. Such malicious insiders can steal valuable data or conduct sabotage through digital means. The aim of our Insider Threat mitigation services is to assist your organization in assessing your risk level and response capabilities while identifying potential insider threats, all towards protecting access to digital assets from unauthorized access/usage. Organizations must deploy appropriate processes and controls to monitor and audit behavioral data access changes of its human resources.

### Third-Party Threats

These are risks associated with outsourcing services to third-party vendors, including Cloud and other Service Providers. Vulnerabilities emanating from outsourcing, including loss or compromise of operational integrity, intellectual property, customer information, or other sensitive information, constitute third-party risks. Such risks arise from inappropriate controls and processes on the side of the vendor/third-party operating environment. To mitigate these risks, key controls must be implemented around data sharing, technology integration, operations dependency, vendor resiliency etc.



## Focus Areas

---

### Data Governance & Privacy

Approaching digital risk from a data governance and privacy viewpoint refers to your organization's legal and financial exposure when corporate and personal (private) data of employees, directors, customers or other private individuals stored and processed by your organization are compromised. Such data can be easily exploited by hackers to harm your organization or to misuse identities for malicious purposes.

The protection of valuable personal data is of paramount operational importance but is also poses a high legal risk as it is a heavily regulated area. The loss of data privacy is subject to hefty fines, and it can have a great negative impact on your organization's image, reputation and viability.

Thus, organizations must be diligent in designing and implementing controls to ensure the auditing and protection of corporate and personal data across the digital ecosystem in various stages of its security and state lifecycle (e.g. in use, data in transit and data at rest). Key control areas to focus must be around data classification, data retention, data processing, data encryption etc.

### Business Continuity

The business continuity approach of digital risk relates to the risks inherent in adopting and relying on automation technology. In other words, the operational information dimension of digital risk refers to the disruption of normal/expected business operations as a result of Cyber, Insider or Third-Party threats. The main motivation behind these threats is the hinderance of your organization's operational capacity through temporary or permanent damage to operations. Those who stand to benefit from such attacks include unethical competitors, disgruntled employees, hacktivists or extortionists leveraging for ransom.

Inherently, Digital Transformation transfers a large segment of business continuity risk to the digital ecosystem. As such, all parts of this complex environment need to be assessed for their criticality to key business operations. Accordingly, they must be adequately protected and constantly monitored for suspicious and/or malicious behavior that can result in compromising or even hijacking business operations.

### Resilience

From a cyber and operational resilience standpoint, digital risks are inherent in adopting a new technology because of the potential damage from failing to optimize systems with which security staff are not familiar. In other words, digital risk emanates from the adoption of new unfamiliar technologies, and when there is a lack of sufficiently specialized and experienced human resources to effectively run, fine-tune and optimize them. In this respect, appropriate measures must be introduced into the Digital Transformation process to ensure that new systems are properly maintained, managed and configured. These measures must accommodate the specific needs and characteristics of your organization while their deployment should be seamlessly integrated into the digital ecosystem so as to not adversely impact it.

### Compliance

The introduction of new systems, technologies or processes that are part of a Digital Transformation process may introduce new legal or regulatory compliance responsibilities. Thus, approaching digital risk from a compliance standpoint encapsulates the focus on the potential failure of an organization to identify these additional responsibilities along with the legal, financial exposure this failure may represent. When adopting a new technology, your organization must engage resources and expertise to ensure that such responsibilities are defined, and that appropriate measures are designed into business operations, data lifecycle policies, and other operational aspects to ensure compliance. Maintaining good knowledge and compliance status monitoring minimizes the risk of compliance-related penalties.



# ONE Methodology

## Manage your Digital Risks

At the pinnacle of our Advisory Services is our proven **Cloud & Information Security methodology** which, while capitalizing on our two-decade long experience and expertise in the field, was specifically fine-tuned to address the challenges presented during a Digital Transformation initiative.

Pivotal part of this Assessment process (Figure 4) is that it is structured to take into consideration both the nature of your business operations as well as your organization's risk appetite.

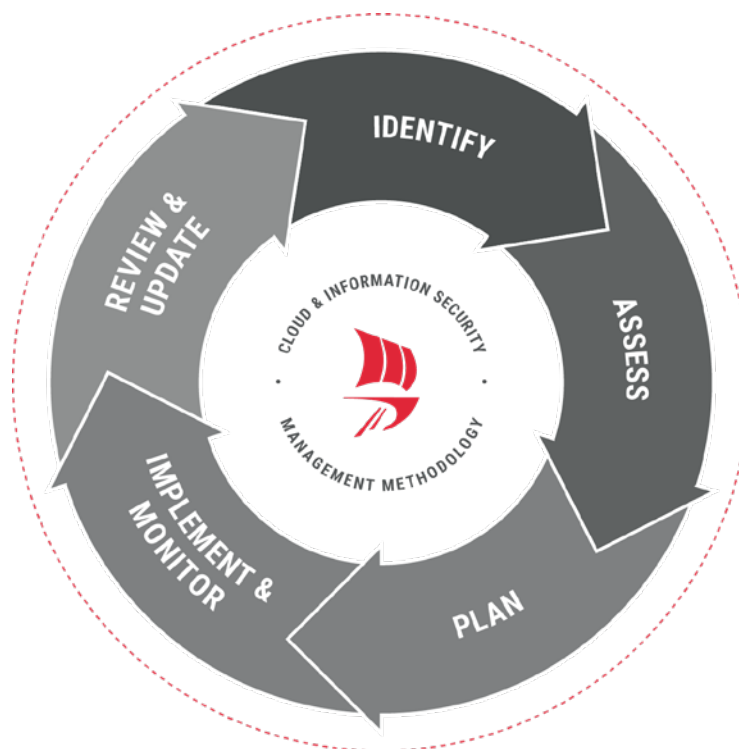


Figure 4: Odyssey's Cloud & Information Security proven methodology

The value you receive through this approach is the mitigation of your organizational Digital Risks to the desired level, and enhancement of both your information security and business continuity baselines, providing a high level of reassurance in terms of operational resilience and reputation.

# Cloud & Information Security methodology steps

## Identify

---

During this process, we help you **“Identify”** the risks threatening your digital ecosystem and operational resilience.

## Assess

---

We **“Assess”** the impact that such risk may pose to the Confidentiality, Integrity and Availability of your digital assets.

The outcome of the **“Assessment”** phase is ingrained in and reflected by our long-term experience in managing digital risk in your specific industry. The feedback and suggestions we provide are geared to help you towards making those difficult decisions pertaining to the effective selection of available Risk Treatment strategies.

## Plan

---

Through the **“Plan”** phase, we assist you in prioritizing appropriate risk mitigation controls and processes, and we help you identify the most efficient and effective implementation path. While we ensure that the risks with the highest priority are addressed first, we do not overlook incidental quick wins and other risk mitigation opportunities, which help you achieve the highest level of assurance in the least amount of time possible.

## Implement & Monitor

---

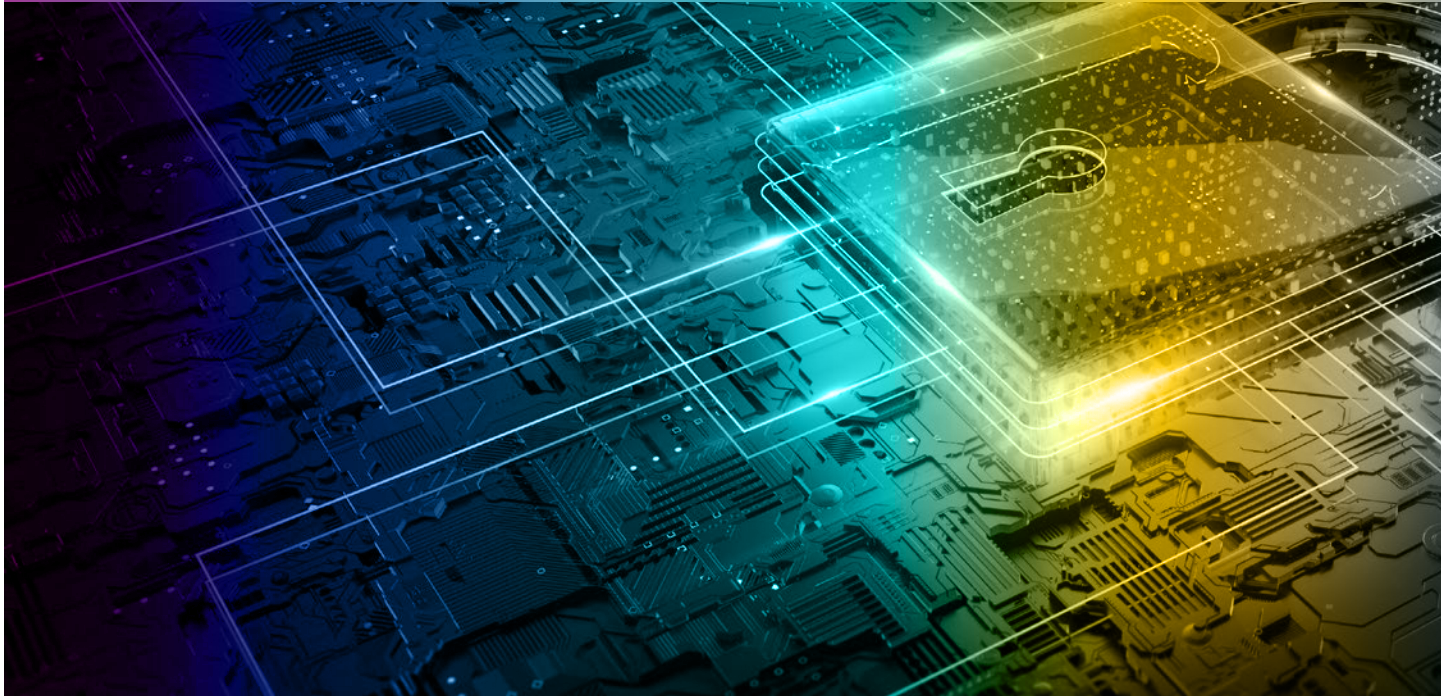
Our comprehensive Information Security and Managed Security savviness skill-set is put to full use during the **“Implement & Monitor”** phase.

## Review & Update

---

Once Risk Treatment controls, whether Operational, Technical or other, are implemented, we then **“Review”** their effectiveness.

Based on the outcome of the **“Review”** phase, we may then suggest the **“Update”** and/or implementation of additional/complimentary measures, or the modification of existing controls and processes, to ensure that identified security/resilience gaps are appropriately treated.



Driving our ability to consistently transform our service/product mix for keeping up with the ever-expanding information-threat landscape and market trends is our company motto: **“Possible Solutions to Impossible Challenges”**.

## **Odyssey at a glance**

**Odyssey is a leader in Cloud & Information Security, supporting organizations around the globe in achieving cyber resilience.**

For more than two decades, we continuously evolve our Cloud & Information Security solutions, services and products to support our clients in effectively managing their digital risks and in adhering to compliance requirements.

Odyssey's Advisory Services empower you to build a cyber resilient organization, so as to effectively anticipate, respond, swiftly recover, and adapt to the emerging threats and vulnerabilities of a dynamically expanding and unpredictable threat landscape.

Our holistic approach combines the award-winning ClearSkies™ Threat & Vulnerability Management Platform, Managed Security Services (MSS), Governance, Risk & Compliance, Threat Risk Assessment services, Cloud Security and Integrated Solutions.

Odyssey is ISO 27001, ISO 9001 and ISO 22301 certified, and accredited by the Payment Card Industry Security Standards Council (PCI SSC) as a Qualified Security Assessor (QSA). We are also honored with the globally recognized Great Place to Work® certification, the assessment methodology used by “The Fortune 100 Best Companies to Work in America”.





STRICTLY CONFIDENTIAL

This document contains confidential and proprietary information of commercial value relating to the business, commercial and financial affairs of Odyssey™, the exposure of which to third parties could adversely affect the business affairs of Odyssey™. This information is supplied in confidence for private use, on the strict condition that no part of it is disclosed to any third party, in particular to any person or organisation that may be in competition to Odyssey™ without the prior written approval of Odyssey™. Unauthorized use or reproduction of this document is prohibited.

## HEADQUARTERS

1 Lefkos Anastasiades Str.  
2012 Strovolos, Nicosia, Cyprus

**T** +357 22463600

**F** +357 22463563

**E** [info@odysseycs.com](mailto:info@odysseycs.com)

**[www.odysseycs.com](http://www.odysseycs.com)**



**OFFICES** CYPRUS | GREECE | USA | UK | KSA