

RESEARCH DOCUMENT

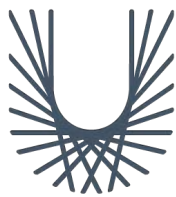


eirguard

Cybersecurity governance and compliance

Peter O'Hare

Project Supervisor
Dr. Christopher Staff



SE
TU

Ollscoil
Teicneolaíochta
an Oirdheiscirt

South East
Technological
University



Peter O'Hare
C00263594
Cybercrime & I.T. Security
Year 4 Project



Table of Contents

ABSTRACT	3
WHAT IS GOVERNANCE?	4
NIS2 OVERVIEW	6
WHO'S AFFECTED?	6
BUDGET IMPLICATIONS.....	7
RESEARCH	9
CYBERSECURITY FRAMEWORKS	11
NIST CSF2	11
COBIT 2019	11
ISO/IEC 27001	12
COMPLIANCE OPTIONS	13
MANAGED COMPLIANCE	13
THIRD PARTY OPTIONS	13
INTRODUCING EIRGUARD	14
SIMILAR APPLICATIONS	15
TECHNOLOGIES	17
APP PLATFORM	17
WEBSITE.....	17
HOSTING OPTIONS.....	18
DATABASE & DEPLOYMENT	18
TECHNOLOGY CONCLUSIONS	19
THE FRAMEWORK CHOICE	19
THE WEBSITE.....	19
HOSTING PROVIDER	20
DATABASE & DEPLOYMENT PLATFORM	20
CHALLENGES	21
CONCLUSIONS	22
APPENDIX A	23
NIS2: IN DEPTH	23
APPENDIX B	25
CYBERSECURITY QUESTIONNAIRE	25
REFERENCES	30

Abstract

Good cybersecurity cannot exist without good governance. Without a firm grasp and understanding of an organisation's goals, security needs, risk appetite, and security posture, it's almost impossible to adequately guard against cybersecurity threats.

This document looks at what governance is and how that fits in with cybersecurity. It also examines several different cybersecurity frameworks, as well as investigating ways organisations can attain cybersecurity compliance. The main thrust of this document however is to introduce eirguard – a cybersecurity governance app that aims to guide SMEs through the process of developing a robust cybersecurity governance framework.

To implement good cybersecurity policies and procedures, a good governance model needs to be in place. The truth is however, that some SMEs lack the information, the experience, or indeed the motivation to dedicate the time and effort into developing tailored cybersecurity governance models for their organisations. All too often, security incidents can be avoided or have their impact lessened if effective procedures and policies had been implemented.

In order to reduce the barriers to good governance, eirguard removes the difficulty, ambiguity and frustration that can come with developing cybersecurity governance policies. It guides the user through the process of creating policies and procedures, while adhering to any legal and regulatory requirements that need to be taken into consideration. In short, eirguard provides everything that an SME would need to devise, create and implement a solid governance model for their organisation.

Eirguard's ultimate goal is to lower the barrier of entry to customised and robust cybersecurity governance for small enterprises.

P.O.H

Introduction

What is Governance?

In his 2012 publication "*Governance: A Very Short Introduction*," [1] Mark Bevir defines governance as follows:

Governance refers ... to all processes of governing, whether undertaken by a government, market, or network, whether over a family, tribe, formal or informal organization, or territory, and whether through laws, norms, power, or language. Governance differs from government in that it focuses less on the state and its institutions and more on social practices and activities. (p. 11)

Governance dictates how an entity, be it a country or a company is run. The Organization for Economic Co-operation and Development (OECD), in its *Principles of Corporate Governance* (1999) [2], were the first to formally define 'corporate governance' as "the system by which business corporations are directed and controlled."

Governance ensures that the ethos, principles and procedures of the organisation espoused by management or the board, are specified in a formal manner, so there is a clear understanding by all involved in how tasks are to be carried out, and if necessary, reported on.

Cybersecurity governance is no different. It lays out formal procedures and policies agreed by management or the board, on how information security should be handled within the organisation.

Alan Calder & Steve Watkins stated in their publication "*IT Governance: An international guide to data security and ISO27001/ISO27002*" (2020) [3]

While most organizations believe that their information systems are secure, the brutal reality is that they are not. Not only is it extremely difficult for an organization to operate in today's world without effective information security, but poorly secured organizations have become risks to their more responsible associates. (p. 18)

Calder and Watkins' statement perfectly sums up the attitude to information security in the eyes of some entities and organisations the world over. The '*it will never happen to us*' mentality must be firmly extinguished and replaced with a managed, proactive cybersecurity approach.

This objective was the impetus behind the EU's Network and Information Systems (NIS) cybersecurity directive when it was announced in August 2016. It aimed to strengthen the bloc's cybersecurity resilience by ensuring each member state enacted the cybersecurity resolutions it had set out.

Its successor, NIS2 (*see Appendix A*), will come into force in October 2024, with an expanded set of requirements, including for governance, with even more organisations now falling under its remit.

Effective governance requires a combination of factors, and depending on where you look, these factors range in number. The *Good Governance Institute*[4] believes there are ten principal themes that inform good governance. The most important of those, would be: clarity of purpose, application of principles, leadership, effective relationships, systems and structures, risk and compliance and organisational effectiveness.

Implementing a governance model for any SME can be difficult. One can understand the reticence of some organisations to re-entering the governance maelstrom in order to develop a whole new governance model just for cybersecurity. It's time consuming, resource diverting and ultimately not worth the time and effort for some organisations. The failure to adequately look at governance can also be attributed to its absence from cybersecurity frameworks and regulatory compliance guidelines.

The original NIS directive barely mentioned governance at all, focussing instead on the practical element of frontline defence. However, this lack of direction lead to some organisations not taking it seriously, with low or indeed no adoption of the recommendations in some cases. While there was a concerted effort in making critical infrastructure more secure, the mechanisms in how those were to be achieved were not given the brevity they deserved.

NIS2 corrects this by ensuring that all organisations under its remit have effective policies and procedures in place, with definite individual lines of responsibility now drawn in the sand. As mentioned earlier in the report, without good governance it's difficult to implement effective cybersecurity protocols.

NIST's CSF2 (*see Cybersecurity Frameworks section*) is undergoing a comprehensive review and update process, that for the first time includes procedures for governance. The framework has been updated after extensive consultations with cybersecurity professionals and those working in the field, to adequately represent what is needed for any organisation to develop good cybersecurity hygiene.

My interest was piqued after seeing the upcoming changes proposed by NIS2, and I wondered how organisations, particularly smaller ones, would cope with the new implementations. Would they struggle to get a firm grasp of what was expected of them? Would there be panic at what could be perceived as Titanic changes in the way they have to conduct business? Would they be able to achieve compliance in the given timescale?

While governance is certainly not the most exciting or thrilling aspect of cybersecurity, it underpins every aspect of how those "exciting" bits are conducted and operate. While I wanted to investigate if there was a way to make governance more approachable, ostensibly to make the transition to NIS2 smoother for those already covered by NIS, it was the organisations that never had to consider cybersecurity governance before, that I was really interested in investigating further. My main question remained: is there a way to make governance more "user friendly"?

NIS2 Overview

The NIS2 update introduces more proactive cooperation with the monitoring body established in each member state. The body can conduct random cybersecurity audits, and demand documentary proof of compliance from organisations that fall under the remit.

The need for NIS2 is illustrated by the graph below from the ENISA *Threat Landscape Report 2023* [5]. It quite plainly depicts that the number of reported cyber incidents from EU entities is on an upward trend, combined with an increase in the number of documented threat actors.

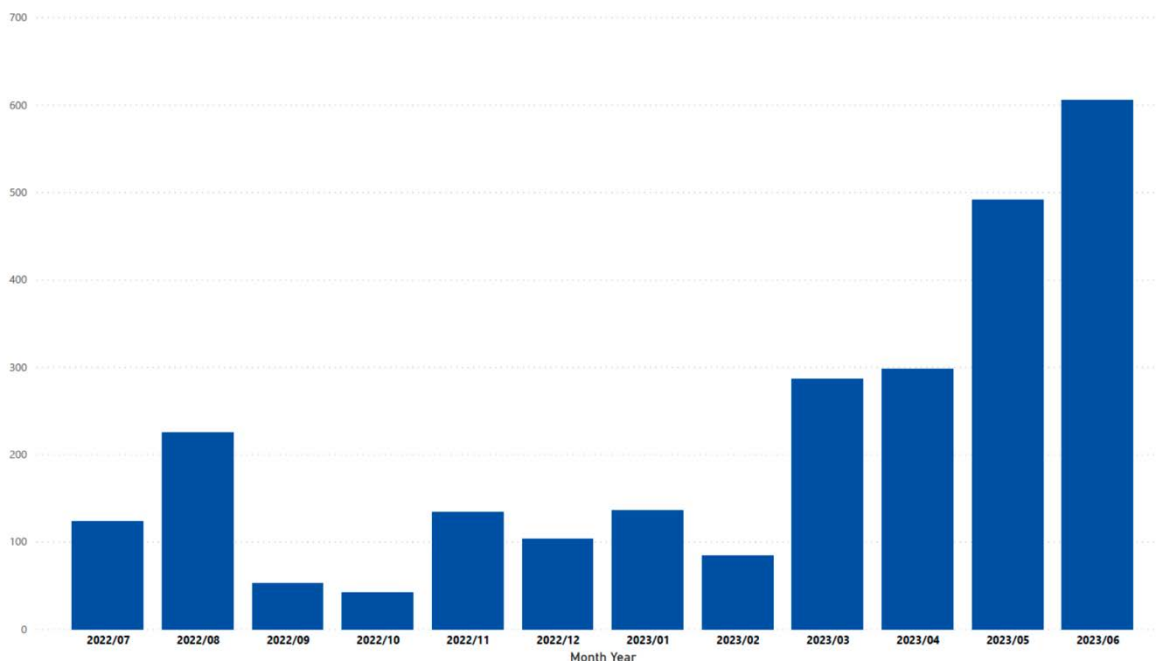


Figure 1: Timeline of EU events 2022 -23 (count of number of observed incidents per month)

With reported incidents expected to increase into the future, NIS2 will help approx. 160,000 entities strengthen their security and make the EU a safer place to live, work and do business.

When introducing the directive, Dutch MEP Bart Groothuis stated, *“If we are attacked on an industrial scale, we have to react on an industrial scale”*. [6]

Who’s affected?

NIS2 completely overhauled the industries that will be covered by the directive. Previously, in NIS1, *Operators of Essential Services (OES)* were identified, and obliged to adhere to the regulations. NIS2 replaces the single OES label with two new classifications for organisations. Now, an organisation can be classed as **essential**, or **important**. This change brings many more organisations that were previously outside the scope of the original NIS regulations firmly under the remit of NIS2, and the obligations contained therein.

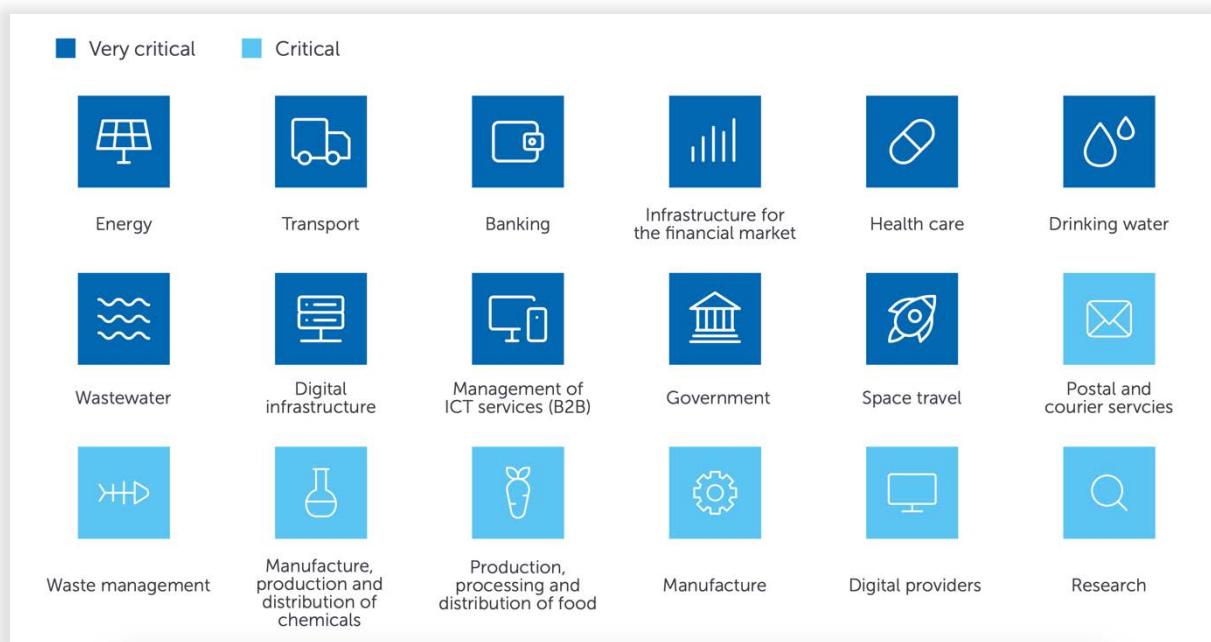


Figure 2: Essential (dark blue) and important (light blue) designations [7]

In general, NIS2 does not target small and micro enterprises of 50 employees or less, or those with an annual turnover of less than €7 million per annum. However, if they play a key role in society, in sectors or services, then member states will be required to ensure they are covered by the directive.

Budget implications

In their white paper on NIS2, international law firm Eversheds-Sutherland[7], state that organisations that are not yet covered by the directive will need to increase their ICT budgets by a maximum of 22%, and those already covered will increase by a maximum of 12%.

Administration tasks associated with the directive will also increase, as the directive shifts to proactive monitoring of essential or critical organisations. The burden is now on the organisation to prove to the monitoring body that they are compliant with all aspects of the directive.

With the changes that NIS2 will bring, it behoves organisations to look at how they deal with cybersecurity. While the changes introduce extra administration work and expense, in the long run it ensures that critical and important organisations in the EU have adequate protection from any potential attack. Organisations that do not fall under the remit of the amended regulations would also benefit from examining the requirements, and doing an internal cybersecurity audit to help strengthen their defences.

NIS2 is not the only cybersecurity change occurring. The EU have also proposed the *Cyber Resilience Act*[8], which will ensure that products with digital elements offered on the European market will have to have significantly reduced number of vulnerabilities, and that manufacturers continue to remain responsible for cybersecurity throughout a product's entire life cycle.

NIST are currently developing Cyber Security Framework 2 (CSF2) to update and widen the scope of their popular cybersecurity framework[9], and the internationally recognised ISO/27001 framework was updated in late 2022 [10]. With the level of change ongoing, any assistance that can be given to organisations regarding governance would be welcomed.

Research

As part of the research into how medium and small enterprises manage their cybersecurity, I conducted a small questionnaire (see Appendix B – live version available [here](#))¹ with 3 respondents (as of 27th Nov 2023)

The results painted a mixed bag of cybersecurity hygiene. While some were quite good at identifying areas that needed to be protected and / or monitored, they were let down by having no concrete policies in place.

Some lacked any overall governance at all, while others had policies in place, but no single person with the responsibility and authority to implement important decisions should an incident occur. Several had outsourced their cybersecurity requirements to third parties who actively monitored their network, and had no in-house understanding of their cybersecurity posture.

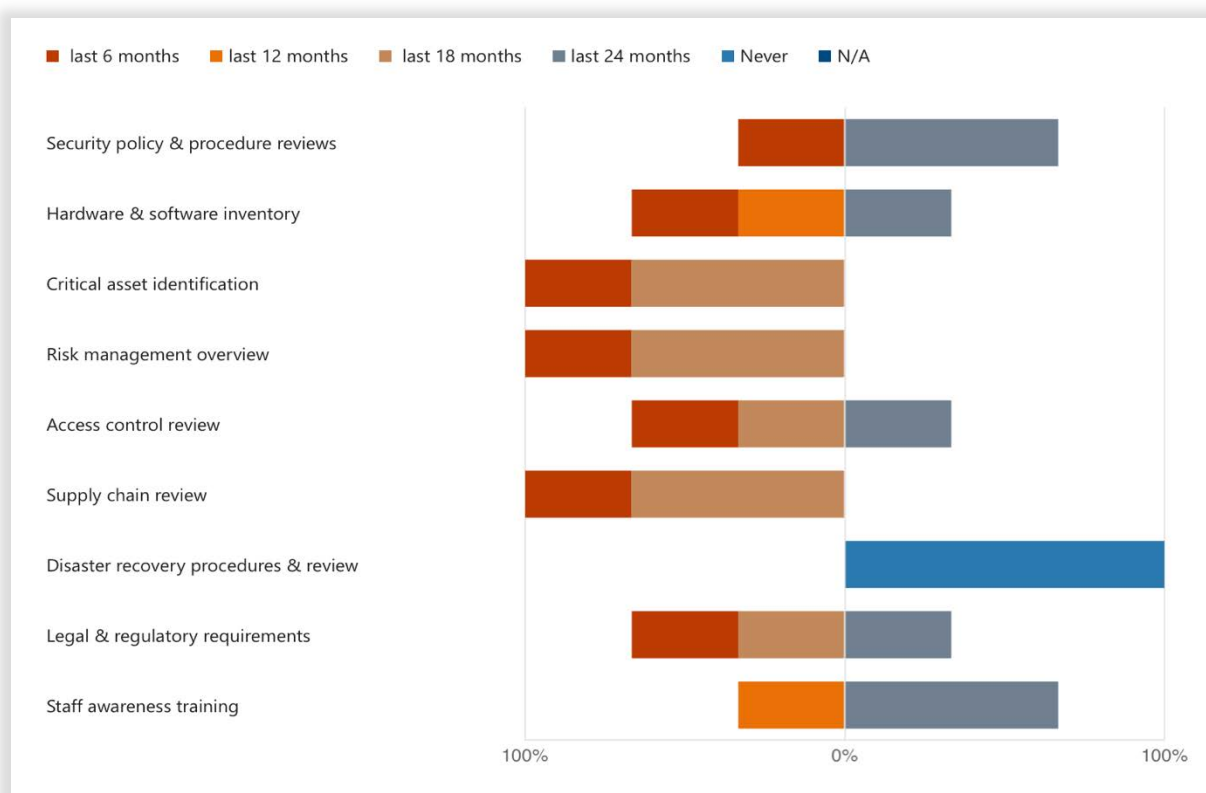


Figure 3: Sample timeline of respondents security policies

One of the survey respondents stated their organisation falls under the incoming NIS2 requirements, and would need to meet the obligations that pertained to them. They also indicated that they were developing an in-house solution to manage compliance. This shows

¹ <https://forms.office.com/e/igzc5peGi6>

there is an appetite for good self-guided approaches to regulatory compliance amongst SME's in Ireland.

Overall it seemed that most respondents took an ad-hoc approach to governance as a whole. While management buy-in was cited in all instances, there was no demonstrated approach to bringing all cyber related tasks under the one umbrella. This, invariably, resulted in a disjointed and disparate approach to in-house cybersecurity policies.

Robust cybersecurity governance is essential to ensuring the security and safety of an organisations' systems and data. Having policies and procedures in place that address sometimes mundane tasks – like patching system software – is an essential aspect of maintaining high cybersecurity hygiene.

While there are a number of options available to organisations to assist in the implementation of cybersecurity controls and mitigations – there is very little available in terms of developing a governance model. Having good governance and procedures in place is instrumental in developing comprehensive cybersecurity policies and procedures.

Cybersecurity Frameworks

This section deals with the most common cybersecurity frameworks available at present. It looks at popularity, cost and ease of implementation.

NIST CSF2



The Cyber Security Framework 2 (CSF2)[11] is administered by the National Institute of Standards and Technology (NIST) in the United States, and is highly regarded. It was intended to be a framework that moves and evolves as technology changed and advanced. This is achieved by engaging stakeholder feedback and ongoing consultations with industry.

To that end, the 2.0 update will be completed in Q1 of 2024, and for the first time incorporates governance as a key pillar of the framework. This adoption outlines the importance of governance in any organisation as they plan and prepare their cybersecurity implementation.

The CSF offers a comprehensive set of cybersecurity procedures, free of charge, that helps organisations improve and harden their cybersecurity protocols, while following industry best practice in order to achieve those goals.

NIST do not offer certification for CSF2. However, this does not diminish it's excellence. On the contrary, it lowers the bar to entry making it a very cost effective option for any organisation. It offers a comprehensive set of tools and procedures to best implement cybersecurity policies and mitigations organisation wide. There is however, an investment of time to figure out what sections apply to your organisation, and developing solid policies and procedures.

COBIT 2019



COBIT, by *Information Systems Audit and Control Association (ISACA)*[12]- while not free, also offers a cost effective method to implement cybersecurity controls. As well as providing the framework itself, ISACA also offers resources, training, mentorship and tools to enable those learning the framework to equip themselves with the best possible information for the task.

COBIT can be tailored to suit the organisation in question, highlighting the items of particular concern, and ignoring those that may not be relevant. It provides guidance as well as checks and balances in order to implement effective cybersecurity policies and procedures.

ISO/IEC 27001



ISO/IEC 27001[13] is a globally recognised framework for information security management systems (ISMS). This standard offers organizations, regardless of their size or industry, a framework to create, execute, sustain, and enhance an information security management system.

In order to become ISO certified, the organisation must pass a recognised external ISO audit. Once achieved, the certification demonstrates the organisation's commitment to information and cyber security to current and potential customers.

ISO/27001 is extremely comprehensive and covers four main control categories - organisational, physical, people and technological. This ensures that every aspect of the business is examined, and appropriate controls put in place.

The downside to seeking ISO/27001 certification is the expense involved. It costs a not insignificant amount of money to gain and keep certification. With internal audits, designing organisational processes, creating and setting controls, and commissioning external audits – costs mount up very, very quickly. These costs mean that attaining ISO certification is beyond the reach of many SME's.

Compliance Options

Managed Compliance

Those looking for a low barrier to entry, can avail of one of the many cloud based managed compliance services. Organisations such as Drata [14], ControlMap[15] , and HyperProof[16], have a range of compliance frameworks to choose from, including GDPR, NIST and ISO/27001, to name but a few.

These services simplify the implementation of a cybersecurity framework by guiding the user through the setup process, and then offering a 24/7 monitoring package to take all the heavy lifting away from the organisation. Services such as these can offer great value for organisations but do come with some downsides. Once everything has been configured and set up, you are inextricably tied into their ecosystems. This of course means incurring an ongoing cost to maintain the service.

However, the biggest drawback in this scenario is you are almost entirely dependent on the platform in question. While some aspects will be locally based – everything else is tied up with the third-party service. If this service experiences an outage or goes out of business then you are firmly on the hook - and almost back at square one, with very little to show for the time, effort, and expense.

While the convenience of such a service can be appealing, a longer-term plan should be implemented, with contingencies built in to cover all eventualities. The last thing an organisation wants is for the cloud service to vanish, and face restarting a process that had already been completed.

Third Party Options

Outsourcing the organisations entire cybersecurity requirements is another hands off approach that an organisation can take. This involves engaging a third party company to conduct the audit of your organisation, design and implement the controls and mitigations, and then run and maintain the whole thing once they are done. Organisations like Grant Thornton[17] , EY[18] , Nostra[19] and Security Risk Advisors[20] , all offer such a service, or variations of it.

This approach has distinct advantages for some organisations as it frees them up to continue their main line of business. Depending on whom they contract, they're sure of getting a modern, robust and resilient framework implementation. On top of that – monitoring and incident handling is also taken care of.

The downsides to this approach is those working within the organisation know very little about their own cybersecurity. A complete hands-off approach, while appealing to some, can introduce issues of its own. Disengaged employees are more inclined to place higher trust in the third parties abilities, and take on more inherent risk that may not be taken if cybersecurity was done in-house.

Again, as mentioned in the previous section – being wholly reliant on a single third party for something as important as cybersecurity, is a risk in and of itself.

Introducing eirguard



Eirguard is an iPadOS app that aims to streamline and simplify the implementation of cybersecurity governance for small and medium sized enterprises. It can be particularly useful for small and medium sized organisations looking to get to grips with cybersecurity concerns amid the upheaval caused by the introduction of NIS2 and the impending release of CSF2. The app is used in conjunction with a web-based administration portal that aims to cover the creation, implementation and continued management of cybersecurity policies and procedures. It aims to make cybersecurity compliance easier, less cumbersome and more cost effective for SME's.

Achieving compliance can be an expensive and confusing endeavour for SME's. Having a resource like eirguard, that walks the user through mapping their organisational goals, and designing and implementing governance policies, would be a huge advantage. Utilising the iPad allows the user to access tasks, information, or reports wherever they may be and streamlines the entire process.

After the users initial registration and setup, Eirguard will take a snapshot of the organisations current cybersecurity stance. It will then ascertain their ultimate aims and goals and create an action plan to achieve those goals. As part of the onboarding process eirguard will also ascertain any legal or regulatory obligations that need to be adhered to and build those into the plan.

Eirguard can be used by a single individual to complete the process, or by a team in larger organisations. An administrator or project lead can create users and roles and assign tasks to individual users for completion within the app. Completed tasks are then fed back to the admin dashboard on the web portal, where progress can be monitored, reports created and shared, or policy reviews scheduled for future dates.

Eirguard will draw from the upcoming CSF2 (Cybersecurity Framework 2) currently undergoing review, as well as the NIS2 requirements (also still under review) as well as industry best practice to achieve both the clients' stated goals, and regulatory compliance goals.

Eirguard targets small and medium sized enterprises who want to take full control of their cybersecurity management and deployment. It will focus on removing the barrier to compliance that can be put in place by sometimes vague and complex language, or difficult to grasp criteria. Eirguard intends to level the cybersecurity compliance playing field by ensuring that all businesses can protect themselves, and their clients or customers from a cyber-attack.

To that end, Eirguard is positioned to be used by both technical and non-technical users. While some knowledge of cybersecurity would certainly be an advantage, eirguard should not be a challenge for the general user, as explanations and tutorials will guide them through each stage of the process.

Similar Applications

As outlined earlier in the report, there are numerous services offering organisations assistance in getting compliance, or monitoring their network. There are however, very few apps in direct competition with eirguard. As it will be outlined later in the document, tablet apps on Android are a rarity at present, and those that are available on iOS are focussed on device protection.

The one application that comes close to eirguard in terms of functionality is CyberSmart[21], a UK based cybersecurity firm. The app allows for device monitoring and access to policy documents.

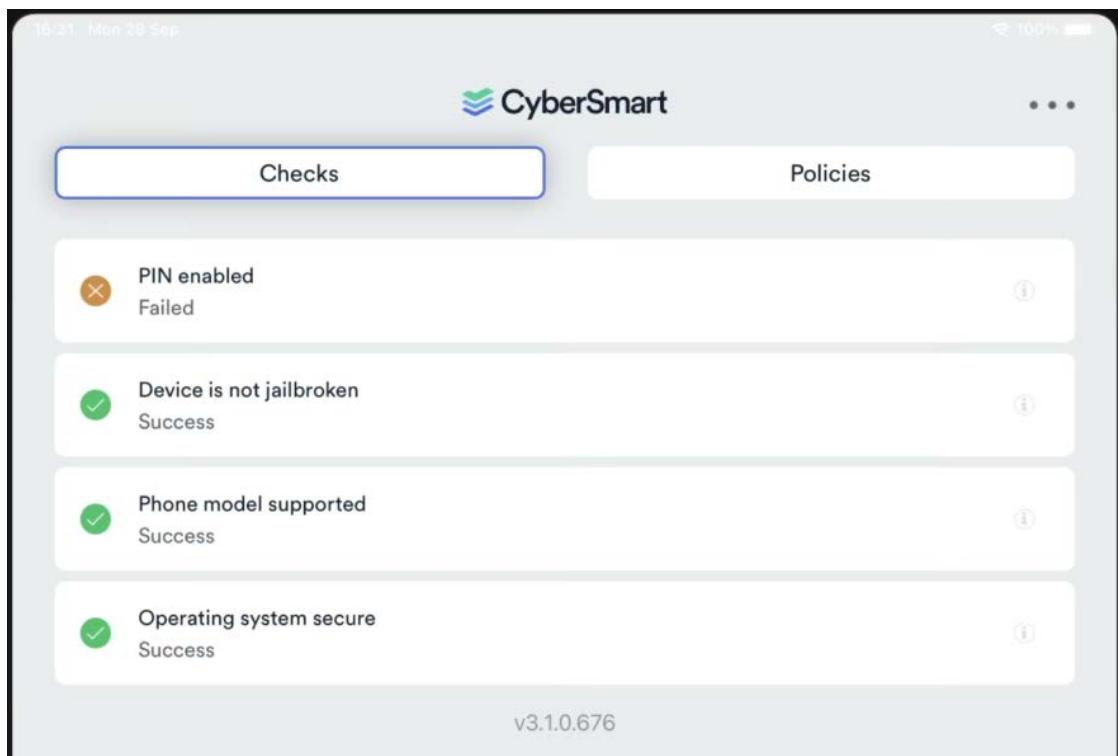


Figure 4: Cybersmart device monitoring

This is one method of securing physical devices owned and operated by the organisation, to track configurations and usage. While useful, device monitoring is not something that eirguard conducts. Eirguard is geared towards the creation and implementation of governance models, not end-device security.

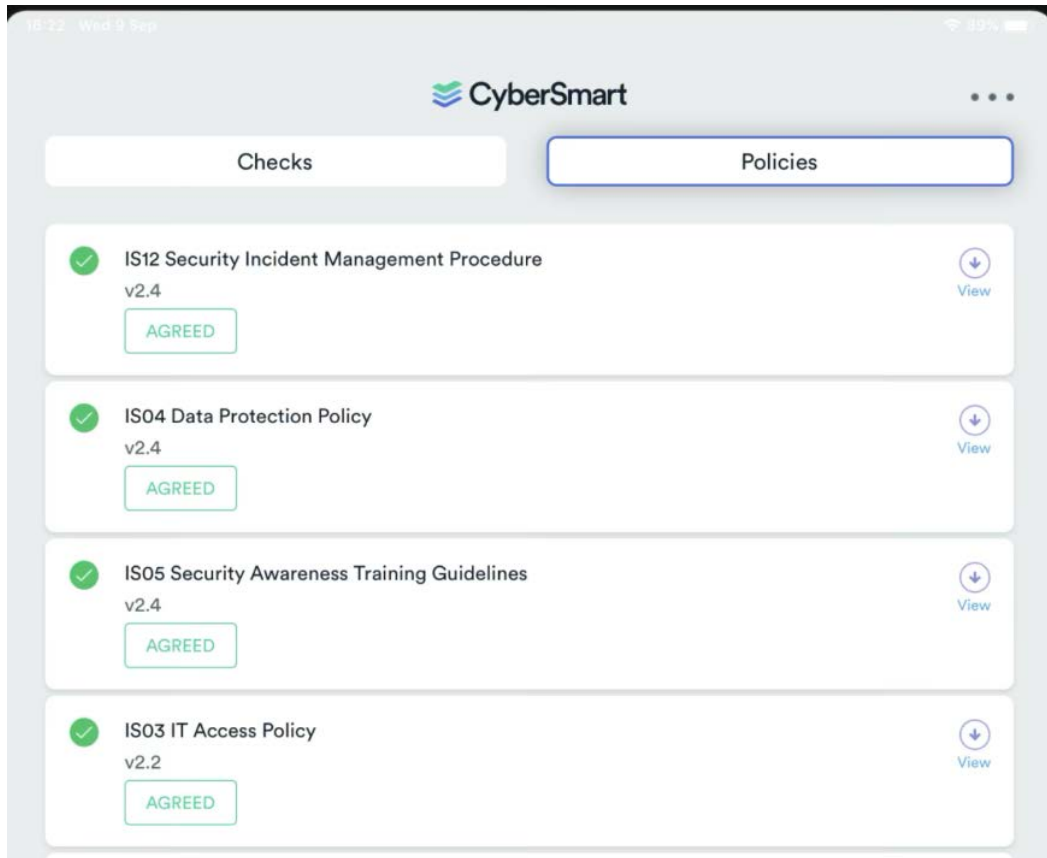


Figure 5: Cybersmart policy document access

While CyberSmart operates in the same sphere as eirguard, and will reference similar policy types, being a UK based organisation, it has a definite slant toward UK legislation over EU regulations. This reason alone sets eirguard apart from it in terms of attractiveness to Irish and EU based organisations, wishing to achieve legal compliance.

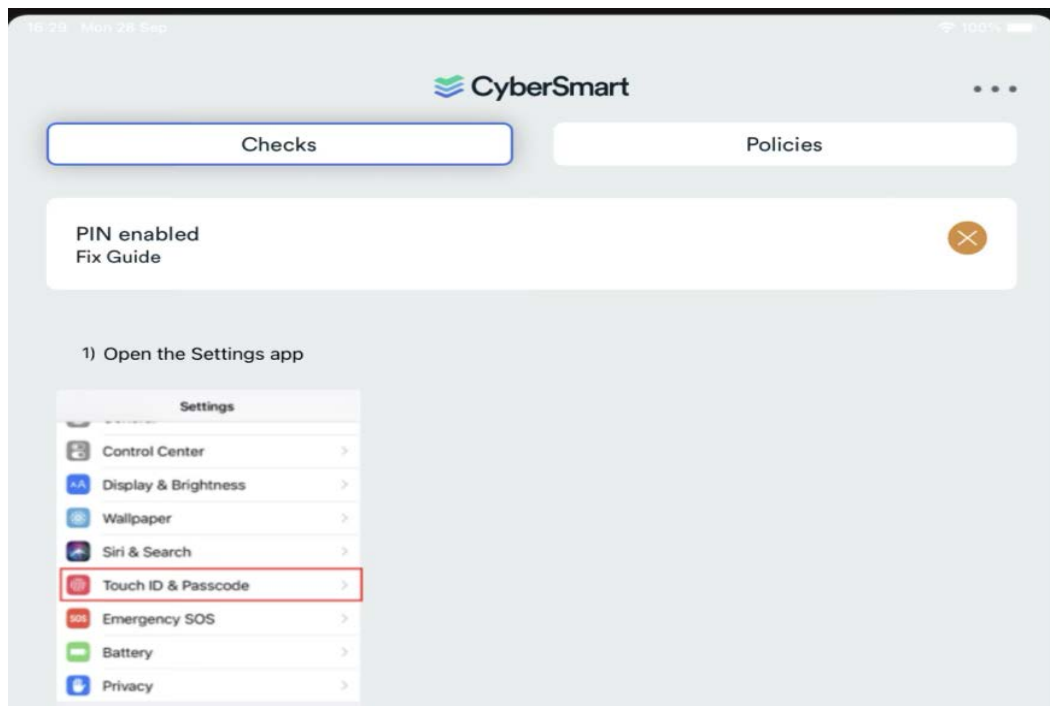


Figure 6: Cybersmart help section

Technologies

This section will deal with the technology behind eirguard. It will first present all the available options that were considered when planning the eirguard build. The section *Technology Conclusions* will outline the decision making process behind the final choices made for the project.

App Platform

At present, there is no dedicated app in either the Google Play Store or the App Store that provides the functionality that eirguard intends to. This gives eirguard a competitive advantage when compared to other vendors mentioned earlier.

Investigating the technologies available for the creation of eirguard's app, I looked at both the Android and Apple ecosystems. Android has a much larger install and user base than iOS, and is available across multiple devices and manufacturers making it highly accessible.

Android apps are developed using either Java or Kotlin, using Android Studio or a similar IDE, with many resources freely available for developers.²

Apps for iOS are written in Swift – a fork of Objective C – but can only be built using an Apple laptop or desktop. Apple provides a wealth of information and documentation for developers as well as strict Human Interface Guidelines (HIG) to ensure all apps perform as they should on any iOS device.³

Website

The web based administration portal for eirguard will need to be robust, secure and reliable. To that end I looked at several technologies that could fit that criteria.

Option 1 is to use a custom site written in PHP. This has a few advantages in that every aspect of the site can be tailored and custom built to the exact specifications that eirguard requires. The drawback is that it will take a considerable time to design, develop, test and implement.

Option 2 is to use a PHP based framework or content management system like Wordpress[22] for eirguard. This has the advantage of being quick to implement, robust, and has a multitude of templates available that can be customised with plugins or custom PHP code.

Option 3 is to use a Python framework like Flask[23] or Django[24]. Again, the advantage here is both are quick to implement, highly customisable and straightforward to use. Django also comes with Django Admin, which can be configured to function as an application dashboard.

Flask is lightweight, mature, and easy to customise with the inclusion of the Jinja2 templating system.

² <https://developer.android.com>

³ <https://developer.apple.com>

Hosting Options

Hosting the site is another area that needed research. Several options were looked at: basic web hosting, shared cloud, and dedicated cloud being the most popular. The cloud options offer more modularity and expansion options than the basic web hosting package with addons and upgrades easily applied.

Several hosting companies were looked into including Blacknight[25] in Carlow, Hetzner[26] in Germany and OVHCloud [27] based in France. All offer both regular web hosting options as well as many cloud options also. No non-EU companies were considered because of GDPR and data privacy considerations.

Database & Deployment

Google's Firebase[28] is the go-to service for app deployment. They offer many configurations to build, deploy and monitor your app. It's a popular choice for many developers.

Supabase [29] is an open source alternative to Firebase. It offers many of the same features as Firebase, as well as some that Firebase do not offer.

Technology Conclusions

This section will outline the decision making process behind the selection of the technologies that used to implement eirguard.

App Platform Choice

In deciding the platform the app would be built on, several issues were taken into consideration. While Android certainly has a much larger user base than iOS, the Play Store can be seen as the wild west. Security, while improving – is nowhere near as robust as the App Store, with thousands of apps uploaded to the Play Store containing malware.[30] Security has to be a consideration when making a decision like this. Apple pushes regular security updates for iOS, while updates for Android are vendor specific, and can sometimes take a considerable length of time to be deployed.

eirguard is envisioned to be a tablet based app to take advantage of the larger screens they offer. On Android, tablet based apps are not something that developers have embraced, despite numerous manufacturers making Android based tablets. Apple's iPad on the other hand, has a robust library of apps designed specifically for the platform, and Apple have many resources available to assist developing for iPad.

Writing an app in Swift for the Apple ecosystem opens up the opportunity to target iPhones, iPads, MacOS, tvOS and watchOS with very minimal code changes required between devices. This allows for a 'code once - deploy often' approach that can enhance the usefulness and lifespan of the app across multiple devices. This is further simplified by the interoperability between devices that the Apple ecosystem offers.

For the reasons outlined above – eirguard will be an iOS based app.

The Website

With many factors to consider for the website, security again took precedence as the most important one. PHP, while robust and mature, has many vulnerabilities and weaknesses that can be exploited.[31] Similarly, the plugin ecosystem offered by the Wordpress platform introduces even more avenues and opportunities for compromise. [32]

Flask is lightweight, mature and robust. However, that lightweight factor ultimately counts against it. In order to accomplish what needs to be achieved with eirguard, a lot of work would be required to attain that exclusively using Flask.

Django offers enhanced security, extensibility and maturity out of the box.[33] It guards against common attacks like cross site scripting, SQL injection, cross site request forgery and clickjacking. It is robust enough to do most of the heavy lifting required by eirguard, and deliver the results in a consistent manner.

Therefore, the Django framework will be used for the web portion of eirguard.

Hosting Provider

Several factors were taken into consideration when assessing the hosting requirements for eirguard. Availability, scalability and solutions offered were the main factors looked at. Of course cost was also taken into consideration.

Blacknight are a local Carlow hosting company who offer services that could suit eirguard. However, when cost was taken into consideration – the attractiveness of hosting locally was quickly extinguished. Costs added up very quickly – making Blacknight a non-runner.

OVHCloud are a relative newcomer to the cloud hosting scene, having initially established themselves as a regular web hosting company. While their pricing was attractive, investigations revealed that their reputation was not. Bad reviews and mentions of links to criminality in the media put OVHCloud well out of the running.

Hetzner has been in business since the 90s offering web hosting and ancillary services. When assessing their offerings for eirguard, they had everything that would be required, at a cost that was reasonable.

Therefore Hetzner will be used to host the eirguard website.

Database & deployment platform

Before selecting a deployment option, the previous technology choices need to be taken into consideration. Firebase utilises a NoSQL database, which will not play easily with Django. Supabase runs Postgres which Django has no issues with. Supabase also includes user authentication and encryption out of the box which are paid additions to Firebase.

Using Firebase can incur extensive costs when compared to comparable Supabase offerings. The fact that Supabase is also open source makes it a very easy decision. Eirguard will deploy on Supabase.

Challenges

There are certainly some challenges ahead in the development process. Creating an efficient design and implementation process for the database will be one such challenge. Being new to PostgreSQL, which is favoured by Supabase, will add an extra layer of complexity. However, Supabase offer some new approaches to traditional database design which should help mitigate some of the expected pain.

Another challenge comes in the development of the app itself. Apple implemented changes in the way gui implementation is handled in the iOS 15 update. Previous to this change, the ui was handled by a framework called UIKit, which utilised a traditional Model, View, Controller (MVC) approach. Apple pivoted to a Model, View, ViewModel (MVVM) approach in iOS 15.

Audrey Tam & Caroline Begbie - authors of SwiftUI Apprentice, describe the difference between the two approaches:

“(In MVC)... Your data model knows nothing about how your app presents it to users. The view doesn’t own the data, and the controller mediates between the model and the view.

A commonly used architecture for SwiftUI apps is Model-View-View Model (**MVVM**). There’s no controller, so the view model prepares model data for the view to display.

A view model’s properties can include the current text for a text field or whether a specific button is enabled. In a view model, you can also specify actions the view can perform, like button taps or gestures.” [34]

While I have some experience using UIKit in Swift, moving to SwiftUI and MVVM will require some research and practice. This leads nicely into the other major challenge facing the project:

Time.

I need to ensure that everything is carefully managed to avoid wasting time. The deadlines are tight – and I need to allow enough time near the end for testing and fixes before final submission. Technical issues and coding problems can always be dealt with, but one cannot regain lost time.

Conclusions

The rapid pace of technological change coupled with cyber criminals ability to harness that changing technology in order to target organisations for their own financial or political gain, acutely demonstrates the need for cybersecurity resilience on the part of all organisations. This situation will unfortunately not change any time soon. While criminality of this nature persists, and organisations and the data they hold are regularly at risk, there will always be a need for laws like NIS2, frameworks like CSF2 - and apps like eirguard.

Looking at the incoming regulatory changes in the EU, the updates to the various frameworks already discussed, and analysing the results of the cybersecurity survey – there certainly seems to be a place for an application like eirguard.

Assisting SMEs establish good cybersecurity governance and helping develop procedures and policies can only be a positive action. Encouraging organisations who are not impacted by regulatory compliance, to examine their own internal policies and controls, and develop a comprehensive set of cybersecurity procedures will only further enhance and promote good cybersecurity hygiene. Being able to do that while remaining cost-effective, straightforward, and efficient, makes eirguard a very compelling option for any organisation.

Appendix A



NIS2: In depth

The original *Network and Information Systems* directive (NIS)[15] was the EU’s first union wide cybersecurity legislation. It was enacted in 2016 and aimed to achieve high levels of common information security across all the blocs’ critical infrastructure, to ensure they were all protected to a similar degree.

It directed member states to develop a *National Competent Authority* (NCA) as well as developing a new *National Cyber Security Strategy* to achieve those aims. Members were then to classify their “operators of essential services” (OES), which were mainly comprised of transport, health, water, power, and digital infrastructure.

Member states were also to classify “digital service providers” (DSP) which comprised of online search engines, online marketplaces and cloud computing providers. Regulations required each identified OES and DSP to implement organisational and technological measures to ensure the security of their networks and any information they may hold. The regulations also imposed mandatory reporting to the NCA in the event of an incident.

With the groundwork already laid with NIS, NIS2 built and expanded on it. Major changes were made in identifying critical infrastructure. Gone is the OES system, to be replaced with a wider ranging list of industries. The new classifications for the affected industries are *essential* and *important*.

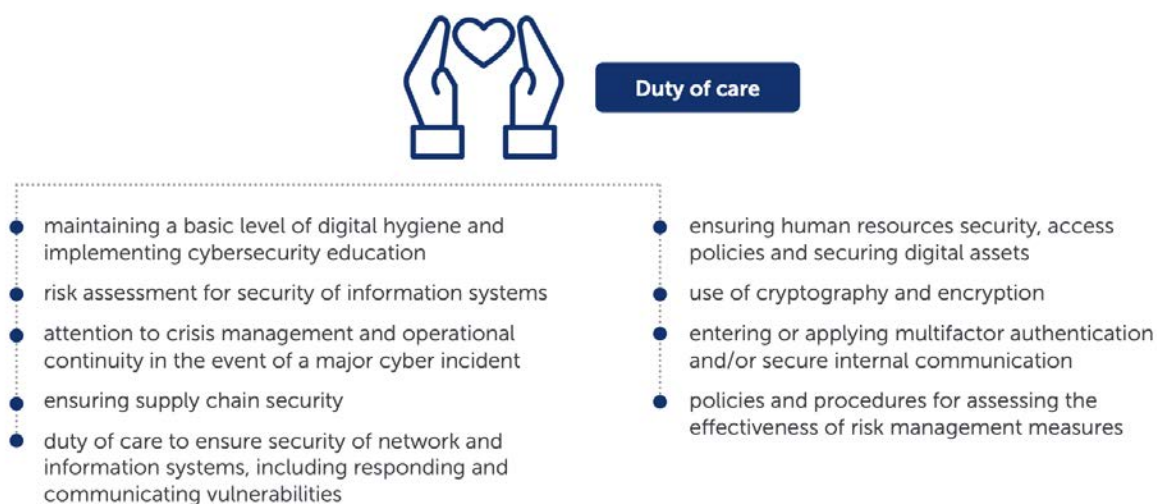
ESSENTIAL	IMPORTANT
 ENERGY	 POSTAL AND COURIER SERVICES
 TRANSPORT	 WASTE MANAGEMENT
 BANKING	 MANUFACTURE
 HEALTH CARE	 DIGITAL PROVIDERS
 DRINKING WATER	 RESEARCH
 WASTEWATER	 MANUFACTURE, PRODUCTION AND DISTRIBUTION OF CHEMICALS
 DIGITAL INFRASTRUCTURE	 PRODUCTION, PROCESSING AND DISTRIBUTION OF FOOD
 MANAGEMENT OF ICT SERVICES (B2B)	
 GOVERNMENT	
 SPACE TRAVEL	
 INFRASTRUCTURE FOR THE FINANCIAL MARKET	<p>° Large: more than 250 employees and an annual turnover of at least 50 million euros (or a balance sheet total of at least 43 million euros).</p> <p>.....</p> <p>° Medium-sized: more than 50 and fewer than 250 employees and an annual turnover not exceeding 50 million euros (or a balance sheet total not exceeding 43 million euros).</p> <p>.....</p>

Essential sectors cover the original OES sectors of energy, transport water, health etc – but water has now been broken out into drinking water and wastewater, and covered sectors have been expanded to include digital infrastructure, space travel, financial infrastructure, government management of ICT services.

Essential services must comply with the regulations regarding strengthening and securing their networks, including documenting their policies and procedures, and produce those documents on demand, making backups and conduct risk analyses.

Important sectors cover the production, processing and distribution of food, the manufacture, production and distribution of chemicals, research, digital providers, manufacturing, waste management and postal and courier services.

Mandatory incident reporting has also been updated. The first notification – the early warning – must be made in the first 24 hours. The incident notification itself must be submitted no later than 72 hours. A final report, or progress report if investigation is ongoing, must be submitted one month after the incident.



Organisations outside the scope of NIS2 can voluntarily report serious incidents, cyber threats or near incidents should they wish to contribute.

Enforcement of the directive is now going to be proactive rather than reactive in nature. The NCA can now carry out on-site compliance inspections, security audits, security scans, request information and access to data.

Failure to adhere to the measures directed by the directive can result in fines of up to €10million or 2% of the company's turnover – whichever is greater. NIS 2 now also provides for personal responsibility for failures by company directors, and sanctions imposed on those individuals deemed liable.

APPENDIX B

Cybersecurity Questionnaire

1

Approx how many employees work in your organisation? *

- Less than 50
- Between 50 - 250
- Over 250

2

Does your organisation have a formal information security policy in place?

This policy provides the information and procedures for risk assessment, risk mitigation, and cybersecurity planning.

Procedures include:

- regular security audits and reports
- hardware and software inventory
- regular software updating and patching
- access control
- password management procedures
- new hire, movers and leavers procedures
- regular staff training and awareness of cybersecurity

*

- Yes - full formal procedures in place
- In progress - some, but not all procedures in place
- Some informal ad-hoc procedures in place
- No formal procedures currently in use

3

If your organisation follows an established cybersecurity framework - which framework listed below most closely describes your organisational policies? (if known) *

- NIST Cybersecurity Framework
- ISO 270001 Framework
- COBIT Framework
- Not known

4

Does your organisation have a clear line of responsibility for cybersecurity?

Is there a person within the organisation designated as the main point of contact for cybersecurity issues?

*

- Yes - we have a dedicated security officer
- No - there is no single individual with that responsibility

5

Does your organisation have clear cybersecurity governance policies in place?

Does the management/board regularly review the policies and procedures in place for managing risk, both internal and external? *

- Yes - management are completely involved
- The Security Officer deals with all governance issues, reporting to management when necessary
- No - management take a hands-off approach with ad-hoc policies in place
- Governance, what's that?!

Does your organisation fall under the incoming EU NIS2 Cybersecurity Regulations - in effect October 2024?

The sectors affected are listed in the image.
A more detailed breakdown of the broader sectors are highlighted in blue below.

The healthcare sector includes:

both public and private healthcare providers, medical equipment and medicine manufacturers, medical insurance providers and other critical health-related services



















The manufacturing sector includes the manufacturing of:

medical devices, computers and electronics, machinery and equipment, motor vehicles, trailers and semi-trailers and other transport equipment

ICT Services sector includes:

Telecom, DNS, TLD, data centres, trust services, and cloud services.

*

 ENERGY	 POSTAL AND COURIER SERVICES
 TRANSPORT	 WASTE MANAGEMENT
 BANKING	 MANUFACTURE
 HEALTH CARE	 DIGITAL PROVIDERS
 DRINKING WATER	 RESEARCH
 WASTEWATER	 MANUFACTURE, PRODUCTION AND DISTRIBUTION OF CHEMICALS
 DIGITAL INFRASTRUCTURE	 PRODUCTION, PROCESSING AND DISTRIBUTION OF FOOD
 MANAGEMENT OF ICT SERVICES (B2B)	
 GOVERNMENT	<p>* Large: more than 250 employees and an annual turnover of at least 50 million euros (or a balance sheet total of at least 43 million euros).</p> <p>⋮</p> <p>* Medium-sized: more than 50 and fewer than 250 employees and an annual turnover not exceeding 50 million euros (or a balance sheet total not exceeding 43 million euros).</p> <p>⋮</p>
 SPACE TRAVEL	
 INFRASTRUCTURE FOR THE FINANCIAL MARKET	

- Yes - we need to comply with NIS2
- No - we do not fall under the remit of NIS2

Note: Q7 is a conditional question, and will only be displayed if the user selected Yes in Q6

7

How are you ensuring that your organisation will be completely compliant? *

- We are engaging an external third party to assist, advise and develop a roadmap to compliance
- We are developing and coordinating in-house policies and procedures, using an industry standard framework, to ensure we are compliant in all areas

8

Which of the following has your organisation completed? *

	last 6 months	last 12 months	last 18 months	last 24 months	Never	N/A
Security policy & procedure reviews	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hardware & software inventory	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Critical asset identification	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Risk management overview	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Access control review	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Supply chain review	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Disaster recovery procedures & review	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Legal & regulatory requirements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Staff awareness training	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Does your organisation know its risk appetite?

Risk appetite is described as "*the amount of risk that an organisation is willing to accept to achieve its objectives.*"

Typically, a risk appetite statement is approved by the management or the board, and outlines the organisation's risk attitude and willingness to accept risk in specific scenarios, with a governance model in place for risk oversight. *

- Appetite is known - definitive policies in place
- Appetite is known - ad-hoc policies in pace
- Appetite unknown
- Haven't a bulls notion!

References

- [1] Bevir, M. (2012) *Governance: A Very Short Introduction*, Oxford University Press.
- [2] 1999, 'OECD Principles of Corporate Governance Meeting of the OECD Council at Ministerial Level', Accessed: Nov. 22, 2023. [Online]. Available: <http://www.copyright.com/>.
- [3] Calder, A. and Watkins, S. (2020) *IT Governance An international guide to data security and ISO27001/ISO27002*, SEVENTH EDITION. Kogan Page Limited.
- [4] 'The basics of good governance | Good Governance'. Accessed: Nov. 28, 2023. [Online]. Available: <https://www.good-governance.org.uk/publications/insights/the-basics-of-good-governance>
- [5] 'ENISA Threat Landscape 2023 — ENISA'. Accessed: Oct. 20, 2023. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- [6] 'Cybersecurity: Parliament adopts new law to strengthen EU-wide resilience | News | European Parliament'. Accessed: Nov. 29, 2023. [Online]. Available: <https://www.europarl.europa.eu/news/en/press-room/20221107IPR49608/cybersecurity-parliament-adopts-new-law-to-strengthen-eu-wide-resilience>
- [7] 'Everything you need to know about the NIS2 Directive | Enhanced Reader'. Accessed: Nov. 23, 2023. [Online]. Available: <https://www.eversheds-sutherland.com/lists/static/uploads/nis2-whitepaper.pdf>
- [8] 'EU Cyber Resilience Act | Shaping Europe's digital future'. Accessed: Nov. 23, 2023. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>
- [9] 2018, 'Updating the NIST Cybersecurity Framework – Journey To CSF 2.0 | NIST', doi: 10.6028/NIST.CSWP.04162018.
- [10] 'ISO - ISO/IEC 27001: What's new in IT security?' Accessed: Dec. 07, 2023. [Online]. Available: <https://www.iso.org/contents/news/2022/10/new-iso-iec-27001.html>
- [11] 'Updating the NIST Cybersecurity Framework – Journey To CSF 2.0 | NIST'. Accessed: Dec. 05, 2023. [Online]. Available: <https://www.nist.gov/cyberframework/updates/nist-cybersecurity-framework-journey-csf-20>
- [12] 'COBIT | Control Objectives for Information Technologies | ISACA'. Accessed: Dec. 05, 2023. [Online]. Available: <https://www.isaca.org/resources/cobit>
- [13] 'ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements'. Accessed: Dec. 05, 2023. [Online]. Available: <https://www.iso.org/standard/27001>

- [14] 'Cyber Essentials Compliance Automation Software | Drata'. Accessed: Nov. 23, 2023. [Online]. Available: <https://drata.com/product/cyber-essentials>
- [15] 'NIST CSF Compliance Automation Software | ControlMap'. Accessed: Nov. 23, 2023. [Online]. Available: <https://www.controlmap.io/nist-csf-compliance-automation-software>
- [16] 'ISO 27001 Compliance Workflows Optimized with Hyperproof'. Accessed: Nov. 23, 2023. [Online]. Available: <https://hyperproof.io/product/iso-27001/>
- [17] 'Digital Risk | Grant Thornton'. Accessed: Nov. 23, 2023. [Online]. Available: <https://www.grantthornton.ie/service/advisory/digital-risk/>
- [18] 'Cybersecurity Managed Services | EY Ireland'. Accessed: Nov. 23, 2023. [Online]. Available: https://www.ey.com/en_ie/cybersecurity/managed-services
- [19] 'Cyber Security & Compliance | Computer Security | Network Security | ICT | Cloud'. Accessed: Dec. 05, 2023. [Online]. Available: <https://www.nostra.ie/services/security-compliance/>
- [20] 'Security Risk Advisors - CyberSOC'. Accessed: Nov. 23, 2023. [Online]. Available: <https://sra.io/cybersoc/>
- [21] 'Reduce your cyber risk by 98.5% and ensure protection | CyberSmart'. Accessed: Nov. 23, 2023. [Online]. Available: <https://cybersmart.co.uk/cyber-essentials-certification/>
- [22] 'Blog Tool, Publishing Platform, and CMS – WordPress.org'. Accessed: Dec. 05, 2023. [Online]. Available: <https://wordpress.org/>
- [23] 'Welcome to Flask — Flask Documentation (3.0.x)'. Accessed: Dec. 05, 2023. [Online]. Available: <https://flask.palletsprojects.com/en/3.0.x/>
- [24] 'The web framework for perfectionists with deadlines | Django'. Accessed: Dec. 05, 2023. [Online]. Available: <https://www.djangoproject.com/>
- [25] 'Cloud Hosting Solutions - Cloud VM - VPS Servers'. Accessed: Dec. 05, 2023. [Online]. Available: <https://www.blacknight.com/cloud-hosting/>
- [26] 'Truly thrifty cloud hosting - Hetzner Online GmbH'. Accessed: Dec. 05, 2023. [Online]. Available: <https://www.hetzner.com/cloud>
- [27] 'OVHcloud VPS - Your virtual private server in the cloud | OVHcloud'. Accessed: Dec. 05, 2023. [Online]. Available: <https://www.ovhcloud.com/en-ie/vps/>
- [28] 'Firebase | Google's Mobile and Web App Development Platform'. Accessed: Dec. 05, 2023. [Online]. Available: <https://firebase.google.com/>
- [29] 'Supabase | The Open Source Firebase Alternative'. Accessed: Dec. 05, 2023. [Online]. Available: <https://supabase.com/>

- [30] 'How cybercriminals evade mobile app store security measures | Security Info Watch'. Accessed: Dec. 05, 2023. [Online]. Available: <https://www.securityinfowatch.com/cybersecurity/information-security/anti-virus-and-malware-defense/article/53074932/how-cybercriminals-evade-mobile-app-store-security-measures>
- [31] 'PHP - Security Vulnerabilities in 2023'. Accessed: Nov. 21, 2023. [Online]. Available: <https://stack.watch/product/php/php/>
- [32] 'WordPress Vulnerability Database - Patchstack'. Accessed: Nov. 21, 2023. [Online]. Available: <https://patchstack.com/database/>
- [33] 'Security in Django | Django documentation | Django'. Accessed: Nov. 21, 2023. [Online]. Available: <https://docs.djangoproject.com/en/4.2/topics/security/>
- [34] Tam A. and Begbie C., (2021) *SwiftUI Apprentice*, 2nd ed., vol. 1. raywenderlich,.

