New Approaches to Risk Management through Regulations and Standards

G4P4 Kansen voor West II

INTRODUCTION

Digitisation is the foreword to many initiatives and innovations. Whether we are reading about the latest government grants, New solutions by providers or tools used by practitioners - digitisation is a key description or requirement. So it goes, that all businesses must digitise or gather insurmountable data for their growth and success.

In this white paper we will not be moralising or analysing the excessive data collection, here we will examine and articulate how we can meet the challenges of digitisation through simplification and a more positive inclusive approach to implementation.

Digitisation is simply defined as:
'The process of converting something to digital' [1]

Yet digitisation can mean very different things for situation or the business in question. Some businesses are implementing the digitisation of their processes and assets whereas others are already predominantly digitised and looking at the next steps of improvement.

Whichever stage, digitisation comes a different series of threats from bad actors and tools, hackers, hacktivists, ransomware, and many more. As such, all digital businesses, in the face of these threats, must deal with similar challenges, that of continuity and safety.

Two areas that are sometimes afterthoughts for businesses, or a challenge that will be resolved at a much later time, or on rare occasions resolved as the business digitises and grows.
So, digitisation is vital for businesses, but they must also implement measures against the (cyber) threats that they face with more digital data. This usually involved aligning themselves to a regulation or standard that reduces these threats and allows them to evidence their resilience to clients or data providers.

In this paper we will examine some of the challenges these businesses face, how regulations help the business and the results of our research which helped us build our Cyber Compliance Platform.

1 https://www.merriam-webster.com/dictionary/digitization

THE CHALLENGES

Choosing a standard

The challenges are many and as already mentioned that the growth of digitisation and data collection attracts bad actors such as hackers and cyber threats that want to access the data or to disrupt the business activity reliant upon the data. The challenge for businesses includes building their resilience, raising the awareness of their people, and then somehow measuring their capabilities.

As businesses face the task of implementing cyber resilience to the digital threat vectors, they discover the myriad of choices and options available to them. Lots of solutions, lots of technical language and lots of starting points. This is when they usually decide upon a structured way to approach their process of building resilience. The structured approach could involve consultants but more likely the businesses will choose a regulation or standard that provides the coverage that helps them to build and evidence their resilience.

So which standard? Here are a few to choose from:

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework (NaCSF)** [2]
- **COBIT an ISACA Framework** [3]
- **Cyber Essentials** [4]
- **ISO27001 Information Security Management** [5]

Through our research and in discussion with subject matter experts we quickly realised that there is synergy and overlap between all these standards. As such, we focused upon this commonality to build a Governance, Risk and Compliance (GRC) platform, more on this later.

2 https://www.nist.gov/
3 https://www.isaca.org/resources/cobit
4 https://www.ncsc.gov.uk/cyberessentials/overview
5 https://www.iso.org/isoiec-27001-information-security.html

> **"THE BIGGEST PART OF OUR DIGITAL TRANSFORMATION IS CHANGING THE WAY WE THINK."**
>
> **— SIMEON PRESTON, BUPA**

We recommend that businesses look closely at the standards and their requirements. Matching closely to align to one that fits them best. However, rest assured the CCP covers all bases and is always being improved to meet the latest standard requirements or changes.[6]

As the business decides upon the standard the real graft starts. The business must work to understand the requirements, understand where they are as a business (if they have not done this already), map the business needs against the threats and risks. A task that usually involves complete knowledge of the standard and a method of recording the results, usually spreadsheets.

Implementing change

Next challenge, start the task of influencing and implementing change within their business. A common problem we found was resistance or maybe reluctance to fund (sometimes costly) information technology solutions that were difficult to understand or to evidence their intrinsic business value.

Still there are actions and implementation efforts a go and perhaps more if the requests were authorised by the business managers. The experts must try to manage the resources, actions, and implementation as they record the changes. Again, many businesses relied upon multiple spreadsheets.

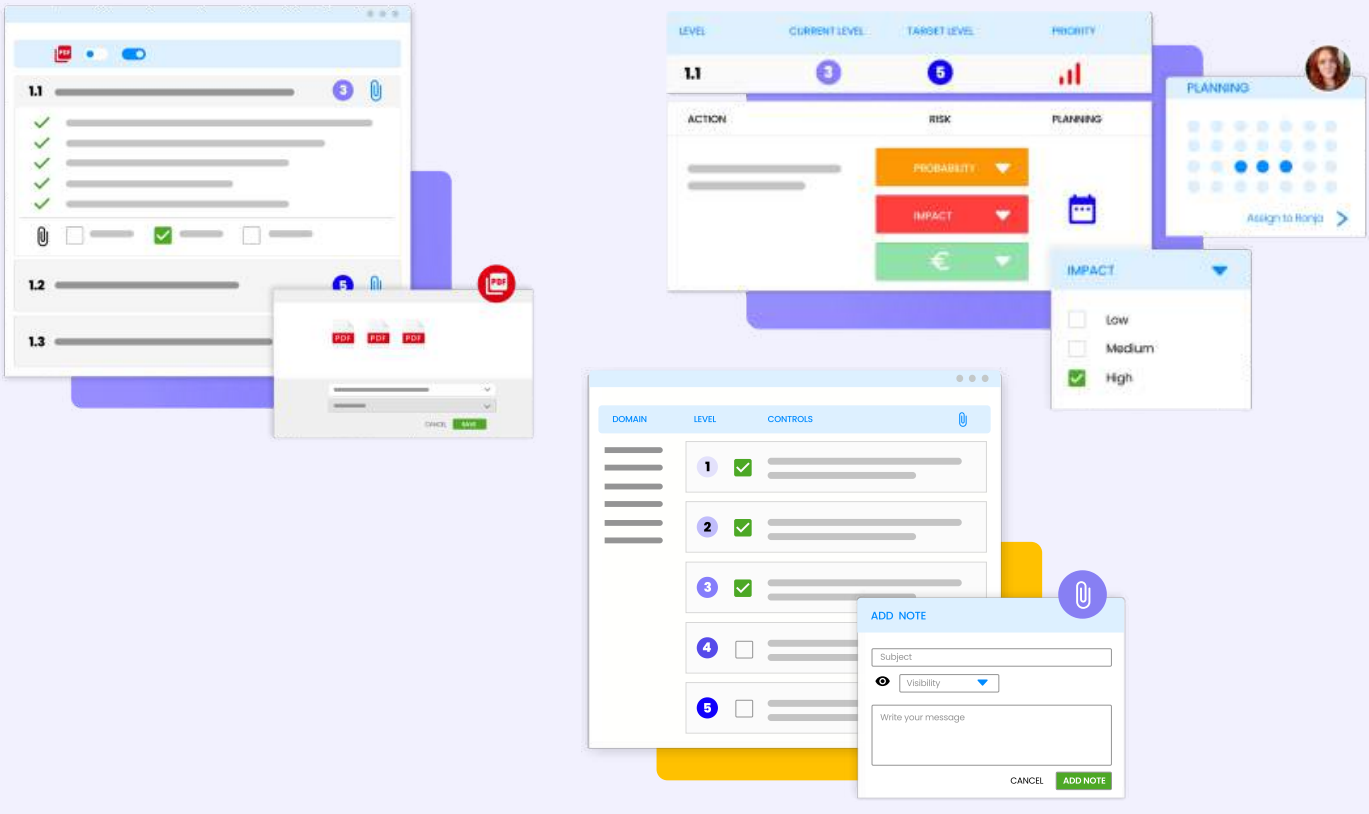
6 We are working closely with NEN to cover the imminent changes to ISO27002

These are a few of the challenges businesses face, and there are many more that we do not have the room to cover. All these challenges are directly compounded by the way that the cyber security sector operates. There is a lack of transparency, despite local and governmental measures, to promote information and threat intelligence sharing.

The support frameworks make it difficult for businesses to share expertise, information, or knowledge. Businesses are bound by non-disclosure agreements or bound to confidentiality regarding subjects that could and should be shared with their business partners or within the sector. Most sectors and businesses do not compete on cyber security and the safety of all is beneficial to their respective reputations.

Our solution

As we developed our understanding of these challenges so did our approach and problem solution fit. Only through effective research and analysis could we plan, invest, and develop a solution that directly solved these challenges but one that also was focused upon the future. Here we explain how the findings directly focused our approach to be innovative and solve the challenges our clients will face.



OUR SOLUTIONS

Simplification

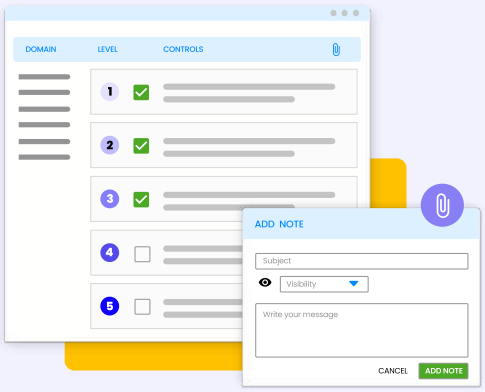
Cyber security is complex and as such so are the standards. The technical language can be difficult to understand and often requires research and further reading to understand. There is little wonder that there are so many courses and qualifications open to subject matter experts. The standards are written as frameworks as they must fit and operate across different businesses and sectors.

We simplified the technical language and built a structure to the framework based upon actual business operations. This supports the practical way our clients operate and helps them to follow organised steps and plan for the next requirements they have.

Achievable

Building resilience to threats and raising awareness of cyber risks is difficult. There are lots of interdependencies, the use of resources across multiple departments and the implementation of many different solutions and requirements. Standard frameworks are also structured to be processed as documents, requiring interpretation and analysis for each business.

We took away this bottleneck by our process control system, this is matched against the standard framework and project management tools. Our approach helps our clients to make their cyber resilience and compliance achievable. Clients are also able to evidence the needs so that they can better influence and get support for their cyber resilience needs.



Technical knowledge is not required. With reduced jargon, simple and straightforward steps, the platform is easy to use and understand for all.

We enable clients to offer and seek help within the community.

Positive Psychology

Complex and difficult problems such as cyber security and implementing standards require attention and encouragement. Very often with solutions or terminology there is a strong inclination to focus upon the negative. This has the converse affect to the desired outcome and reduces buy-in from those in need or working on the problem.

Our approach is to accentuate the positive to increase engagement and the inclination to work on the problems at hand. Our testing of the platform and current clients showed that this approach was not only refreshing but one that helped them to continuously work on improving their resilience and compliance using the platform.

Social Network (Community)

Our research and that of our trusted partners NEN showed that the implementation specialists were very keen to help or seek help from their peers. This positive approach was almost universal within different sectors and businesses. The specialists understood the threat of cyber security requires a unified front with all businesses working together.

The Isuna platform has a full community space available for our clients, especially those that are more open to gain from a social network approach to producing solutions. This clearly has lots of benefits from increasing the available support network to encouraging communication and innovation between specialists.

Risk & Project Management

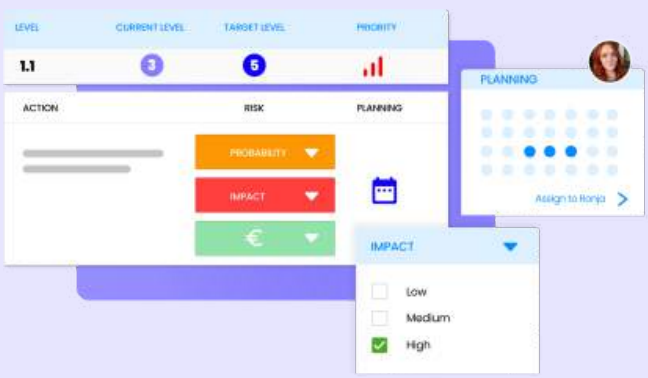
With so many tasks, interdependencies, resources and options for implementation management and prioritisation can prove to be especially difficult. Specialists told us about their challenges in these areas and that a common process was to develop projects using spreadsheets, complete independent risk assessments (sometimes on paper) and then use yet another project management tool for implementation.

With this in mind, we built our platform so that it could be the one-stop-platform for our clients. Risk management tools are integrated into the platform allowing our clients to assess the probability, impact, and cost of improvements. These tools directly connect with the tasking and project management tools. Giving our clients the power to successfully implement and improve their resilience using our complete solution.

Sharing is Caring (Knowledge Centre)

A solution for community would not be complete without a space to enable our clients to share key information and documents. We were acutely aware of the cost of implementing cyber security and about the amount of duplication of knowledge products such as policy and security guidance documents. Also, that the documents available online came with inherent risks such as confidentiality and reduced trustworthiness.

We developed a Knowledge Centre so that our clients can directly find their required documents in a safe and tested location. These documents are peer assessed, categorised, and uploaded so that the clients can save time and money by using trusted materials.



Risk management tools are integrated into the platform allowing our clients to assess the probability, impact, and cost of improvements. These tools directly connect with the tasking and project management tools.

SUMMARY

Digitisation is not just an initiative but a movement towards a more accessible, efficient, and enriched service provision by businesses. Clearly beneficial and valuable it also comes with risks and threats. These can be resolved with effective cyber security and mapping these to the right regulation or standard such as ISO27001.

Businesses must work to the best of their capabilities to ensure that they implement the cyber security and associated standard effectively whilst balancing resilience and cost. The understanding and implementation processes are complex and difficult. Through our committed research and analysis, we have developed an effective platform that can help businesses.

With thorough research and working with experts we provide powerful Cyber Compliance Platform that can enable digitalisation, save businesses money, and increase their resilience.

Isuna BV (KvK 77631692)
HSD Campus
Wilhelmina van Pruisenweg 104
2595 AN The Hague
The Netherlands
info@isuna.net
+31-708903446
www.isuna.net