REALCGR®
Regulatory Technology

RealCGR® provides "RaaS" ("RegTech" or Regulatory Technology as a Service).
We provide secured integrated software that automates, simplifies and embeds compliance into company governance processes. We optimise compliance effectiveness, while keeping cost-of-governance in control.

EU-NIS AND BUSINESS CONTINUITY MANAGEMENT

The EU-NIS Directive (NIS = Network Information Security) is being (or already has been) transposed into national law.

The legislation mainly applies to "Essential Service Providers" (ESPs) as well as digital service providers. These service providers (to be designated by national authorities) will also need to be NIS compliant.

Europe is aiming for a high and common level of security of network and information systems for all ESPs because of their importance for the security and economy of a country.

The EU-NIS directive does not apply directly to ESPs, but to the Member States themselves who implement the EU-NIS through national legislation.

Each Member State therefore introduces technical and organisational obligations that can be considered as "minimum standards".

WHY IS NIS IMPORTANT FOR YOUR ORGANIZATION?

First, your organisation can itself be a provider of essential services. After all, it concerns sectors such as: utilities in general (energy, transport, gas, supply and distribution of drinking water), banking (although with many exceptions), infrastructure and service providers for the financial market, healthcare (hospitals) and digital service providers.

It is also possible that your organisation interacts with the provider(s) of essential services. In many cases, such an organisation will demand the same level of safety from its partners and suppliers. (This is because ESP's have reporting obligations in case of incidents, so, for those reasons, their major suppliers are involved).

It is also possible that your organisation may wish to comply with the principles of EU-NIS for other reasons on its own initiative.

HOW DOES BUSINESS CONTINUITY MANAGEMENT FIT INTO THE NIS STORY?

The NIS irrefutably requires Member States to ensure that providers of essential services take appropriate measures to prevent and minimise the effects of incidents that affect the security of network and information systems used to provide those essential services to guarantee the continuity of these services.
The goal of this guideline is of course to prevent or limit incidents. This must ensure that the continuity of the service provider is assured.

Business Continuity Management is dealt with explicitly many times and has therefore become an unmistakable element in what is (from now on) legally regarded as "good security".

REALCGR®
Regulatory Technology

HOW DOES RISK MANAGEMENT FIT INTO THE NIS STORY?

Not only is the continuity of a company discussed, but also the risks with which it can be confronted are mentioned. Although the risks are not explicitly listed (this would be impossible given the sector specificity), these include cyber risks, physical risks etc.). The "pallet" of risks is therefore broad and non-exhaustive.

The ESP's are required to detect, manage and handle risks through measures including effective Business Continuity Management.

Again, we see that Business Continuity Management, factually and legally, is good business practice.

HOW DOES DATA PROTECTION FIT INTO THE NIS STORY?

The EU-GDPR clearly states that any incident (of a technical or non-technical nature) may involve an infringement if they involve risks for those involved (the data subjects). In other words, losses or unavailability of personal data can be considered as a possible infringement.

The incidents or events that give rise to a GDPR infringement can also cause a NIS infringement.
Handling such incidents or events can therefore be carried out simultaneously, from a NIS point of view, but also from an EU GDPR point of view. The same principle applies about reporting obligations.

WHICH SOLUTION CAN WE OFFER YOU?

RealBCP is a comprehensive business continuity tool (& methodology), when you apply it you will directly contribute to NIS compliance as well as EU-GDPR compliance. (RealDPG is available for EUGDPR compliancy building).

In addition to the numerous benefits of RealBCP, we also provide:

- Five methodical points of contact between EU-GDPR and Business Continuity.
- Compliance with the mandatory ISO22301 documents.
- Compliance with the ISO27001 obligations regarding the continuity of information risk management.
- Full "mapping" of ISO27001 / ISO22301 / EU-GDPR / EU-NIS, which makes your contributions clear and simple.

In short, when you use RealBCP, you effectively contribute to the NIS compliance of your organization.

If you have any questions, we are happy to give you answers.

REALBCP® Business Continuity	REALDPG® Data Protection Governance	REALDSR® Data Subject Rights	REALCRC® Crisis Communication
Business Continuity, governance ISO 22301, ISO 77001	Dataprotection Governance GDPR, ISO 27001 EU & UK GDPR, ...	Data Subjects Rights Using blockchain tables	Smart Alerting and Crisis Communication

Please visit **www.realcgr.com** for more information.