THREATS

Terrorist attacks on Hospitals:
Risk & Emergency Assessment, Tools & Systems

"Co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union''

Report No: DR/ 1/ 004

Report on the synergies that exist between other Critical Infrastructures and the Health Sector and evaluate their portability to hospitals

Version: 1.0

Date: 15 June 2015

Authors: CD, SC and CA

Approved by: CA

Table of Contents

Executive Summary

Our research and our subsequent findings and recommendations contained within this report lead us to conclude that existing critical national infrastructure synergies can to a greater or lesser extent be transported to the healthcare sector. The methodologies for the protection of critical assets developed primarily for the transportation, energy, information and communication sectors can be adapted and developed to support the protection and vulnerability reduction programmes within the healthcare sector. A cross sector approach has enabled this portability to the healthcare sector and the adaption of existing tools and methodologies are required to enable their effectiveness.

Some European Union Member States (EUMS) have already begun and have implemented programmes to enable this. This has required a strategic governance model to be established between the healthcare sector and other critical infrastructure owners and operators, governmental agencies and the intelligence community. Funding streams have had to be established and secured to enable this initiative.

The findings of our research has identified that there is little evidence for a standardised Europe wide network for the reduction of risk to the healthcare sector from terrorism. Whilst many other healthcare service delivery and resilience issues are highly developed, integrated and standardised, terrorism risk and vulnerability reduction is more disparate.

A system with appropriate levels of protection is required to reduce the vulnerability of the healthcare sector from terrorism. This network could share information; good practice, research and develop standardised risk reduction methodologies and guidelines.

1. Introduction

1.1 Strategic Directive

The THREATS project was designed to step through from an analysis of the current situation, through an identification of the management of risk and a study of the risks to the Health infrastructure to an analysis of the methodologies used against terror risks. However a common thread that has emerged throughout the research phase of each deliverable report in Work Package 1 (WP1) of the THREATS project is the lack of accessible publically available information relating to risk management methodologies and vulnerability reduction programmes within the field of critical infrastructure protection (CIP). Some European Union (EU) Member State (MS) governments provide a national or strategic level directive to the Critical National Infrastructure (CNI) sector that is available within the public domain (see D1.1), such as Poland and Sweden. The directives typically contain information and guidance relating to the threats and hazards that might affect specific sectors and the risks, such as flooding and the subsequent impact upon services and utilities with operational infrastructure in the affected area. Other information relates to collaboration across a sector to share information and best practice, supported by regulation and codes of practice. These documents therefore provide some sort of strategic directive but fall short of being a full "methodology" because of the issues of National Security that have been discussed in earlier deliverables.

Therefore it seems that the strategic directive issued at National Government level is a useful point of reference for implementing risk management and vulnerability reduction programmes at operational and tactical level within a CNI sector. Research carried out already by the THREATS team has found some evidence to indicate that progress is being made in some sectors but the evidence does not extend to all sectors or all EU MS, although the European Commission (EC) has sponsored projects and initiatives to gain deeper understanding of CIP and raise awareness across all 28 EU Member States.

1.2 Operational management

Deliverable Report 1.3 (D1.3) reported on the COUNTERACT (2009) report that addressed a series of issues affecting risk assessment methodology across all sectors of CIP. These included the lack of expertise or experience in assessing risks and limited ability to scan the threat horizon effectively, or understand which hazards and threats are likely to affect the organisation. The report highlighted barriers to effective risk management, including lack of guidelines or best practice (COUNTERACT, 2009:4-9). Although many of the observations

listed in the report will need to be acknowledged at a senior level, they are mainly applicable at the operational or practitioner level with oversight at a tactical level within an organisation.

Establishing meaningful standards in order to measure performance and implement best practice across a network of organisations within a given sector of CIP has been discussed previously in D1.2 and supported by evidence contained within the literature. Establishing a network to share information relating to the threat landscape could be a useful step towards a more joined up approach, notwithstanding commercial or competitor issues. The research team continue to uncover evidence that standards have yet to be implemented in some areas although organisations acknowledge the benefit and utility of standard practice and shared information networks:

> 'Improving the effectiveness of risk management across supply chains and transport networks requires risk exposure to be better quantified and made more visible. Companies struggle to quantify the risk exposure of their own organisations due to lack of understanding, standardised metrics and relevant and up-to-date data on supply chain risk; without a platform to share data and information, assessing systemic global exposure is difficult'.
> (World Economic Forum, 2012:12)

Challenges with communication within an organisation are nothing new. There are many events throughout recent history where serious consequences have occurred and the subsequent investigation has attributed some of the blame to poor communication between personnel at all levels, the effect has been the lack of shared knowledge or situation awareness between critical personnel, such as the Love Parade catastrophe in Duisburg, 2010. The problem with communication and developing better working practices remains and was highlighted by the European Commission sponsored project European House of Design Management during the 2013 Milan workshop, which summarised its findings relating to the public sector as:

> **'A. Knowledge and information sharing.** It appears difficult to share knowledge and information between different public sector organisations as well as varying levels within an organisation.
>
> Public sector organisations, in particular in Italy, are not capable of looking past their own activities and see the value of sharing knowledge. Often, this is a direct result of bad coordination.
>
> It was suggested that there are varying silos within the public sector and that, within

those silos, little gardens exist that are a private territory, highly resistant to collaboration or contributions by others.

B. Cyclicity. One of the major challenges for implementing design management in the public sector is cyclicity, also previously pointed out during the workshop in London. In politics there are classic periods in which a party/person can initiate developments. However, as soon as the reign of this party/person is finished, there is a big risk of the project being stopped and not completed.

C. Evidence of Design & Design Management. In order to convince public sector organisations to implement design management methodologies, they will need to be convinced by evidence of ROI. Case studies and pilot projects are seen as a ways of evidencing design and design management, however, it is very important that the examples are relevant to geographic area, project scale and industry.

D. Understanding the process. There is little understanding of design and design management processes in the public sector. Instead of seeing design management as a radical method of running a project, a gradual increase in project size/risk should be stimulated – starting small and increase the size of project once the smaller project has provided evidence of success'.
(EHDM, 2013)

1.3 Cross-sector approach

In other areas such as the transport sector there is evidence to indicate that a cross sector and cross MS approach to risk management is being adopted and practices are becoming standardised. This ensures that transportation that crosses international borders has been managed, in terms of risk management and all the component parts that underpin an effective risk management strategy; such as maintenance, have been conducted to an agreed standard. The Office of Rail Regulation in the UK work to a common safety method for risk evaluation and assessment and the guidance document (Guidance on the application of Commission Regulation (EU) 402/2013, 2015) provides information to assist the risk assessment process by setting out criteria to determine when a risk assessment is required (in order to avoid duplication of work) and to outline the legal requirements within the UK and other parts of the EU as appropriate. Other areas of the transport sector, such as aviation and maritime, have similar standards and compliances to ensure shipping or aircraft entering sovereign territory are operating safely. This provides useful data that demonstrates common practices and standards can be shared and has good utility across discrete organisations operating in the same sector within the international arena.

This provides a snapshot of the various approaches applied to risk management within the field of CIP but the emerging themes are an ‘all hazards approach’, ‘systematic approach’ and ‘enterprise risk management’ (ERM). One important aspect that must not be overlooked is the consideration of ‘profit’ and commercial competitiveness. Many organisations that contribute to the national infrastructure are ‘for profit’ and although operational compliances, regulation, monitoring and strategic governmental oversight will be in place, the primary drivers for the organization are likely be profit and sustainability/competitiveness in the global market. Hospitals, on the other hand, provide a mix of public and private organisations, sometimes forming part of a wide network of associated hospitals or standalone private entities. It might be useful if this paper can take a step towards establishing a level of commonality across all entities.

1.4 Scope

This report forms part of a progressive and cumulative development of knowledge within CIP and the health sector of CNI. Much of the information available for analysis is constrained to national strategic directive and organization top management policy contained within annual public reports. The detail about how risks are managed at the operator level and within specific boundaries remains elusive, in part due to the sensitivities relating to CIP but also due to the absence of shared sector wide information and practice. Information relating to risk assessment methodology is available though information relating to vulnerability reduction methods is scarce.

The scope of this paper includes an analysis of the risk assessment methodologies and vulnerability reduction programmes and attempts to identify the synergies that exist between other CNI sectors and the health sector, with a view to selecting methods or component parts of specific methods that have portability to the health sector. The preceding deliverable reports of the THREATS project provide a detailed and comprehensive insight to CIP within the health sector but the evidence of risk assessment methodology and vulnerability reduction programmes within the health sector has been very scant and therefore it may not be possible to fulfil the aim of this paper in its entirety. However, there does exist some information relating to specific sectors of CNI at tactical and strategic level that may prove useful and this paper will attempt to gather up the various strands of publically available information and seek to identify if there is indeed anything useful and portable to the health sector and the hospital setting.

2. Literature Review

2.1 National Directive

Deliverable report D1.1 provides a useful start point to look at how risk is managed at the strategic level and guidance in the form of a policy or directive assists service and utility providers of CNI to risk manage their operation in a way that supports the national directive. The way CIP is managed across all EU MS is very much dependant upon individual MS and the approach adopted at government level, which is driven by the perceived threat and the priority sector of CNI, such as the focus on critical infrastructure information protection (CIIP) in Bulgaria and Estonia (see D1.1 Annex A). Some EU MS governments have been proactive with setting the strategic framework for CIP, while other governments seem to be less developed in this field. This will undoubtedly have an effect on the way risk is managed operationally.

The UK government provide an example of the type of information that is useful to all sectors of industry but does not disclose information that is sensitive or useful for attack planning purposes. A series of documents can be found at www.gov.uk and examples include Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards (2010) supported by the recently up dated version of the National Risk Register (2015). This type of approach sets the tone for risk management at a national level and provides a strategic directive for operators and service providers to ensure they manage their contribution to CNI in a way that supports the national effort. Moreover, the UK government has established an agency, Centre for the Protection of National Infrastructure (CPNI), to provide close support and guidance to CNI providers. D1.1 identified similar arrangements in other MSs, such as Sweden and the MSB (Swedish Civil Contingencies Agency) but also discovered that coordination is being conducted as part of a network of countries (CIVPRO) that may not encourage any specific coordinated effort at a national level.

2.2 Managing Risk

The research and review of the literature for this paper has identified a variety of risk management methods that are specific to managing commercial risks such as market and financial hazards, the methods seem to be profit driven and provide limited evidence to suggest the scope extends beyond profit and competitiveness. There is very little information available to indicate that terrorism has been considered as a hazard or threat and where malicious events have been indicated as a potential threat the corresponding information is

not available for analysis. Two example organisations that do list terrorism as a potential hazard are German electricity provider EnBW, a subsidiary of EDF and the Portuguese energy company Galp Energia.

EnBW operate a risk management system that is managed across the whole organisation and is implemented as part of a 'top management down' approach whereby the policy is set by the executive board and various management processes are implemented to ensure the risk management plan is carried out effectively at the strategic level, down through the business functions to the operational level. This means the risk management system is embedded or integrated throughout the organisation:

> The integrated risk and opportunity management system (iRM) is based on the internationally established COSO II framework standard for risk management systems that span entire companies. The iRM system aims, through a holistic and integrated approach, to effectively and efficiently identify, evaluate and manage risks and opportunities (including monitoring) and report on the risk/opportunity position, as well as to ensure the appropriateness and functionality of related processes. Risk management involves measures for avoiding, reducing or transferring risk, as well as measures for managing or tolerating risk in the financial statements. EnBW defines a risk/opportunity as an event that might cause a potential non-attainment/over-attainment of strategic, operational, financial and compliance goals in the future. In order to identify and categorise risks and opportunities, the risk and opportunity map that is anchored throughout the Group is utilised.
> (EnBW, 2014:74)

The risk and opportunity map (see Fig. 1.0) lists the various hazards and threats under four main headings: 'strategic; operational; financial and compliance'. Each area is further sub divided, including 'operational' that is divided into 'business activity; infrastructure; mankind & environment'. The 'mankind & environment' section includes 'criminality, sabotage and terrorism' as hazards (EnBW, 2014:74). The report does not provide any detailed information relating to the operational activity that is being used to mitigate the risk nor does it describe how it monitors the hazards and takes action when they become a threat. However the map provides a clearly defined matrix of identified risks that could impact the organisation and is the single point of reference, as directed by top management, for identified risks to the organisation. The map provides the first layer of information required to create a risk register, similar to the UK National Risk Register mentioned previously. Although the map does not provide any specific detail, it does inform each critical function of

the risks identified at strategic level and where they might impact the operational level. Furthermore, the map does not prioritise one function over the other and it seems that financial risks are managed in a similar manner to the risks in the operational and compliance functions.

Strategic	Operational			Financial				Compliance
	Business Activity	Infrastructure	Mankind & environment	Market	Lending	Liquidity	Financial reporting	
Governance	Models	Plants/ grids/ storage	Personnel/ labour market	Market price in general	Counterparties	Cash flow	Financial accounting	Active corruption
Market development/ society & trends	Business processes	Locations/ buildings	Occupational health and safety/ health protection	Interest	Countries	Convertibility into cash	Tax	Passive corruption
Technology	Operations	IT management	Environmental protection	Margin	Issuers	Refinancing for own account	Debtors	Antitrust law
Politics	Products/ contracts	Information security	Contaminated sites	Forecast [volume/ structure]	Collateral		Creditors	Data protection
Competition	Projects		Weather/ natural phenomena				Asset accounting	Confidentiality
Clusters/ concentration	Approvals/ licenses/ patents		Criminality/ sabotage/ terrorism				Consolidation	General fraud
M&A/ investments	Legislation/ regulation/ litigation						Service billing	Financial fraud
								Procurement fraud

Fig. 1.0 Risk Opportunity Map (EnBW, 2014:74)

The map is contained within a publically available annual report and goes some way to illustrating the level of diligence applied to the management of risk within the company. Although not specified within the narrative, it would be logical that detailed risk registers are held and maintained within each of the business functions and further detailed and specific registers are maintained at operational level within specific departments. This type of approach enables risk to be managed efficiently within functions, a threat in one area may not necessarily affect other areas of the business. Conversely, threats affecting a specific area of the business could impact across multiple areas of a single function and spill into other functions due to dependency and interdependency relationships (see D1.2 para 1.8 and 2.7).

Galp Energia operate and manage risk in a similar manner to EnBW, adopting the COSO guidance and operating an 'internal control system' within the organisation. The internal control system is described as:

> ... a set of policies and procedures adopted to ensure, with reasonable likelihood of success, the fulfilment of the Company's goals in the following areas: orderly and efficient conduct of its businesses; safeguarding of its assets; prevention and detection of fraud and errors; compliance with laws and regulations; and reliability of financial reporting.
>
> This system is based on the guidance provided by the Committee of Sponsoring Organisations of the Treadway Commission (CoSO) on the main features of Galp Energia's internal control system: the control environment, risk assessment, monitoring, information and communication.
> (Galp Energia, 2014:51)

The annual report (2014:54) contained information detailing the various risks that could affect the company. The information was listed under four main headings: 'strategic risks; operational or compliance risks; external risks and financial risks'. The operational or compliance risk section included a sub heading 'Health, safety and environment' and detailed the following risks:

> Given the range and complexity of Galp Energia's operations – for example, in ultra-deep-water exploration and production, or during the refining process – the potential HSE risks are considerable. These include major incidents involving the safety of processes and facilities, failure to meet approved policies, natural disasters and civil unrest, civil war and terrorism. Exposure to generic operational, health and personal safety risks and criminal activities are also included.
>
> A major incident of this sort may cause injury, loss of life, environmental damage or the destruction of facilities. Depending on the cause and severity, they may affect Galp Energia's reputation, operational performance or financial position.
> (Galp Energia, 2014:54)

The similarities between EnBW and Galp Energia in the way they manage risks are clear and are linked to a common approach to risk management, the COSO framework. Both organisations manage risk in separate business function areas and neither company has indicated a priority of one function over another. Furthermore, the process of identifying potential risks has led both companies to list terrorism as a hazard within the operational business function.

2.3 Committee Of Sponsoring Organizations of the Treadway Commission (COSO)

The Committee Of Sponsoring Organizations of the Treadway Commission (COSO) are a United States of America (USA) based 'voluntary private sector initiative dedicated to improving organisational performance and governance through effective internal control, enterprise risk management, and fraud deterrence (McNally, 2013:2). SOCO released the original framework in 1992 but has up dated the guidance in recent years to align with the Sarbanes-Oxley Act (SOX) Section 404, that is part of US federal law to ensure public companies implement an internal control framework and report on the effectiveness of the framework annually as part of a comprehensive audit system. Although SOX is not part of European law it does impact upon companies listed in the USA but operating in Europe. Moreover, the framework designed by SOCO may provide utility to sectors of CIP, including health, and is a proven method of managing large networked organisations. The framework is currently being used to good effect by numerous multinational organisations with networks of outlets or subsidiary companies operating remotely to the main Group headquarters.

A closer look at COSO identifies the core objectives and integrated components of the COSO framework as:

> ...three categories of objectives—operations, reporting, and compliance—and still consists of five inte- grated components of internal control—control environ- ment, risk assessment, control activities, information and communication, and monitoring activities. The Frame- work continues to be adaptable to a given organization's structure, allowing you to consider internal controls from an entity, divisional, operating unit, and/or functional level, such as for a shared services center. Finally, the important role of management judgment in designing, implementing, and maintaining internal control, as well as assessing its effectiveness, is retained. (McNally, 2013:4)

This suggests the framework is useful throughout the complete management structure of an organisation and can be used by the Executive Board to apply across the whole company or focused on a specific operation.

Aguas de Portugal Group consists of 41 companies involved with the water production and wastewater management industries. Risks to the group are categorised using the COSO methodology and monitoring of the risk landscape is centralised and conducted across the

whole group. However, each company within the group has deferred authority to ensure conformity to the group policy, planning and reporting are dealt with and monitored by each individual company, a method that is mirrored by the Croatian oil exploration and production company, Industrija Nafte (INA). Although INA don't provide specific risk management information, there is evidence to imply a risk framework for subsidiaries is determined top down at group level (INA, 2013:45). Both companies demonstrate a form of ERM that sets the policy for managing risk but then enables individual operations to risk manage locally. The auditing and risk control department operate independently to the boards of each company, which ensures each company have to manage their risk register effectively and are accountable for their actions via an established audit process at Group level.

2.4 Enterprise Risk Management

Many CNI service and utilities providers are large organisations that often have business interests in more than one MS. The organisation may be responsible for a vast network of outlets that collectively, provide an important contribution to CNI, such as electricity generation and distribution. These types of organisations can be described as an enterprise and are often managed using the Enterprise Risk Management (ERM) approach whereby the risks are assessed further up the management chain and the assessment is applied across the whole network. An example of the ERM approach can be observed with the German based electricity and gas utilities and service provider E.ON. The company currently has operations in numerous EU MS; including Czech Republic, France, Germany, Hungary, Italy, Netherlands, Romania, Slovakia, Spain, Sweden and the UK and has global reach as far as the United States of America and Russia (E.ON, 2014). The 2014 Annual Report provides a chapter dedicated to risk management though the preeminent theme was about financial risks, described as 'systematic risk management to monitor and control our interest-rate and currency risks and manage these risks using derivative and non-derivative financial instruments' (E.ON, 2014: 62).

Other CNI utilities and service providers adopt a different approach that maintains control of financial risks but manages the financial part of the business discrete to the operational component. The Water Services Corporation in Malta is an example of this approach and describes risk management as:

> 'The Corporation manages operational risk in an integrated manner within its Management Systems, whilst financial risk is managed through the Internal Audit department. Both are intended to detect issues and recommend mitigation measures to control and minimise risks. Whereas Management Systems reports to the CEO,

> Internal Audit reports to the Internal Audit Committee that is composed of three Board members thus ensuring independence'.
> (WSC, 2011:12)

Due to the size and geographical disposition of Malta threats identified in one location are likely to be a risk to operations in a different part of the country and therefore an 'integrated' management approach is highly appropriate. However organisations spread across large regions and different MS are likely to face different threats at different times and therefore an integrated approach may not be the most efficient or effective methodology, though integration could indicate a level of standardisation within a large organisation.

GAZPROM are a Russian gas and oil company that have global business interests, supplying a large quota of gas to the Russian market and exporting to over 30 countries throughout Europe and further afield. The global reach of the company will certainly expose it to different operational risks that are critical in one region but irrelevant in another. GAZPROM owns and operates the world's largest gas transmission network that crosses international boundaries, including regions that are experiencing political unrest or conflict such as Eastern Ukraine. The operational, regulatory and financial risks affecting the company are likely to form a complex risk matrix that prevents a 'one size fits all' approach in this case.

Conversely the Association of Gas and Water (DVGW) in Germany has taken significant steps since 2004 to improve practices across the water supply industry and develop a collaborative approach that encourages use of best practice across all business functions and seeks to support a programme of continued improvement. Critically, service providers supported this initiative even though the initial reaction was one of 'scepticism' because Germany had enjoyed a continuous and safe drinking water supply for the last 150 years.

It may not be possible to identify a single risk management methodology that will fit perfectly with the Health sector, the methods currently being used across other sectors of CNI have been adopted because they provide the management with the tools required to manage risk in a specific field and a single method is unlikely to be effective across multiple sectors. However, there are similarities with some of the component parts of risk management methods that have potential utility in many sectors, including health. The research team has focused on components that are currently being used by organisations with a wide footprint across a State, using a network of outlets that often span multiple MSs, in a similar way to hospital networks.

2.5 Risk Committees

Risk committees provide a team of dedicated experts within a company to focus their attention on the hazards and threats that have potential to impact the organisation. The hazard and threat matrix is applied across the business functions where the business activities are used to provide context and enable the risk exposure to be measured or quantified. The risk committee can then report their findings to the Executive Board where an informed decision can be taken to adjust activity to reduce the assessed risk or take other risk management options.

In most cases the risk committee are situated at a tactical level within the company that provides a view across the operating functions and department heads that have one 'foot in the operational area and one foot in the senior management area' of the company often populates the committee. An example of this approach is Eesti Energia, an Estonian based electricity, gas and oil producing company that uses a risk committee to manage the risks in a top down approach across the whole company. According to the Annual Report (2014:66) the committee reports direct to the Chairman but there is no information to imply any external or independent audit of the management process.

The German gas provider RWE have a adopted the risk committee approach but have implemented a tiered system to ensure management decisions are validated and responsibility for the management of Group wide risk does not sit with one single team. RWE make it clear that the overall responsibility for risk management resides with the Executive Board but the Risk Management Committee, made up of heads of department, is responsible for monitoring and refining the risk management system. The team that actually enacts the management system sits below the Risk Management Committee and is called the Group Controlling Department. They are responsible for the control, steering and coordination of the risk management system (RWE, 2012:88).

Enel, an Italian electricity and gas provider uses an additional level of risk management. A risk committee sits at Group level and provides a similar function to the previous examples but has applied additional risk committees at company level to horizon scan for risks and apply management systems locally (Enel, 2014:100). The report does not provide additional information but the research team can see the benefit of managing risk locally as long as the lines of communication between the two risk committees are effective to provide a timely alert to any changes on the risk landscape at the strategic and operational level.

2.6 Risk Models

There are many ways to measure risk to an operation, methods include computer modeling and simulations or other forms of statistical or mathematical techniques. The two distinct types of simulations are parametric and non-parametric simulations, each has advantages and disadvantages and should be carefully applied by an expert to ensure the relevant approach has been adopted and the results are reliable.

Parametric approaches, including the widely used Monte Carlo simulation, are 'a simulation, where specific distributional parameters are required before a simulation can begin' (Mun, 2006:77). In simple terms a set of defining parameters are required to be measured against various scenarios or a simulation of algorithms which enables the result to be calculated using a random process to generate solutions. Alternately a non-parametric approach could be used when the parameters are particularly hypothetical; Dowd (2005) describes the non-parametric approach as:

> All non-parametric approaches are based on the underlying assumption that the near future will be sufficiently like the recent past that we can use the data from the recent past to forecast risks over the near future – and this assumption may or may not be valid in any given context. In deciding whether to use any non-parametric approach, we must make a judgment about the extent to which the data from the recent past are likely to give us a good guide about the risks we face over the horizon period we are concerned with.

What has become apparent to the author of this paper is the use of mathematical and statistical risk management is reliant upon accurate and relevant data to set the parameters for simulations. This might be a useful tool for predicting financial and other statistical matters such as the insurance industry, and may be able to accurately project the cost and impact of a terrorist attack but is less likely to forecast when and where an attack is likely to take place. The Monte Carlo simulation and other mathematical approaches go some way to project the impact of risk in terms of cost and potential disruption to the business but they do not remove the uncertainty associated with risk. Uncertainty will always be present even though the risk may never actually occur and organisations will need to ensure they are postured to respond to uncertainties, should they develop to become actual risks.

Mathematical or statistical methods like the Monte Carlo simulation method are often used as a component part of a risk management strategy, as seen with Austrian State owned electricity provider, Verbund. The company emphasise a company-wide approach to risk management and have a separate strategic unit for coordinating processes (Verbund Risk, *n.d*.5). However the Austrian gas company, OMV also use the Monte Carlo simulation method to project and monitor risks but key risks are considered to be financial and are

managed as a Risk Bearing Ability and Equity. The company provides no other information relating to operational risks or security.

The financial impact of risk is a priority consideration and will likely be a key driver to the way risk is managed within an organisation. The French electricity and gas provider, E.ON manage the risk to the company based on categories of earning impact: low (under €0.5 billion), intermediate (€0.5-1 billion), high (€1-5 billion) and very high (over €5 billion). Statistical methods, simulations and expert opinion are all considered to inform the risk management process and E.ON specify that they use the Monte Carlo simulation method to identify dependencies between individual risks in order to understand the potential for impact across business functions (E.ON, 2014:62-68).

2.7 Standards

A potential benefit for the ERM approach to risk management would be the application of a common standard across all subsidiaries of a company, but it has already been discussed in D1.2 (see para 1.5) that organisations often operate to multiple standards within a single company, particularly when business functions are managed within silos. But this research has discovered that some organisations, like CEZ Gas in the Czech Republic, are working towards a common standard within their company. CEZ Gas operates an integrated risk management system but has taken steps to have the system audited externally in order to ensure it complies with industry recognised best practice and legislation (CEZ Gas, 2013:52-53). The MVM Group in Hungary operate in a similar manner, although detailed data relating to the business operations was not identified, the company state the use of a 'code of practice' that has been integrated across the group (MVM, 2014:22). Other companies, such as Enel (Italy), subscribe to 'international best practices' but no further information is available to identify which practices and accredited methodology is actually being applied, unlike the telecommunications company Vivacom (Bulgaria) that have announced accreditation to ISO IEC 20000-1:2011: 'a service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS. The requirements include the design, transition, delivery and improvement of services to fulfill agreed service requirements (ISO, 2011).

The International Standards Organisation (ISO) operates across international boundaries and provides useful standards in most areas of industry. Many companies now align themselves to specific ISOs because it is becoming widely recognised as best practice and they are able to demonstrate that they operate and are accredited to a globally recognised standard. Gaz System (Poland) has embraced the ISO and is developing the current level of ISO accreditation, currently Gaz System are ISO 14001:2004 'Environmental Management

Systems', ISO IEC 27001:2005 'Information Safety Management System' and ISO9001 'Quality Management Systems' accredited. According to the Annual Report (2013:40-42) the company are working towards gaining the ISO 22301 'Business Continuity' accreditation.

Hospitals may not need to gain ISO accreditation but common recognised standards to ensure the hospital and the various business functions within the hospital and wider trust are managed and monitored in a way that ensures they remain viable and cost effective components of the health sector in the same way other sectors of CIP manage their activity to remain profitable and competitive.

2.8 Supply Chain Risk Management

Supply chain and transport risk presents a complex area of industry to risk manage because by definition the asset that requires the protection and risk management is in a constant state of motion and is invariably coming into close contact with multiple risks associated with the environment, geopolitics and the economy, notwithstanding the multiple interdependencies relating to complex global transport networks and the hazards and threats are outside of the risk owner/ manager control. The World Economic Forum (2011:8) conducted a survey (Fig. 2.0) to identify which external events, when combined with existing network vulnerabilities, have the potential to cause widespread, systemic disruptions:

Environment	Natural disasters	59%	
	Extreme weather	30%	
	Pandemic	11%	
Geopolitical	Conflict & political unrest	46%	
	Export/ import restrictions	33%	
	Terrorism	32%	
	Corruption	17%	
	Illicit trade & organized crime	15%	
	Maritime piracy	9%	
	CBRN weapons	6%	
Economic	Sudden demand shocks	44%	
	Extreme volatility in commodity prices	30%	
	Border delays	26%	
	Currency fluctuations	26%	
	Global energy shortages	19%	
	Ownership/investment restrictions	17%	
	Shortage of labour	17%	
Technological	Info and communication disruptions	30%	
	Transport infrastructure failures	6%	

	Uncontrollable
	Influenceable
	Controllable

Fig. 2.0 World Economic Forum survey (2011:8)

Although the main categories are similar to those identified through the COSO method, these results are derived from a survey (although the narrative didn't specify the survey target audience – it is assumed by the research team to be operatives and managers involved in the transport infrastructure sector).

These potential impacts or vulnerabilities have been widely accepted throughout the global transport and supply chain sector and are not specific to a small group of isolated organisations. This means a more collaborative effort can be made across sector partners and between public and private entities. The interdependencies between different networks and across different parts of the globe need no further discussion and so it would seem logical that the risks affecting so many sector operations would encourage a joint effort to develop a common approach to managing those risks, and it is worth remembering that a network is only as resilient as the weakest link and therefore it is in the interest of all parties to make good progress.

The World Economic Forum and industry partners have made significant progress to a joined up approach to risk management and have already conducted research to analyse 'the difference between the risk management methods available today and those most important in the future enabled the identification of the five specific mitigation methods requiring further development (World Economic Forum, 2012:15). The tone of the report is most encouraging and makes a series of comments that imply a sector wide effort in the near future to improve risk management within the supply chain and transport sector:

> Experts noted that these priority risk management areas are not mutually exclusive; implementation might be enhanced by thinking of these tools as part of a set of management measures (Figure 8). The first step for businesses and governments will be identifying and developing the trusted networks integral to effective collaboration. Bringing together different public and private sector entities will allow greater sharing of data and information, enabling organizations to better understand and quantify supply chain and transport risks. This in turn will inform public and private sector investment in areas of vulnerability and facilitate the development of proactive and effective legislation, as will the collaboration of key players from across companies, regions and sectors in multistakeholder scenario planning.

The effort and progress that is taking place within a complex and competitive industry sector makes good reading and sets a good example to illustrate that joint effort can be

accomplished if all stakeholders engage. The World Economic Forum report (2012) provides a useful guide to establishing a common risk management framework across the EU health sector and although many individual hospitals will no doubt have developed plans and processes in place to manage risks and respond to terrorist threats, a collaborative effort will enhance those hospitals that may be struggling to meet the contemporary threat in terms of preparedness, response and business resilience.

A series of existing risk management tools and processes identified by the World Economic Forum (2012:21) has been included at appendix 2. Many of the tools are likely to be used already across the health sector but the table provides a useful reminder of some of the simple but effective management methods that can easily be overlooked.

2.9 Managing risk under normal operation and in crisis situations

An important component of risk management is managing the risks during a crisis situation. The literature provides examples and insights to crisis management but it is not immediately obvious without close scrutiny. However Merkel and Castell-Exner (2010:19-22) have produced an insightful piece of work in collaboration with the German Association of Gas and Water (DVGW). The paper discusses how a complex operating environment like a water supply company manages the operation during normal operating conditions and how different processes engage to manage the operation during a period of crisis.

DVGW have taken extensive steps to review the practices and procedures across the industry in German to identify and implement some best practices. The driver for improvement was the World Health Organisation Water Safety Plans (2004) that were designed to provide a safe standard of drinking water globally. WSP (2004) triggered a process within DVGW that ultimately resulted in a new German industry standard for the safety of drinking water: DVGW Technical Guidelines W1001 ‘Safe and secure drinking water supply – risk management under normal operating conditions’ and W1002 ‘Safe and secure drinking water supply – organisation and management in the event of crisis’. These two standards were developed by sector practitioners and have been embraced across the whole industry in Germany as best practice.

Merkel and Castell-Exner (2010:19-20) explain that W1001 Safe and secure drinking water supply – risk management under normal operating conditions ‘takes the fundamental elements of the WHO WSP approach and integrates them into the DVGW technical rules. It serves as a basis for risk-based and process-orientated management of normal operation’ and encourages a culture for continuous improvement and ‘promote mutual understanding

between, and cooperation of, water suppliers with the local supervisory authorities'.

W1002 Safe and secure drinking water supply – organisation and management in the event of a crisis 'enables water suppliers to take action in the event of a crisis in order to ensure the continued supply of water to the greatest possible extent and to restore normal operating conditions as quickly as possible (Merkell and Castell-Exner, 2010:20).

The DVGW model makes a very clear distinction between normal operations and operating during a crisis. Sometimes organisations pay limited attention to crisis management and are fooled into thinking the management of a crisis is conducted with the same management team with some additional assets. DVGW assert under normal operating conditions the existing operational functions in a company can 'work jointly on a systematic risk management process'. The team includes a mix of operators and managers who work out all hazards in the supply chain from resource, treatment, distribution to tap' (Merkell and Castell-Exner, 2010:20).

The DVGW approach suggests a 'utility cannot foresee a particular event', though the impact of an event is dependent upon the use of risk registers and the overarching risk management methodology. But once the crisis has been confirmed and the operation is changed from normal operating conditions to emergency conditions the nominated crisis management team can 'step up to the plate'. A critical factor for the effectiveness of the crisis management team are the defined working procedures and the 'hierarchical decision-making process' during a crisis that must be designed, tested, accepted and endorsed by all members of the management team before a crisis occurs. Included within the crisis management planning process is consideration to succession planning and additional capacity to manage an enduring incident and careful consideration must be given to lines of communication between operating groups and the crisis management team to ensure information flows quickly both ways and accurate information is available to the team to inform decision making processes.

Strategic messaging or communicating with the outside world is included in the crisis management plan to ensure a suitable person has been nominated and is trained and practiced in the field of public and media relations. It is important the spokesperson only discloses 'validated information to the outside world with high reliability'.

According to Merkell and Castell-Exner crisis management in a real case will only work properly after sufficient training. So training emergencies should be designed and organized in regular intervals to verify functioning and to evaluate and to refine structures and processes' (2010:21).

The DVGW approach to risk management during normal operating conditions and during periods of crisis provides some useful tools and practices that may have utility in the hospital setting. The importance of selecting and training a dedicated team to manage the operation through the period of crisis cannot be underestimated, the crisis management team will have been carefully trained and regularly exercised to ensure they remain 'match fit' and the additional training and testing commitments may be beyond the capacity of the regular management team.

2.10 Protective Measures

The companies that apply the COSO framework to their risk management approach invariably identify terrorism along with sabotage and crime as hazards to the operation. However, apart from acknowledgement by some MS governments within the policy and strategy documents, terrorism is not widely identified or acknowledged as a potential threat and when it is included as a hazard or threat the information does not provide any details about how the risk of terrorism will be managed.

However, the State owned Swedish electricity and gas provider, Svenska Kraftnät, have identified sabotage as a hazard that could impact upon the uninterrupted supply of gas and electricity to the Swedish population. Svenska Kraftnät have outlined measures to reduce the risk to parts of its infrastructure, measures that are closely aligned to the 'physical protection of buildings and assets' critical pillar (see D1.2 para 1.7):

> At present the risk and likelihood of sabotage in relation to Svenska Kraftnät's facilities is slight. However, the threat scenario can change rapidly. In conjunction with converting or building new station facilities, physical protection has been increased through better perimeter security. An investigation has even been conducted to identify the parts of the national grid most vulnerable to sabotage. Camera surveillance has been installed to monitor facilities, and important elements are equipped with alarms.
> (Svenska Kraftnät, 2012:15-16)

This information implies that simple security measures have been implemented to target harden critical components of the infrastructure and deter potential attack from criminal through to terrorist attack. The deployment of closed circuit television (CCTV) should provide an element of deterrence but will also support the detection of potential attack, both during the actual assault but also during the hostile reconnaissance or attack-planning phase. Furthermore, good quality surveillance still and full motion video footage provide an excellent

evidential product in the event of a prosecution. An additional benefit of CCTV surveillance is the ability to provide support and monitoring for staff that are working alone or in small teams at remote sites.

Alarms can provide an excellent level of deterrence and detection. Audible alarms can deter potential intruders from progressing further into the facility, ensuring only the outer zone is penetrated. Passive alarms are also useful, especially when suitable reactive measures are in place to detain intruders before they can escape. Both audible and passive alarms can be used with CCTV, the alarm wakes up the CCTV surveillance system to capture the evidence and provide a live feed to the security team. These simple security measures can be deployed as a high profile visual system or more discreetly, in a similar way to surveillance and alarm systems currently deployed at airports, shopping centres and other crowded public spaces. There are likely to be issues relating to privacy and patient confidentiality within the hospital setting but surveillance systems can be deployed in a manner that supports privacy issues but also provides a level of protection for staff, patients, visitors and contractors in the public spaces of hospitals or the quieter areas such as service corridors.

Perimeter fences or barriers will seldom prevent unauthorised access to the determined intruder but they do provide a visual and physical deterrence and the first ‘layer of the onion’ when establishing a layered security system. Many types of security are only effective against specific threats and there will often be gaps or vulnerabilities within the defences. A layered security system uses multiple types of security components to form a security layer, and when the layers are combined into a single system they will provide a comprehensive system that provides a good level of deterrence, detection and protection against the type of attack identified during the threat assessment process. In the case of Svenska Kraftnät, a vulnerability study has been conducted across the infrastructure and additional security measures have been deployed at critical or vulnerable locations. The improvement to perimeter fences, use of CCTV and surveillance monitoring and the continued surveillance of the risk landscape will assist the company to protect its assets.

2.11 Beyond the European Union

The research team felt it would be remiss not to look beyond the EU for risk methodologies or tools that have portability to the EU Health Sector. The Health sector in North America is well developed with risk methods for managing risks relating to a broad spectrum of hospital centric issues from medical litigation, facility management to dealing with mass casualty events resulting from natural and man made incidents. However Carroll et al. (2014:3) describes the implementation of Enterprise Risk Management in the US health sector as:

‘while making significant strides – still lag behind large organisations, public companies, and financial services organisations’. The use of ERM in other sectors is well documented throughout this paper but an example of ERM being applied to the Health sector may be a useful contribution. The ERM framework set out by Carroll et al. (2014:1-21) illustrates how an ERM approach can be used to risk manage hospitals. The process and steps are clearly defined and include:

- Risk and opportunity identification
- Risk evaluation and assessment
- Strategic risk response
- Review/ evaluate/ monitor

A key component for ERM is the hazards and vulnerability analysis (HVA) or sometimes called the threat assessment. The HVA is integrated into the framework discussed by Carroll but other HVAs can be effective to support risk management outside of the ERM approach. The American Society for Healthcare Engineering (ASHE) of the American Hospital Association offers a standard methodology developed in 2000 for performing a hospital HVA. Kaiser Permenente (2001) developed another all hazards HVA which is widely used in hospitals. The Kaiser tool includes ten categories of hazard, including: ‘biological terrorism; VIP situation; infant abduction; hostage situation and bomb threat’. FEMA also has a system (Homeland Security, 2013) which is based around the Threat and Hazard Identification and Risk Assessment (THIRA) process. This four step process comprises:

- Identify the Threats and Hazards of Concern.
- Give the Threats and Hazards Context.
- Establish Capability Targets.
- Apply the Results.

FEMA defines human-caused threats as including:

- Biological attack
- Chemical attack
- Cyber incident
- Explosives attack
- Radiological attack
- Sabotage
- School and workplace violence.

There are therefore a number of tools out there for the conducting of HVA in hospitals and other aspects of the Health CNI, however there are further considerations that may complicate their use.

3. Methodology

3.1 Research Approach

It was already established in D1.1 that the public domain information on Health as a part of the CNI of each MS was not extensive and therefore it would be challenging to provide synergies between the Health sector and other areas of CIP. However, the authors have attempted to identify methods and practices currently being used within some sectors that may be useful to developing risk management systems in hospitals and are portable to the Health sector.

As with the previous deliverable reports the scope of the research was limited to publicly available data written in English. This approach was adopted to ensure time and resource was managed across the whole project and optimized the research capability of the UK based English speaking team responsible for the delivery of WP1. Consideration was applied to the use of language translation services but the time required to first check the usefulness of documents prior to a full translation incurred a time delay that was not a workable solution in the case of this paper. The Italian and French speaking project partners were available to translate Italian and French documents when required. Issues relating to disclosure of sensitive information and other security issues to explain the paucity of available data remain extant.

3.2 Search terminology and methodology

An initial Internet search was conducted to identify a sample of utility and service providers operating in each of the 28 EU MS that were identifiable to the research team during the initial trawl. Once company names and business type had been identified, a list was drawn up to group companies, business type and EU MS. The plan was to identify three separate organisations per EU MS. Internet search engine Google was used throughout this phase because it was available, accessible and provided useable results. The companies were selected at random depending upon the search results, e.g. ‘water utility companies in...*insert EU MS’* would be used and the same search conducted using the same terminology but working through all 28 EU MS. The same type of search was conducted for electricity providers, gas providers and telecommunications providers. A decision was made during the early stages of the research to constrain the search to utilities and service providers because a short search of the financial sector yielded results that were very specific to market risks and other financial concerns, the risk management data made no reference to CIP or hazards and threats beyond the financial domain. The transport sector

provided some results that were constrained to the global transport network; some of the information is contained within this report, but additional detailed EU MS specific data was not identified. The primary aim of this paper was to identify useful synergies and information that would add value to the health sector and so the decision to discount the financial sector from the search was agreed. A similar process was conducted for governance. However it was agreed that all useable data had already been collected during D1.1 when the first deliverable report had attempted to identify the current situation of CIP throughout the EU. During D1.1 every EU MS government website had been visited by the THREATS team and useful data added to the findings chapter of the report.

Once three companies per MS had been identified a further detailed search was conducted for each company, initially each company website was visited to identify the availability of English language data. Some websites provided a search tool to look for specific documents and the research team would look for 'risk' and 'risk management' related data. In most cases the search terms identified Annual Reports as useful data and so the team included 'Annual Report' as part of the search terminology. On occasion the company website was not available in English or provided very little useful data so further internet wide searches were conducted using the same search terminology and including the company name e.g. 'Galp Energia risk management'. The results are contained in the table at appendix 1 to this report.

4. Findings

4.1 Risk management methodology

The report has not identified any specific synergies between risk management methods in the health sector and other sectors of CNI. But the research did identify risk management methods that are being used effectively to manage large and often networked organisations that are conducting complex and hazardous activity, such as gas and oil extraction. Some of the organisations analysed during the research use a very similar approach to managing risk, some have adopted an ERM approach whereby the risk management methodology is driven from the top but conducted at the operational level. There were subtle differences between organisations about how they monitor business activity across subsidiaries, but the risk committee featured as a critical management component to sit between the executive level and the operational level to translate information up and down the communication chain and ensure all discrete operations were linked at a Group management level.

4.2 Key findings

The key findings for risk management methods being used in other sectors of CIP were focused primarily on financial risk and maintaining a competitive edge within the sector. There was limited mention of maintaining support to CNI and supporting the national effort and organisations that did acknowledge responsibility were usually State owned organisations.

Statistical methods and mathematical simulations are complex and very reliant upon the type and accuracy of the information being applied to the parameters. They can be very accurate and have great utility, particularly in financial risk management where statistics and probabilities are much more reliable, the way they are applied in other sectors of CNI would potentially have limited utility in the health sector. However the research team can see the potential value with computer modelling from a crisis management perspective. With the availability of relevant data to inform the simulation parameters, the ability to predict the outcomes or impacts to a hospital in the event of a terrorist attack would be useful. This would mirror work being carried out in the crowd and event management industry whereby greater understanding and knowledge is now known about the way crowds behave and move under normal conditions and then during emergencies such as a fire in the building. The importance of understanding crowd dynamics should not be overlooked because the outcome of a terrorist attack at a hospital will depend upon the time of day it was carried out, such as early morning or during the middle of visiting time.

Risk management at hospitals is a common feature of the management approach but the review of the literature identified the focus to be upon patient standards of care and the protection of the hospital and staff from medical negligence. Most environmental hazards extended to natural disasters such as extreme weather events and earthquakes but seldom included terrorist attacks to the hospital facility.

Information relating to the findings of this research is contained within the table at appendix 1 of this report. A summary of those findings includes:

- Information on risk management was usually focussed on financial risk. This was likely to be for the benefit of potential investors.
- Security risks were rarely mentioned.
- Governance structures associated with risk management are covered but details relating to their methodology are rarely provided.
- Smaller companies rarely provide the detail of their approaches to risk management.
- Almost no mention of malicious threats except by organisations already highlighted in the literature review.
- Information relating to risk assessment methodology is far more available than vulnerability reduction information – this is likely to be due to sensitivities relating to the disclosure of sensitive information.
- Most risk information in this table is drawn from company annual reports.

5. Conclusions and Recommendations.

5.1 Assessing risk

Much of the data related to risk management in CNI is about risk assessment activity. Although risk assessments are an important facet of risk management, they are limited to identifying the risks and attempting to measure the impact of a specific event. In some cases when the risk rating is beyond the tolerable or acceptable level changes are made to try and reduce the rating and the additional measures or changes to the activity are recorded in the risk assessment document. This activity is important, though it is usually only conducted in detail at the operational level for a specific activity to fulfil health and safety and other duty of care compliances. However, vulnerability reduction is often overlooked as a complimenting activity to the risk assessment process. As part of the assessment of risk a system to inform a threat assessment, intelligence and information gathering processes must be in place. The methods identified in this report each have their merits and utility specific to the task but the Kaiser Permenente (2001) HVA provides a simple and logical method for assessing risk. The US Homeland Security (2013) THIRA method is a similar approach and may provide a useful example for establishing a common method in the EU. In relation to the assessment of the risk from terrorism effective systems must be established with national and local intelligence gathering organisations. This would require information and intelligence sharing and a system of protective security and protective marking would need to be established within the respective health care / hospital facility.

5.2 Threat assessment

By conducting a detailed threat assessment and measuring the likely impact to the hospital, using realistic parameters to gain an accurate result, will help to adjust security and risk management activity as the risk landscape changes. This means risk management strategies that form the operational security plan can be adjusted to respond to specific threats as they emerge, enabling the hospital to operate a threat level indicator, similar to the UK National level threat indicator (UK Government, 2015). Furthermore a threat assessment conducted by a suitable expert will help to reduce some of the uncertainty that is intertwined with risk and enable hospitals to manage the exposure to risk in a more practical and informed way. This approach will require more collaboration between government security agencies, in order to provide relevant and accurate information related to the current and emerging terrorist threat. That information does not need to contain sensitive information but useful detail that will enable hospital management teams to think about how they can prepare the hospital and staff to respond effectively to a low probability but potentially high impact event.

5.3 Security systems

Hospitals are supposed to be places of safety, where many patients and visitors at likely to be vulnerable because of personal circumstance. The THREATS team do not recommend that hospitals are 'locked down' and made to look and feel like a prison. But adaptive risk management methods can be adopted to ensure the risk management team are constantly monitoring the changing threat landscape and they have a series of useful tools to enable them to increase or decrease the protective measures in place.

Security systems and processes at hospitals should be designed to fulfil the critical elements of the THREATS critical pillars: physical protection of buildings and assets; security of people and protection of data and information. These critical pillars have been discussed in detail in D1.1 and referred to in D1.2 and 3. The combination of simple physical security measures that are supported by relevant processes or 'drills' can provide an effective layered security system, but the system needs to become part of the security culture and embraced and supported throughout the hospital community. This requires an investment by the management team to ensure all staff are informed, instructed and assessed on their specific role and responsibility, in a similar way that fire evacuation drills are managed. Without effective instruction and training, supported by an assessment and testing programme the system is vulnerable to failure because it will not have been embedded into the organisational culture or integrated into everyone's role and responsibility.

Examples of simple procedures that have not been identified during any of the research to date, but could easily be implemented in every hospital in the EU, are lock down procedures to respond to a 'roving threat' in the building. Many commercial buildings now use invacuation (move to a safe centralised place within the building close to your workstation), shelter in place (secure your immediate perimeter i.e. lock your office door and hide under your desk or somewhere suitable close by) and controlled evacuation procedures. Evacuation procedures now go far beyond getting out of a building as quickly as possible. Additional consideration is now given to the direction of the threat and therefore the most suitable route of escape. The building occupants need to understand what to do and when to do it so great thought is applied to training and testing the alarm and providing accurate and timely messages to building occupants via a public address system. Other considerations include staff training and how to protect patients, visitors and self, police and emergency services first response (what are the police likely to do in the first minutes following arrival at the hospital). This type of activity, advisory and training is undertaken regularly by the authors and research team for WP1 whom operate throughout the public and private sector and have comprehensive knowledge and experience that underpins this report.

5.4 Training

Training the staff to become more security aware and support the overall security culture will take time and effort but will be achievable if the project is embraced and supported from the top management down. Training can be included as part of staff training days, short training serials during less frenetic periods of the shift cycle and testing exercises to measure the effectiveness of the system and raise awareness. But managers must be aware of the cycle of activity required to maintain an operational capability: training – theory and practical based learning, on the job training to apply the knowledge in a real life setting, assessing – to measure the current capability and provide remedial or revision to adjust or improve practical ability, testing – to measure the effectiveness of the activity against a specific threat. Once the testing results provide evidence that the capability is at an acceptable level, the cycle begins again to sweep up new personnel and remind/revise current staff.

At the tactical and strategic level tabletop scenario based exercises are useful to provide an opportunity for management to run out the crisis management team (that may be a different team to the routine management team). These exercise opportunities enable the contingency or emergency plan to be tested against a set of planned objectives and can also provide interagency dynamics to be exercised before a real event occurs.

6. References

American Society for Healthcare Engineering (2000) *Hazard Vulnerability Analysis.* ASME. Available from: www.dp.ccalac.org/Policies/.../Hazard%20Vulnerability%20Analysis.pdf [Accessed 29 April 2015].

Cabinet Office (2015) *National Risk Register of Civil Emergencies.* London: TSO. Available from: https://www.gov.**uk**/.../uploads/.../**2015**0331_**2015**-NRR-WA_Final.pdf [Accessed 03 April 2015].

Cabinet Office (2010) *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*. London: TSO. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf [Accessed 03 April 2015].

Carroll, R. et al. (2014) Enterprise Risk Management: A Framework For Success. *American Society for Healthcare Risk Management.* Available from: www.ashrm.org/.../**white_papers**/**ERM**-**White**-**Paper**-**8**-**29**-**14**-**FINAL**.**pdf** [Accessed 29 April 2015].

COUNTERACT (2009) *Deliverable 3 PT4: GENERIC GUIDELINES FOR CONDUCTING RISK ASSESSMENT IN PUBLIC TRANSPORT NETWORKS FINAL REPORT 4.* Available from: http://www.transport-research.info/web/projects/project_details.cfm?id=36152 [Accessed 03 April 2015].

Council of the Baltic Sea States [n.d.] *Civil Protection Network* [online]. Available from: http://www.cbss.org/safe-secure/civil-protection-network/

E.ON. (2014) *2014 Annual Report.* Düsseldorf: Jung Produktion. Available from: http://www.eon.com/content/dam/eon-com/ueber-uns/publications/150312_EON_Annual_Report_2014_EN.pdf [Accessed 09 March 2015].

GAZPROM (2013) *Annual Report 2013: Unlocking the Planet's Potential.* Moscow: GAZPROM. Available from: http://www.gazprom.com/f/posts/60/660385/gazprom-annual-report-2013-en.pdf [Accessed 01 April 2015].

International Standards Organisation (2011) *ISO/IEC 20000-1:2011 Information technology – service management – Part1: service management system requirements* [online]. Available from: www.**iso**.org/**iso**/catalogue_detail?csnumber=51986

McNally, J. (2013) *The 2013 COSO Framework & SOX Compliance: One Approach To An Effective Transition*. Committee of Sponsoring Organizations of the Treadway Commission [online]. Available from: www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf

Merkel, W. and Castell-Exner, C. (2010) Managing risk under normal operation and in crisis situations. *Water Utility Management International.* **5** (3), 19-22. Available from: http://www.dvgw.de/fileadmin/dvgw/wasser/organisation/sicherheit/managingrisk_castell10.pdf [Accessed 01 April 2015].

Office of Rail Regulation (2015) *Common Safety Method for risk evaluation and assessment: Guidance on the application of Commission Regulation (EU) 402/2013.* London: ORR. Available from: http://orr.gov.uk/__data/assets/pdf_file/0006/3867/common_safety_method_guidance.pdf [Accessed 09 March 2015].

Rządowe Centrum Bezpieczeństwa. [*n.d.*] *Government Centre for Security* [online]. Available from: http://rcb.gov.pl/eng/?page_i d=210 [Accessed 27 March 2015].

Swedish Civil Contingencies Agency (2014) *Action Plan for the Protection of Vital Societal Functions and Critical Infrastructure.* Karlstad: MSB. Available from: https://www.msb.se/RibData /Filer/pdf/27412.pdf [Accessed 27 March 2015].

Water Services Corporation (2011) *WSC Annual Report 2011: Introduction.* Luqa: WSC. Available from: http://www.wsc.com.mt/sites/default/files/Annual_Report_2011_-_Introduction_1.pdf [Accessed 10 April 2015].

World Economic Forum (2012) *New Models for Addressing Supply Chain and Transport Risk.* Geneva: WEF. Available from: http://www3.weforum.org/docs/WEF_SCT_RRN_NewModelsAddressingSupplyChainTransportRisk_IndustryAgenda_2012.pdf [Accessed 09 March 2015].

Zigliani, C. *et al*. (2013) Design management for public services. *In: European House of Design Management: EHDM Milan workshop.* [s.l.]: EHDM. Available from: http://ehdm.eu/wp-content/uploads/2014/04/EHDM-Milan-Workshop.pdf [Accessed 01 April 2015].

Singh, B. and Ghatala, H. (2012) Risk Management in Hospitals. *International Journal of Innovation, Management and Technology.* **3** (4) 417-421. Available from: www.ijimt.org/papers/266-CM244.pdf [Accessed 03 March 2015].

UK Government (2015) *Terrorism and national emergencies* [online]. GOV.UK. Available from: https://www.gov.**uk**/terrorism-national-emergency/terrorism-**threat**-**levels** [Accessed 29 April 2015].

7. Bibliography

Charles River Associates. (2013) The State of Enterprise Risk Management for Power Companies. *In: NAPCO Conference.* Scottsdale:CRA. Available from: http://www.rmgfinancial.com/core/files/rmgfinancial/uploads/files/CRA_for_NAPCO_ERM_-Power Companies 1 17 2013(1).pdf [Accessed 03 March 2015].

Department of Energy & Climate Change. (2012) *Energy Security Strategy.* London:TSO

United Kingdom Health Protection Agency and partners (2011) *Safe Hospitals: Prepared for Emergencies and Disasters.* Disaster Risk Management for Health Fact Sheets: Global Platform – May 2011. PHE. Available from: www.who.int/hac/events/drm_fact_sheet_safe_**hospitals**.pdf [Accessed 17 April 2015].

Giannopoulos, G., Filippini, R. and Schimmer, M. (2012) Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. Luxembourg: European Union. Available from: http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf [Accessed 21 October 2014].

8. Appendices

8.1 Appendix 1 - Utility Company Risk Methodologies

Ser	Country	Company	Notes	Risk Methodologies
1	Austria	Verbund (electricity)	Company website: www.verbund.com State owned. 2010 revenue 3.3 billion Euros (Annual Report.2010: 3).	Emphasise a company-wide approach to risk management and have a separate strategic unit for coordinating processes (Verbund Risk Doc: p5). Use Monte Carlo Simulation method (Verbund Risk Doc: p5). Verbund risk document available from: http://www.verbund.com/cc/~/media/170D913A42A647D3B1418377FD970FF1 Use Accelus risk management software (Reuters) available from: http://accelus.thomsonreuters.com/sites/default/files/GRC01356.pdf
2	Austria	OMV (gas)	Company website: www.omv.com One of Austria's largest listed Company's (Annual Report 2014:8).	Hazards and event risks are centrally evaluated. Total risk is monitored by Monte Carlo Simulation and Risk Bearing Equity (Key Risks) available from: http://www.omv.com/SecurityServlet/secure?cid=1255758193266&lang=en&swa_id=1371394666575.7415&swa_site=wps.vp.com No mention of security risks on company website
3	Austria	Wabag (water)	Company website: www.wabag.com 2011 revenue $3.2 billion.	No available information.
4	Belgium	Electrabel (electricity, gas and nuclear). GDF Suez subsidiary	Company website: www.electrabel.com Belgian market share: 50% electricity and 46% gas (Facts and Figures.2013: p4).	No specific information of security risks. Other company facts and figures available from: https://www.electrabel.com/assets/be/corporate/documents/activity-report-2013_EN.pdf
5	Belgium	Sibelga (Electricity and gas)	Company website: www.sibelga.com 2012 revenue 302 million Euros (Rapport D'Activities).	No available information. Annual report 2012 available from: http://www.sibelga.be/uploads/assets/359/fr/1372929652763-Full-Rapport-annuel-Sibelga-2012.pdf
6	Belgium	Antwerp Water Works (water)	100 million Euro yearly revenue.	No available information.
7	Bulgaria	Bulgarian Energy Holding (electricity, gas and coal)	State owned. Company website: www.begnh.com	Other than a mention of risk management strategy, no details of methodology.
8	Bulgaria	Sofiyska Voda (water)	Company website: http://www.sofiyskavoda.bg/ Provides water to over 1.5 million people. 2013 Revenue 125 million BGN (Auditor's Report).	No available information. Auditor's report (2013) available from: http://www.sofiyskavoda.bg/BusinessDocuments%20English/Consolidated%20Fiancial%20statment%202013ENG.pdf

9	Bulgaria	Vivacom (telecommunications)	Company website: https://www.vivacom.bg/ Formerly state owned monopoly.	Accredited ISO IEC 20000-1:2011 'Information Security Management' (Profile). No other information available. Profile available from: https://www.vivacom.bg/en/about/about-us/company/who-we-are/company-profile
10	Croatia	Hrvatska Elektroprivreda - HEP (electricity and gas)	Company website: http://www.hep.hr/ 2013 operating income 7.7 billion HRK.	No available information.
11	Croatia	Jadransji Naftovod – Janaf (crude oil transportation)	Company website: www.janaf.hr	No available information.
12	Croatia	INA - Industrija Nafte (oil exploration, production, processing and distribution)	Company website: www.ina.hr/ 2013 revenue 3672 million HRK. Medium sized company (Annual Report, 2013:4).	No mention of how operational risk is mitigated. The 2013 annual report implies that a risk framework for subsidiaries is determined top down at the group level (p 45). Annual Report (2013) available from: http://www.ina.hr/UserDocsImages/eng_GI%20objava.pdf
13	Cyprus	Electricity Authority of Cyprus	Company website: https://www.eac.com.cy/ Revenue 907 million Euros.	No available information.
14	Cyprus	Petrolina (oil and gas distribution)	Webs Company website: http://www.petrolina.com.cy/	No available information in English.
15	Cyprus	Water Development Department (water)	Company website: http://www.cyprus.gov.cy/moa/wdd/WDD.nsf/index_en/index_en?OpenDocument	No available information on risk framework. Annual Report (2013) available from: http://www.cyprus.gov.cy/moa/WDD/WDD.nsf/All/0C2D1E1836A2F4FCC2257CE7002C8173/$file/Etisia_en_2013.pdf?OpenElement
16	Czech Republic	Ondeo Services Ceska Repulika (water)	Company website: http://www.ondeo.cz/en/ Suez Environment subsidiary.	No available information.
17	Czech Republic	CEZ (Gas)	Company website: www.cez.cz 2013 revenue 217 billion CZK (Annual Report, 2013:58)	Cez group has developed an integrated risk management system. This system is vetted and audited externally to ensure mechanisms comply with best practices, standards and legislation. An important risk management body is the Risk Management Committee that advises the board. Risk policies are determined at the board level. Risks in the form of specific threats or events are managed in a decentralised manner, with only the most significant reported centrally. Operational risk is quantitatively assessed (Annual Report, 2013:52-53). Annual report (2013) available from: http://www.cez.cz/edee/content/file/investors/2013-annual-report/vz2013aj.pdf
18	Czech Republic	EP Holding (coal mining, gas and electricity)	Company website: www.epenergy.cz 23.9 billion CZK revenue in 2012 (Annual Report, 2012:2).	Identifies malicious risks such as terrorism or cyber threats, but does not provide mitigations or risk management methodologies. Annual report (2012) available from: http://www.epenergy.cz/en/investors/reports/year2012/
19	Denmark	Dong Energy (electricity and gas)	Company website: http://www.dongenergy.com/en/ Denmark's largest energy company. State owned. 67 billion DKK revenue in	No information clearly published on company website but Google provided some details of Dong Energy's risk management structure. Risk is managed by a series of authorities that have policies centrally approved for implementation across individual business areas and subsidiaries (Risk Report). Available from: http://griuk.dongenergy.com/pdf/uk/28-29.pdf Annual report (2014) available from:

			2014 (Annual Report).	http://assets.dongenergy.com/DONGEnergyDocuments/com/Investor/Annual_Report/2014/dong_energy_annual_report_en.pdf
20	Denmark	Energinet (electricity and gas transmission operators)	Company website: www.energinet.dk	IT and information security listed as a priority in the organisation's strategic plan. Information security committee created to determine cyber security policy. To increase security Energinet have upgraded their SCADA systems for electricity, and will do the same for gas systems soon (Annual Report, 2014:14). The supervisory board has overall responsibility for risk management. The internal risk control system based on the committee of sponsoring operations (COSO) framework (Annual Report, 2014:35). Annual Report (2014) available from: http://www.energinet.dk/SiteCollectionDocuments/Engelske%20dokumenter/Om%20os/Annual-report-2014.pdf
21	Denmark	Danva (water)	Company website: http://www.danva.dk/	No available information in English.
22	Estonia	Eesti Energia (electricity, oil and gas)	Company website: https://www.energia.ee/ 2014 revenue 966 million Euros (Annual Report).	Risk analysis is based on simulation methods (Annual Report, 2014:66). Information on risk management structure (Annual Report, 2014:63). Annual report (2014) available from: https://www.energia.ee/-/doc/10187/pdf/concern/annual_report_2014_eng.pdf
23	Estonia	Tallinna Vesi (water)	Company website: www.tallinnavesi.ee 2013 revenue 53.1 million Euro (Annual Report, 2013:14).	Provides information on financial risk, but not security or operational risk. Annual Report (2013) available from: http://www.tallinnavesi.ee/images/stories/dokumendid/Investor/tv_ar_2013_eng.pdf
24	Estonia	Viru Keemia Grupp (shale, heat generation and electricity)	220.4 million Euro turnover in 2013 (Website Reporting)	No information provided of operational risk management. Reporting website: http://www.vkg.ee/eng/company/reporting/annual-report Annual report (2011) available from: http://www.vkg.ee/cms-data/upload/kontsern/vkg-aa-eng-2011.pdf
25	Finland	Helsingin Energia (electricity, heating and cooling	Company website: https://www.helen.fi/en/ 2014 revenue 8.2 billion Euros (Annual Report).	Risk is managed by bodies independent of operational business activities (Annual Report, 2014). Annual report (2014) available from: https://www.helen.fi/en/annual-report/annual-report-2014/year-2014/financial-statements/report-on-operations/
26	Finland	Vesilaitosyhdistys (water)	Company website: http://www.vvy.fi/ Two thirds of Finnish water is provided by local authorities and the remaining third by central government.	No information on risk was available online from any Finnish water companies.
27	Finland	Gasum	Company website: http://www.gasum.com/ 1.2 billion Euro revenue in 2013 (Annual Report, 2013:44).	No information provided of operational risk management. Annual Report (2013) available from: http://verkkojulkaisu.viivamedia.fi/data/gasumvuosikertomukset/2553/2553-lowres.pdf
28	France	E.on (electricity and gas)	Company website: www.eon.fr/	Technical and organisational measures to ensure information safety (Annual Report, 2014:61). Risks are categorised in terms of earnings impact: low (under €0.5 billion), intermediate (€0.5 to €1 billion), high (€1 to €5 billion), and very high (over €5 billion). Statistical methods, simulations and expert opinion are used to address risks (Annual Report, 2014:62). Monte Carlo

				Simulation used which factors in independencies between individual risks (Annual Report, 2014:68). No specific mention of malicious threats. Annual report (2014) available from: https://www.eon.fr/content/dam/eon-fr/fr/downloads/Rapports/EON_Annual_Report_2014_GB.pdf
29	France	Veolia Environment (water and energy)	Company website: www.veolia.com 22.3 billion Euro revenue in 2013 (Annual Results, 2013:2)	Veolia's Executive Committee meets three times per year through the risk committee, which is chaired by the General Secretary. This provides a direct link between Veolia's strategy and risk management process. Country specific committees were set up in 2013 to monitor and approve risk mapping at the national level (Governance Structure). Governance Structure available from: http://www.veolia.com/en/veolia-group/profile/governance/executive-committee Annual Results (2013) available from: http://www.veolia.com/sites/g/files/dvc181/f/assets/documents/2014/04/pr_20140227.pdf
30	France	Electricite de France (electricity)	Company website: france.edf.com 40.2 billion Euro turnover in 2014 (Annual Report, 2014:13).	No information provided on operational risk. Annual Report (2014) available from: http://shareholders-and-investors.edf.com/fichiers/fckeditor/Commun/Finance/Publications/Annee/2014/rapport_annuel/va/04_EDF2013_ra_full_va2.pdf
31	Germany	EnBW (electricity)	Company website: www.enbw.com EDF subsidiary	Integrated risk and opportunity management system based on COSO II framework (Annual Report, 2014:74). Central Risk Management and Internal Control System unit is responsible for developing methods and processes (Annual Report, 2014:75). List terrorism as a threat (Annual Report, 2014:74). Annual report (2014) available from:
32	Germany	Gelsenwasser (water)	Company website: www.gelsenwasser.de 1.2 billion Euro revenue in 2013 (Annual Financial Report, 2013:2).	Supervisor Board provides guidance on risk management to the Management Board (Annual Financial Report: p7). Annual Financial Reports (2013) available from: https://www.gelsenwasser.de/fileadmin/EN/unternehmen/annual_report_2013.pdf
33	Germany	RWE (gas)	Company website: www.rwe.com 6.4 billion Euro turnover in 2012. (Annual Report, 2012:1).	Overall responsibility for the group wide risk management system sits with the Executive Board. The Risk Management Committee is in charge of monitoring and refining the risk management system. It is composed of the heads of RWE departments, which are accountable for the entire Group. The Group Controlling Department, which sits below the Risk Management Committee, bears responsibility for the control, steering and co-ordination of the risk management system (Annual Report, 2012:88). Annual Report (2012) available from: http://www.rwe.com/web/cms/mediablob/en/1838516/data/1838296/11/rwe/investor-relations/agm/annual-general-meeting-2013/annual-report-2012/RWE-Annual-Report-2012.pdf
34	Greece	OTE (telecommunications)	Company website: www.ote.gr 4 billion Euro revenue in 2013 (Annual Report, 2013).	No specific information on security risk mitigation methods. Annual Report (2013) available from: https://www.ote.gr/documents/10280/30244/ANNUAL_REPORT_2013_ENGLISH.pdf/7c824279-de82-41ed-b904-84fb5990772d

35	Greece	Depa (gas)	Company website: www.depa.gr 1.6 billion Euro Revenue 2013 (Financial Report, 2013:6)	No specific information on security risk mitigation methods. Financial Report (2013) available from: http://www.depa.gr/uploads/files/29_09_2014/report_Eng.pdf
36	Greece	Athens Water Supply and Sewerage Company - EYDAP SA (water).	Company website: www.eydap.gr 353 million Euro revenue in 2013 (Annual Report and Annual Bulletin, 2013:39).	EYDAP has formed a comprehensive framework, strategy, policies and procedures for managing and monitoring the risks undertaken by the Company. For the effective application of those tasks, the responsible Division has access to all the activities of the Company and all data and information necessary for the fulfilment of its tasks (Annual Report and Annual Bulletin: p30). Annual Report and Annual Bulletin (2013) available from: https://www.eydap.gr/userfiles/Presentations/etisio_deltio_2013_en.pdf
37	Hungary	MVM Group (electricity)	Company website: www.mvm.hu 2014 Revenue 647 billion HUF.	Risk management code of practice has been integrated across the group, which uses a uniform methodology (Annual Report, 2014:22). Available from: http://www.mvm.hu/en/documentstore/Documents/mvm_group_annual_report_2010.pdf
38	Hungary	Vizmuvek – Budapest Water Works (water)	Company website: www.vizmuvek.hu 2012 Revenue 2.9 billion HUF (Annual Report, 2012:18).	No risk information available online. Annual Report (2012) available from: http://vizmuvek.hu/files/public/Fovarosi_vizmuvek/tarsasagi_informaciok/FVM_Eves_Jel_ENG.pdf
39	Hungary	MOL Group	Company website: www.molgroup.info 21 billion USD revenue in 2014 (Key Financial and Operating Data)	At the group level, risks are incorporated into a system arranged by Enterprise Risk Management (ERM). ERM integrates financial and operational risks along with a wide range of strategic risks, also taking into consideration compliance issues and potential reputation effects. Risks are assessed based on a unified methodology and collected into risk maps at different levels. Risk responses and controls are reviewed and mitigation actions set by top management (Annual Report, 2014:237). Annual Report (2014) available from: http://annualreport2014.mol.hu/en/downloads
40	Ireland	Irish Water (water)	Company website: www.water.ie National utility.	No available information.
41	Ireland	Bord Gais (electricity and gas)	Company website: www.bordgais.ie 505 million Euro revenue in 2013 (Annual Report and Financial Statements, 2013:1).	Risks are quantified centrally – the board is responsible for annually reviewing its risk management policy (Annual Report and Financial Statements: p16-17). No mention of security risks. Annual Report and Financial Statements (2013) available from: http://www.bordgais.ie/corporate/media/BGAR13AnnualReportFINAL07.141.pdf
42	Ireland	SSE (electricity and renewables)	Company website: www.sse.com	SSE operates an Enterprise Risk Management Framework (ERM) to ensure a consistent approach to risk across the organisation. Core responsibility for the identification and management of key risks is held at the business unit level, with overall 'top down' responsibility for the identification and assessment of SSE's principal risks, managed by the Executive Committee with regular updates given to the Board. A small, centralised team provides synchronisation between these processes; ensures alignment of SSE's strategy with risk management; engages with the business units; produces a consolidated analysis of total SSE risk exposure (Annual Report, 2014:24). Annual Report (2014) available from: http://sse.com/media/241200/2014AnnualReport.pdf
43	Italy	Enel (electricity and gas)	Company website: www.enel.com 2014 revenue 7.5 billion Euro (Board of	Specific risk management policies are developed for each category of risk. ENel have risk management committees at both the group and company level (Annual Report, 2014:100). Use statistical methods to assess risk in probabilistic and monetary terms (Annual Report, 2014:102). Mitigations are based on international best practices (Annual Report, 2014:103). Mentions the

			Directors Report).	threat of terrorism but gives no further detail (Annual Report, 2014:103). Available from: https://www.enel.com/en-GB/doc/report2013/bilancio_consolidato_enel_spa_2013_en.pdf Board of directors report available from: http://www.enel.com/eWCM/salastampa/comunicati_eng/1663454-1_PDF-1.pdf
44	Italy	ACEA (water and electricity)	Company website: www.acea.it 186 million Euro revenue in 2014 (Annual Report, 2014).	Analysis given of financial risk but not security risk. Annual Report (2014) available from: http://www.acea.it/GetMedia.aspx?lang=en&id=6bf69beac59840c7ac5dc1549817277b&s=0
45	Italy	Terna	Company website: www.terna.it 1.9 billion Euro in 2013 (Press Release).	External threats to operational risk is covered by specialist insurance cover. The Chief Risk Officer is responsible for supporting senior management in their handling of the Risk Management process at the Group level effectively, with respect to all financial, operational, business and other risks. Terna carries out this process by using the Enterprise Risk Management (ERM) methodology (Annual Report, 2013:70-73). Annual Report (2013) available from: http://www.terna.it/LinkClick.aspx?fileticket=ZTRli5mvMyw%3D&tabid=6315 Press Release available from: http://www.terna.it/default/home_en/the_company/press_room/press_releases/pr_2014/pr_march_2014/Terna_Board_of_directors_2013_results_approved.aspx
46	Latvia	Latvijas Gaze (gas)	Company website: www.lg.lv 2013 revenue 574 million Euro (Annual report)	No available information. Annual report (2013) available from: https://www.enel.com/en-GB/doc/report2013/bilancio_consolidato_enel_spa_2013_en.pdf
47	Latvia	Latvenergo (Electric)	Company website: www.latvenergo.lv State owned. 1.1 billion Euro revenue in 2013 (Press Release).	No available information on operational risk. Press Release available from: http://www.latvenergo.lv/eng/news/press_releases/5949-latvenergo-group-publishes-the-audited-annual-report-2013-the-group-profit-is-eur-46-million
48	Latvia	Rigas Uden (water)	Company website: www.rigasudens.lv 26.9 million LVL revenue in 2013 (Financial Report, 2013:1).	No available information. Financial Report (2013) available from: https://www.rigasudens.lv/about-company/annual-reports/en/
49	Lithuania	Lietuvos Energija (gas)	Company website: http://www.le.lt/en/ State controlled.	No available information.
50	Lithuania	Litgrid (transmission system operator)	Company website: www.litgrid.eu 616 billion LTL revenue in 2013 (Annual Report, 2013:26).	No information on the risk of malicious threats. Annual Report (2013) available from: http://www.litgrid.eu/index.php/news-events-/publications/annual-reports/2392
51	Lithuania	Vilniaus Vandenys (water)	Company website: http://www.vv.lt/	No available information.
52	Luxembourg	Service des Eaux (water)	Company website: http://www.vdl.lu/	No English text website.
53	Luxembourg	Enovos Luxembourg	Company website: www.enovos.eu	Risk management is integrated into every aspect of the organisation. Risk definitions, tools, methodologies and tolerance are decided centrally by the Risk Committee. Operative activity sits with middle offices (Annual Report, 2013:40).

		(electricity)		Annual Report (2013) available from: http://brochure.enovos.eu/enovos/rapport_annuel/2013/luxembourg/en/index.html#/40/zoomed
54	Luxembourg	Gas Natural Fenosa	Company website: www.gasnaturalfenosa.com 25 billion Euro sales revenue in 2013 (Annual Report, 2013:2).	Risk management functions are segregated at the operating level. Gas Natural Fenosa sets standards, procedures and systems for managing risk at the group level (Annual Report, 2013:83). Annual Report (2013) available from: http://www.gasnaturalfenosa.com/servlet/ficheros/1297141214998/GasNaturalFenosa_Consolidatedannualaccounts2013sininforme,0.pdf
55	Malta	Enemalta (electricity)	Company website: www.enemalta.com.mt	No available information. Annual report (2011) available from: http://www.enemalta.com.mt/enemaltastorage/images/files/annual%20reports/annual%20report%20and%20financial%20%20statements%2031%20dec%202011.pdf
56	Malta	Water Services Corporation (WSC) (water)	Company website: www.wsc.com.mt 70 million Euro – 2011 revenue (Annual Report, 2013:18).	Operational risk is managed in an integrated manner within WSC Management Systems, separate from financial risk that is managed by WSC Internal Audit Department. Management Systems reports directly to the CEO. WSC have a business continuity plan that is submitted to their regulators. Provides a list of operational risks. Malicious threats are absent (Annual Report, 2013:12-13). Annual Report (2011) available from: http://www.wsc.com.mt/sites/default/files/Annual_Report_2011_-_Introduction_1.pdf
57	Malta	Liquigas Malta (gas)	Company website: www.liquigasmalta.com/	No available information on risk.
58	Netherlands	Eneco (electricity and gas)	Company website: www.eneco.com 2014 revenue 4.6 billion Euro (Annual Report: p 6).	Sensitivity analyses, including single event stress tests and scenario analyses are used. Risk control systems specified for each level encompass specific mitigating measures. A 'heat chart' is used for internal communication with respect to risks (Annual Report, 2014:15). Annual report (2014) available from: http://www.eneco.com/about-us/finance/
59	Netherlands	Waternet (water)	Company website: www.waternet.nl	Waternet's website suggests that the company plans for an emergency together with municipal authorities, other water authorities and emergency services (Safety). Safety document available from: https://www.waternet.nl/about-waternet/water-and-us/safety/
60	Netherlands	Essent (gas, electricity and heat)	Company website: www.essent.nl Subsidiary of RWE.	For further details see Germany: RWE.
61	Poland	Polska Grupa Energetyczna (electricity)	Company website: http://www.gkpge.pl/ State owned.	No available information.
62	Poland	Tauron Group (energy and coal)	Company website: www.tauron-pe.com 2014 revenue 2 billion Euro revenue	Annual Report (2014:46) highlights financial risk, but does not cover operational risk. Annual Report (2014) available from: http://www.tauron-pe.com/tauron/investor-

			(Annual Report, 2014:1).	relations/Documents/Tauron_Standalone_annual_report_2014.PDF
63	Poland	Gaz System	Company website: www.gaz-system.pl/ 2.2 billion PLN net sales income in 2013 (Annual Report, 2013:10).	All the sources of information regarding relevant risks are integrated within the Enterprise Risk Management (ERM) process. Accredited with ISO 14001:2004 "Environmental Management Systems", ISO/IEC 27001:2005 "Information Safety Management System" and ISO 9001 "Quality Management Systems". Audit and corporate risk management functions are separated into a dedicated unit. Gaz systems are in the process of implementing ISO 22301 for business continuity (Annual Report, 2013:40-42). Annual Report (2013) available from: http://en.gaz-system.pl/fileadmin/centrum_prasowe/wydawnictwa/EN/GAZ-SYSTEM_annual_report_2013.pdf
64	Portugal	Galp Energia	Company website: http://www.galpenergia.com/ 18 billion Euro revenue in 2014 (website homepage).	Provide information on their risk management governance structures (Annual Report, 2014:50). Galp Energia's 2014 Annual Report illustrates the main risks the group faces and mitigations implemented to reduce their likelihood and impact. Terrorism and war are highlighted as risks but the only mitigation listed is continuous political risk analysis (p54). Annual report (2014) available from: http://www.galpenergia.com/EN/Investidor/Relatorios-e-resultados/relatorios-anuais/Paginas/ultimos-relatorios-anuais.aspx
65	Portugal	Aguas de Portugal (water)	Company website: www.adp.pt 791 million Euro revenue in 2012 (Annual Report, 2012:79).	Board of directors devote lots of attention to the group's risk. Aguas de Portugal has developed integrated assessments of the group's risks and systematised its risk management processes. Risk categorisation is based on the Committee of Sponsoring Organizations of the Treadway Commission (COSO) methodology. Integral and residual risk are taken into account. The Internal Auditing and Risk Control department operates with independence from the boards of companies within the group. Governance, strategy, planning, conformity and reporting are dealt with and monitored by each individual company. This approach to operational and infrastructure risks is complemented by centralised monitoring and control structures, with responsibility for identifying and managing the principal risks (Annual Report, 2012:56-57). Annual Report (2012) available from: http://www.adp.pt/files/1239.pdf
66	Portugal	Energias de Portugal (Electricity)	Company website: www.edp.pt 16.1 Billion Euro turnover in 2013 (Annual Report, 2013:173).	Specially dedicated department analyses risk at the group level. The Risk Management Department's main responsibility is to coordinate the Group's risk assessment studies, in order to assist the Executive Board of Directors in controlling and mitigating them, and providing integrated risk return (Annual report, 2013:111-136) Annual Report (2013) available from: http://www.edp.pt/en/Investidores/Resultados/2013/Annual%20Repot/2013%20Annual%20Report.pdf
67	Romania	Rompetrol (oil)	Company website: www.rompetrol.com Revenue in 2013 11.2 billion USD (Annual Report: p98).	No details of the management of malicious risks. Annual report (2013) available from: http://www.rompetrol.com/sites/default/files/raport-rpl-00015-revised-all-mobile.pdf
68	Romania	Apa Nova Bucuresti (water)	Company website: http://www.apanovabucuresti.ro/en/	No information available on risk.
69	Romania	Transelectrica	Company website: www.transelectrica.ro 2.4 billion LEU revenue in 2013 (Annual Report, 2013:29).	Does not provide details of how operational risks are managed. Annual Report (2013) available from: http://www.transelectrica.ro/documents/10179/114797/Raport+Anual+2013_EN.pdf/655a21a8-fafd-4f82-9c80-0ff5f9440350

70	Slovakia	Stredoslovenská Energetikav (electricity)	Company website: www.wwe.sk Second largest electricity company in Slovakia.	No information on security risk management. Annual report (2013) available from: http://www.sse.sk/portal/page/portal/stranka_SSE/spravy/zoznampdf/vyrocna_sprava_SSE_2013.pdf
71	Slovakia	Trencianska Vodohospodarska Spolocnost (water)	Company website: www.tvs.sk	No information available in English.
72	Slovakia	Slovenský Plynárenský Priemysel	Company website: www.spp.sk 1.9 billion Euro revenue in 2013 (Annual Report, 2013:26).	No information on operational risk management. Annual Report (2013) available from: http://www.spp.sk/en/all-segments/about-us/annual-reports/
73	Slovenia	Elektro-Slovenija (electricity)	Company website: http://www.elektro-energija.si/ State owned.	Risk is assessed centrally by the wider group, thus all subsidiaries use identical processes and criterion (Annual Report, 2013:39). Available from: http://www.elektro-energija.si/Portals/0/Content/dokumenti/letna-porocila/AnnualReport_ElektroeEnergija_2013.pdf
74	Slovenia	HSE (Electricity)	Company website: www.hse.si State owned. 1.6 billion Euro revenue in 2013 (Annual Report, 2013:107).	System of operating risk management established at the group level. The companies within the group have risk committees to identify risks and mitigation processes. A risk Controlling Manual has been developed for risk management across the group's companies (Annual Report, 2013:81-82). Annual Report (2013) available from: http://www.hse.si/en/files/default/letna-porocila/en/HSE2013-annual-report.pdf
75	Slovenia	Gen Energija (nuclear power)	Company website: www.gen-energija.si State owned. 608 million Euro revenue in 2013 (Annual Report, 2013:13).	A Risk Management Manual and Risk Management Guidelines were developed in 2013. Companies within the Gen group identify and determine the severity of risks posed. The Group manages operational risks through clearly defined business processes, clearly defined roles, responsibilities and competences, and codes of practice and rules (Annual Report, 2013:61-64). Annual Report (2013) available from: http://www.gen-energija.si/upload/katalogi/GEN_Annual_Report_2013.pdf
76	Spain	Iberdrola (electricity)	Company website: www.iberdrola.ec	Provides details of how they management business risks but not security risks (General Risk Control and Management Policy, 2015). Available from: https://www.iberdrola.es/webibd/gc/prod/en/doc/riesgos_control.pdf
77	Spain	Endesa (electricity and gas)	Company website: www.endesa.com 31.2 billion revenue in 2013 (Annual Report, 2013:18).	Information on financial risk management, but no detail of how operational risk is managed. Annual Report (2013) available from: http://www.endesa.com/EN/SALADEPRENSA/CENTRODOCUMENTAL/Informes%20Anuales/IA%202013%20ING.pdf
78	Spain	Canal de Isabel II Gestion (water)	Company website: www.canalgestion.es 1 billion Euro revenue in 2013 (Financial Statement, 2013:8).	No information about risk. Financial Statement (2013) available from: http://www.canalgestion.es/en/galeria_ficheros/comunicacion/documentacion/Estados_financieros/NIIF-UE__EEFF_CG_INGLES_061014.pdf Annual Report (2013) available from: http://www.canalgestion.es/es/galeria_ficheros/comunicacion/documentacion/USB_visibleII/CANAL_MEMORIAS/CANAL_UK_

				RES_2013.pdf
79	Sweden	Vattenfall (electricity)	Company website: www.coporate.vattenfall.com Fully state owned.	No information on security risk management.
80	Sweden	Svenska Kraftnat (electricity and gas)	Company website: www.wvk.se State owned. 923 million SEK turn over in 2012 (Annual Report, 2012:3).	Risk management is carried out in accordance with the national requirements made in the Ordinance on Internal Management and Control. 'Significant' risks are identified by the Board. The group's analysis of operational risks and threats are reported to the Swedish Cabinet Office and Civil Contingency Agency. Physical protection has been improved by better perimeter security. An investigation has been conducted to identify the parts of the national grid most vulnerable to sabotage. Camera surveillance has been installed to monitor facilities, and important elements are equipped with alarms. Identifies the likelihood of sabotage to be 'slight'. (Annual Report, 2012:16-17). Annual Report (2012) available from: http://www.svk.se/siteassets/om-oss/organisation/finansiell-information/annual_report_2012.pdf
81	Sweden	Malar Energi	Company website: http://www.malarenergi.se/	No information available in English.
82	United Kingdom	British Gas (energy)	Company website: http://www.centrica.com/index.asp?pageid=279	Business continuity plans for each aspect of the company (Risk Management). Available from: http://www.centrica.com/files/reports/2005cr/index.asp?pageid=7
83	United Kingdom	Scottish Power	Company website: www.scottishpower.com £8.2 billion revenue in 2013 (Annual Report, 2013:1).	The Board of Directors are responsible for establishing the *General Risk Control and Management Policy*, which identifies and monitors risks for companies within the group. As a consultative body, the Audit and Risk Supervision Committee, monitors and reports upon the appropriateness of the system for assessment and internal control of significant risks, acting in coordination with the audit and compliance committees existing at other companies of the Group. The country subholding companies are assigned the duty of specifying the application of the Specific Risk Policies of the Various Business of the Group, given the characteristics and particularities of each country (General Risk Control and Management Policy, 2015:3-4). Annual Report (2013) available from: http://www.scottishpower.com/userfiles/document_library/Consolidated_Report_&_Accounts_Scottish_Power_UK_plc_2013.pdf General Risk Control and Management Policy available from: https://www.iberdrola.es/webibd/gc/prod/en/doc/riesgos_control.pdf
84	United Kingdom	Welsh Water (water)	Company website: www.dwrcymru.com £736.5 million revenue in 2014 (Report and Accounts, 2014:87).	Each member of the leadership team maintains a detailed register of risks, reviewed monthly with their teams. The significant risks from each team are reported to and reviewed at one of the Executive meetings each month. These risks are then 'mapped' to the current Board Strategic Risks to ensure that there are no gaps and to give a view as to the current status of each risk, taking account of the effectiveness of mitigation steps in place. Audit Committee has accountability for overseeing the risk management processes and procedures, and reports to the Board. A detailed list of risk and mitigations is provided, but does not include risks from malicious threats (Report and Accounts, 2014:19-21). Report and Accounts (2014) available from: http://asp-gb.secure-zone.net/v2/1963/3110/9010/Glas-Cymru-Cyfyngedig-Report-and-Accounts-2014.pdf

8.2 Appendix 2 – Existing Risk Management Tools and Processes (World Economic Forum, 2012:21)

These are the existing tools and processes to support supply chain risk management, although predominantly focused at the operational level.

An awareness of the importance of circumscribing, measuring and managing risk is growing. In response a number of tools, processes and governmental and professional initiatives have been developed that aim to reduce the impact of disruptions on supply chain and transport networks.

Internal company tools	Cross-company tools	Professional bodies	Government bodies and initiatives
Track and trace tools	Supplier audit collaboration	Industry associations e.g. Retail Industry Leaders Association (RILA), International Air Transport Association (IATA)	Customs authorities
Risk mapping/ prioritisation	Standardised certifications (e.g. BSI development on supplier continuity planning)	Supply Chain Risk Leadership Council	WCO SAFE Framework and AEO
Business continuity planning	Disruption news feeds	Professional associations e.g. Chartered Institute of Logistics, Business Continuity Institute, Chartered Institute of Purchasing and Supply	Federal Emergency Management Agency
Scenario planning		Supply Chain Council and SCOR model	International Civil Aviation Organisation
Event management tools		ISO28000	Department of Homeland Security (US)
Centralised risk management unit/ personnel			UN Declaration of Human Rights/ Global Compact
Centralised/ standardised supplier assessments			Security initiatives e.g. C-TPAT
Supplier codes of conduct			EU/US competition law
Quantification metrics			World Food programme
Employee training initiatives			World Health Organisation
Supply chain mapping			Department of Trade and Industry initiatives
Business impact analysis tools			Authorised Economic Operator Programme
			PS-Prep Programme
			Environmental legislation

However, the sophistication and effectiveness of these tools are varied for the following reasons:

- Significantly different levels of adoption between companies – risk management initiatives are up to the individual company's discretion
- Mitigation tools and processes are often devised and/or applied on a local or regional basis, resulting in less globally cohesive risk management
- Minimal formal standardisation or certification exists in this area
- Laws and certification that do exist are often drawn up in isolation from industry insight, or are not integrated into company processes

(World Economic Forum, 2012:21)