Cloud Security Incident Reporting

Framework for reporting about major cloud security incidents

December 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors (or editors)

Dr. Marnix Dekker, Dimitra Liveri, Matina Lakka

Contact

For contacting the authors please use cloud.security@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

This work has been done in collaboration with Prof. Christopher Johnson, University of Glasgow.

Many thanks to the experts of the ENISA Cloud Security and Resilience EG (in no particular order): Frank van Dam (Ministry of Economic Affairs, NL), Arjan de Jong (Ministry of the Interior and Kingdom Relations, NL), Tuija Kuusisto (Ministry of Finance, FI), Jesper Laursen (Agency for Digitisation, DK), Steve Agius (MCA, MT), Vangelis Floros (GRNET, GR), Aleida Alcaide (SEAP, ES), Veaceslav Puşcaşu (e-Government Center, MD), Tobias Höllwarth (EuroCloud), Aljosa Pasic (Atos), Roxana Banica (RO), Fritz Bollmann (BSI, DE), Ali Rezaki (Tubitak, TR), Marko Ambroz (MJPA,SI), Putigny Herve (ANSSI, FR), Boggio Andrea (HP Enterprise Security), Tjabbe Bos (DG CONNECT, EC), Daniele Catteddu (CSA), Peter Dickman (Google, UK), Paul Costelloe (EuroCIO), Olivier Perrault (Orange, FR), Paul Davies (Verizon, UK), Raj Samani (McAfee), Jan Neutze (Microsoft, BE), Antonio Ramos (Leet Security)

ISBN 978-92-79-00077-5 doi:10.2788/14231

Executive summary

Cyber security incidents make the media headlines daily. A natural question for anyone to ask is "how often do cyber security incidents occur?", "what was their impact?", "what causes them?" But unfortunately, when it comes to security incidents we are usually navigating in the dark. Organisations often do not detect incidents when they happen and there is hardly any reporting about incidents to government authorities or the public. This makes it hard (for anyone) to understand which are the threats causing these incidents, what is the impact, etc. Without this information it is also hard to appreciate what is going well and what could be improved.

In 2013 the EU published a cyber-security strategy focusing on preventing large scale failures and attacks on network and information systems. A cornerstone of the cyber security strategy is the obligation for businesses providing critical services to report about security incidents. The strategy follows discussions in many countries about tighter regulation on cyber security issues – and particularly the lack of legislation, which obliges organizations to take appropriate security measures and to report about past incidents.

The proposed NIS Directive mentions cloud computing explicitly. This is not surprising. Cloud infrastructures play an increasingly important role in the digital society. A large part of the EU's Digital Agenda is the European cloud strategy which aims to speed up adoption of cloud computing for financial and economic benefits. ENISA has often underlined the security opportunities of cloud computing. Cloud computing is becoming the backbone of the EU's digital society. It is easy to see that certain cloud security incidents could have a major impact in society. In this paper we look at how incident reporting about cloud security incidents could be implemented in an effective and efficient way. It needs to be underlined that this document is not a guide on how to implement the Proposed NIS Directive but a first step towards studying how to implement incident reporting in cloud computing deployed services.

We asked a range of experts from industry and public sector to give their perspective on the issue of cloud security incident reporting. Which incidents should be reported, what should be reported, how we can use reporting to improve security. Some key issues which were raised:

- It is difficult to assess the criticality of the cloud services for a national regulator. There are many interdependencies, different layers of the cloud stack, different deployment models and different kind of data stored. A lot depends on the specific setting – and often the cloud computing customer is in the best position to judge the criticality and the potential impact of incidents.
- Cloud services are often based on other cloud services; they are distributed systems and built up in several layers. Incident reporting is different in these different layers.
- From the cloud customer's point of view, most standard contracts do not commit providers to reporting about security incidents to customers. Even though, some cloud providers do have dashboards where some incidents are published and explained.
- From the provider's side, it is up to the customer to include incident reporting obligations in contracts. For this reason, in many cloud contracts incident reporting is not addressed.
- Incident reporting is becoming more and more common in regulated sectors, like energy and finance where operators need to report incidents to regulators.
- Incident reporting should be part of a bi-directional flow of information where providers report about security incidents to authorities and authorities' feedback common threats and common issues to the cloud providers so they can improve security and resilience.

In this report we analyse how cloud providers, customers in critical sectors, and government authorities can set up cloud security incident reporting schemes, in four use case scenarios:

A. One cloud for one critical information infrastructure sector;
B. One cloud for multiple critical sectors;
C. One governmental cloud;
D. One widely used cloud.

Based on the feedback received from experts we present two schemes for cloud security incident reporting that cover those four cases. The parties involved are the cloud service provider (CSP), the cloud operator or customer, the national competent authority and the collaboration network.

We make several recommendations in this report. Summarizing them:

- We recommend customers in critical sectors to address incident reporting in their contracts and SLAs [recommendation 2]. We encourage setting the scope after conducting a national ICT infrastructure risk assessment [recommendation 1]. In a number of countries there are now legislative initiatives forcing operators in critical sectors [recommendation 3] to report about security incidents, and this means that these customers should include incident reporting in their contracts with cloud service providers.
- We recommend government authorities, which are responsible for governmental cloud programs or government IT to address incident reporting obligations in their security requirements [recommendation 4]. Incident reports provide a valuable crosscheck on the effectiveness of the security measures in place, and the security of the procured cloud services overall. Information sharing between all parties in a reporting framework [recommendation 5] will enhance knowledge on good practices in reporting cloud security incidents.
- We also encourage providers to discuss and agree on the scope [recommendation 6], start small and the authorities to encourage voluntary incident reporting schemes, because it is important that government and the public get information about common threats and the overall impact of security incidents in cloud computing [recommendation 7]. Incident reporting would also enable government authorities to better inform the private sector about threats and common root causes. Obviously there is a catch-22 here: If nobody shares incident reports, then nobody will benefit from sharing [recommendation 8]. Providers should jointly start with voluntary reporting schemes and engage with the government authorities about how incident reporting can help the providers to address problems.

ENISA has frequently highlighted the important security challenges of cloud computing. Some cloud service providers are leading the way in implementing state-of-the-art security measures. In cloud computing, using the economies of scale, a high-level of security becomes affordable also for small customers. We look forward to working with cloud providers and (public and private) customers to improve the transparency in cloud computing security by implementing efficient and effective incident reporting schemes across sectors and across the EU.

Table of Contents

1 Introduction

In the past every organisation would have its data and applications on their own servers. Some years ago most organisations have begun switching to outsource their applications and data to large datacentres, hosting providers and cloud providers. Commissioner Kroes, responsible for the implementation of the EU's Digital Agenda, has remarked that cloud services are becoming the backbone of our digital society. Public data about the uptake of cloud computing shows that in a short time the majority of organisations will be dependent on cloud computing. Large cloud providers will be serving tens of millions of end-users. Cloud computing services are increasingly playing an important role for society and the economy. The EU's cloud strategy, published in 2012, aims to speed up adoption of cloud computing for financial and economic benefits. ENISA has often underlined the security benefits of cloud computing. The Japanese government, for example, after the large earthquake of 2011, actively promoted cloud computing as a way to improve the resilience of information infrastructures to withstand natural disasters.

The increased dependency of society on cloud computing makes cloud computing also relevant from a national CIIP (Critical Information Infrastructure Protection) perspective. Cloud computing is, in a way, a double-edged sword: On the one hand, cloud computing offers important benefits in terms of information security and resilience, for example in the face of DDoS attacks. On the other hand, the concentration of IT resources in a few large datacentres implies that failures or cyber-attacks could have a large impact on society and the economy.

The 2009 CIIP action plan already calls for discussions on a governance strategy for cloud computing. The EC's 2013 Cyber security strategy focuses on preventing large scale failures of, and large scale attacks on, network and information systems in the EU. The strategy explicitly includes cloud computing services in scope. It is widely acknowledged that the current lack of transparency about network and information security incidents complicates efforts by government authorities and industry to increase the resilience of our critical information infrastructures. A cornerstone of the EU's cyber security strategy is to extend incident reporting obligations to other critical information infrastructures, besides the telecom sector[1].

In this report we take a CIIP perspective on cloud computing. We analyse how reporting about significant Network and Information Security (NIS) incidents could be implemented for cloud computing services.

Goal

The benefits of incident reporting are well known and widely supported: information sharing, the dissemination of lessons learnt and experience exchange, identification of route causes and mitigation techniques, data and trend analysis are some of the most important advantages of a large scale reporting scheme.

The goal of this report is to provide government authorities (ministries, regulators, cyber security agencies) with an overview of issues and challenges when implementing (national and pan-European) schemes for reporting about significant security incidents in cloud computing.

We also provide government authorities with guidance on the first steps that could be taken to implement voluntary reporting schemes.

[1] In the electronic communications sector the reform of Framework directive introduced obligations for providers to assess risks, to take appropriate security measures and to report about significant incidents. These provisions have now been implemented across the EU.

This document is not a guide on how to implement the Proposed NIS Directive but how to implement incident reporting in cloud computing deployed services.

Target audience

This report is targeted at:

- government authorities in the EU (ministries, regulators, cyber security agencies, et cetera), who are involved with the protection of critical information infrastructures and/or the supervision of IT e-government services, electronic communication services, large data centres, IT used in critical sectors, etc.
- operators of critical infrastructure who consider using cloud computing to support their core services, cloud providers with customers in critical sectors or performing vital functions, and cloud providers who play a critical role in the digital society.

Scope

In this report we take a CIIP perspective on cloud computing. We focus on reporting network and information security incidents involving cloud computing services.

We do not address all kinds of cloud computing services, but we restrict ourselves to those cloud computing services[2], which when failing or attacked, could have a major impact on the society or the economy. This mirrors the scope of the CIIP action plan and the EU's cyber security strategy, focussing on:

- Cloud services which are used by operators of critical infrastructures (transport, energy, et cetera) to support their core services.
- Cloud services which are by themselves critical, being key enablers of services in the digital society.

This means we look at public cloud services, which anyone can subscribe to, as well as private and community clouds, which are dedicated for one customer or a community of customers. Also we look at supply chain management, including cloud services which are directly or indirectly used by operators.

This report does not address personal data or personal data protection[3] in detail – although some security incidents could well have an impact on personal data. From a CIIP perspective the focus is on incidents with a significant impact on the society and the economy, while from a data protection perspective the focus is on the impact to the individual. Also, while cloud users may have their own individual end users (i.e. employees or customers using the service procured) we primarily focus on the cloud user's relationship with its cloud provider.

[2] Cloud computing definition by the National Institution of Standards and Technology (NIST) : Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[3] Note that under data protection legislation even very small incidents have to be reported to data protection authorities, while CIIP legislation specifically focusses only on large failures and large attacks, which could have a major impact on the society or economy.

Methodology

The recommendations and guidance in this report were developed in cooperation with an expert working group including representatives of the stakeholders mentioned in previous paragraphs, major cloud service providers, government agencies, industry association, and the customers of cloud services, both in the public and in the private sector. Their input was collected using an on-line survey and a series of more open-ended interviews. The intention was to identify their views, best practices in incident reporting, both in Europe and abroad, with a particular focus on Critical Information Infrastructures.

Structure

This document is structured as follows:

- In Section 2 we introduce the notion of cloud security incidents, first by defining the cloud computing model and introducing different types of cloud services;
- In Section 3 we give an overview of the related legislative initiatives, summarizing the EU's CIIP directive, Article 13a of the electronic communications framework, and Article 14 of the proposed NIS directive; all the activities the community is taking towards a common framework for reporting incidents and improve network resilience across the EU.
- In Section 4 we explain and give examples of cloud security incidents to focus on their criticality for the citizens.
- In Section 5 we summarize the views and perspectives of the experts in the ENISA expert group on the specific topic and more specifically, to report the technical details of cloud security incident reporting.
- In Section 6 we list the challenges when reporting cloud security incident by elaborating on four (4) use cases.
- In Section 7 we conclude with a set of high level recommendations for national authorities.

2 Definitions: Cloud computing services

This section introduces cloud computing services model and explains most "incident related" terms that will be used throughout this report.

2.1 Cloud computing services model

NIST developed a reference architecture for cloud computing, explaining the different existing types of cloud computing and all the actors and processes involved[4]. Different types of cloud services, each involve different types of technology and assets. We give an overview below – see Figure 1.

- **Infrastructure as a Service**: In IaaS the provider delivers storage (virtual databases) or computing resources (virtual hardware), via the internet. Examples include Amazon's Elastic Compute Cloud, Google's Compute Engine, Amazon Simple Storage Service, Google Cloud Storage, Microsoft Windows Azure Storage, Rackspace, et cetera. Customers start and stop virtual machines, or they store or access data.
- **Platform as a Service**: In PaaS, the provider delivers a platform for customers to run applications on (typically web applications). Often PaaS providers supply software development tools to construct applications for the platform. Typical types of applications that run on these platforms are scripts (PHP, Python, e.g.) or byte code (Java servlets, C#). Examples include Google App engine, Microsoft Azure, Amazon Elastic Beanstalk, et cetera.
- **Software as a Service**: In SaaS, the provider delivers fully-fledged software or applications, via the Internet. Applications range from email servers, email clients, document editors, or customer relationship management systems. SaaS services can often be accessed with a browser or a web services client.
- **Facilities**: Facilities are the basic IT resources which underlies all types of cloud services (IaaS, PaaS, and SaaS), network, housing, cooling, power.
- **Organisation**: Organisation is the human resources, the processes and the policies and procedures that maintain the facilities and support the delivery of services.

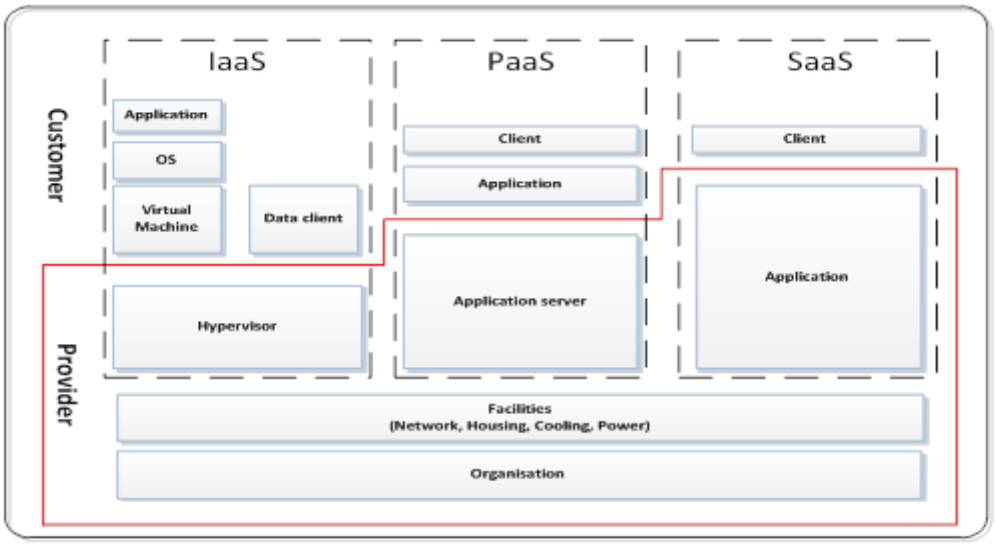

Figure 1 Map of different technologies across different types of cloud services

[4] http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

Note that some providers only offer IaaS or PaaS services, some providers only offer SaaS. SaaS providers often run their applications on IaaS or PaaS infrastructures.

2.2 Definitions

In this section we give definitions[5] of terms that are widely used across this report:

- **Incident**: A breach of security or a loss of integrity that has impact on the operation of network and information system core services, which public administrations and market operators provide. The "reportable incident" is the one that has deemed significant impact.
- **Incident Reporting**: The procedure by which the reporting party (cloud provider or cloud operator) shall submit to the national competent authority a report with information on the incident, on ad-hoc basis.
- **Impact:** A measure reflecting the average number of affected parameters/assets per incident, to show
- **Root cause:** The reason that caused the incident.
- **Parameters:** the criteria to be used to measure impact of an incident.
- **Thresholds:** The specific values of the parameters that when overpassed, the impact of the incident is deemed significant and the incident falls into the incident reporting scope.
- **Early warning:** The procedure based on which the dissemination of information on incident is done in a fast way to the interested companies to alert them of an on-going attack or other incident, so that immediate action could be taken.
- **Threat:** A threat is an event or a circumstance which could cause a security incident.

[5] The definitions are based on the Technical Guideline on Incident Reporting adopted for cloud computing incident reporting: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting/technical-guideline-on-incident-reporting

3 Background: Policy context

In this section we summarize relevant EU policy and legislative initiatives on CIIP and security incident reporting.

3.1 EC Communications on CIIP

The Communication on Critical Information Infrastructure Protection (CIIP) issued by the EC in 2009 aimed to improve preparedness, security and resilience, with the goal to protect Europe from large scale cyber-attacks and failures. The motivation for this communication was that Information and Communication Technology (ICT) is increasingly intertwined in our daily activities, and that some ICT infrastructures form a vital part of the European economy and society, either because they provide essential services (such as emergency communications) or because they underpin other critical infrastructures. ENISA is responsible for a range of activities mentioned in the CIIP action plan.

The CIIP communication defines Critical Information Infrastructures (CIIs)[6] as all ICT systems which are either,

a) critical infrastructure themselves, or;
b) essential for the operation of other critical infrastructures.

This builds on the definition of critical infrastructures in COM(2005) 576; "*Critical infrastructures include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments".*

COM(2011) 163 notes that: "*It is essential to strengthen discussions on the best governance strategies for emerging technologies with a global impact, such as cloud computing. These discussions should certainly include, but not be limited to, the appropriate governance framework for the protection of personal data. Trust is essential in order to reap its full benefits*".

In its Conclusions on CIIP of 27 May 2011, the Council of the European Union stressed the pressing need to make ICT systems and networks resilient and secure to all possible disruptions, whether accidental or intentional; to develop across the Union a high level of preparedness, security and resilience capabilities and to upgrade technical competences to help Europe face the challenge of network and information infrastructure protection; and to foster Member States' cooperation by developing incident cooperation mechanisms between them.

Two Ministerial Conferences on CIIP took place respectively in Tallinn in 2009 and in Balatonfüred in 2011. Tallinn started the debate on the general direction of the European efforts towards an increased network and information security for the future. Balatonfüred provided a forum to take stock of progress, assess lessons learnt and discuss the challenges ahead and next steps. It also investigated the way forward to engaging all stakeholders and in particular the private sector.

In 2011, the EC took stock of the results achieved so far and indicated future steps. The CIIP communication emphasises the need to identify best governance strategies for cloud computing, and that these discussions should include, but not be limited to the protection of personal data.

The European Parliament Resolution of 12 June 2012 on "Critical Information Infrastructure Protection: towards global cyber-security" broadly endorsed the 2011 Communication and made recommendations to the Commission for the way forward. Many of these recommendations have

[6] The OECD defines CII as those information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy. Both definitions are equivalent.

been taken on board in the Cyber security strategy and proposal for a Directive on network and information security published in 2013.

3.2 Article 13a of the Framework directive

The reform of the EU legal framework for electronic communications, which was adopted in 2009 and was transposed by most EU countries around May 2011, adds Article 13a to the Framework Directive (2009/140/EC). Article 13a addresses the security and integrity[7] of public electronic communications networks and services. The legislation concerns national regulatory authorities (NRAs) and providers of public electronic communications networks and services[8]. It has three main provisions:

- NRAs must ensure that e-Comms providers take appropriate steps to guarantee the security and resilience of electronic communication networks and services.
- Providers of electronic communication networks and services must report significant incidents to competent authorities (NRAs)
- NRAs must provide a summary of significant incidents to ENISA and the EC.

In other words, Article 13a asks EU Member States to set up a reporting scheme for significant incidents. The actors and information flows in Article 13a are depicted in Figure 6.

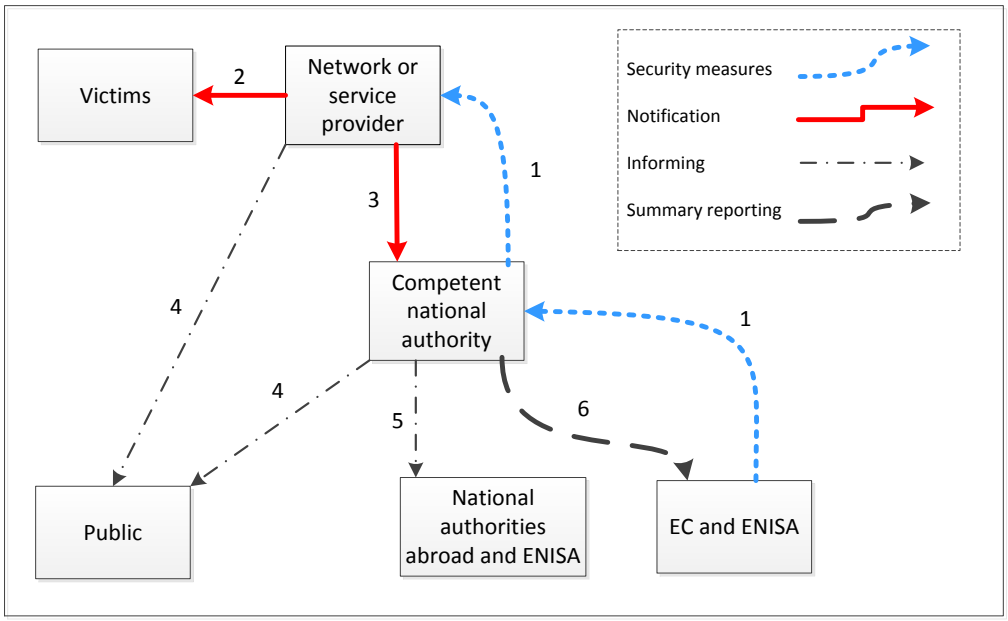

Figure 2 Actors and information flows in Article 13a

Article 13a of the Framework directive, together with Article 4 of the e-Privacy directive, are currently the only EU directives that oblige providers to report security incidents. Both directives are limited to electronic communications networks and services. Article 15 of the draft regulation on electronic identification and trust services for electronic transactions, requires that trust service providers have to undertake extensive security measures and notify competent bodies of any breach

[7] Here integrity means network integrity, which is often called availability or continuity in information security literature.
[8] *More information on Article13a can be found here: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting*

of security and loss of integrity with significant impact on the trust service provided and on personal data maintained therein.

3.3 Proposal for a Network and Information Security (NIS) Directive

In 2013 the European Commission communicated its Cyber Security Strategy and proposed a European Network and Information Security Directive. The key motivation for the directive was that several member states are taking action to improve cyber security, but there is no common and consistent approach across the EU. The NIS directive was proposed to ensure a level playing field for businesses across the EU and to avoid a weakest link[9].

The main pillars of the proposed NIS directive include: (1) the implementation of national NIS strategies and the national NIS cooperation plans, (2) the enforcement of CERTs, (3) the cooperation between competent authorities and (4) the enhancement of security of the NIS systems of public administrations and market operators. These will need to be implemented by Member States.

One of the main goals of the proposed NIS directive is to extend Article 13a of the Framework directive beyond the electronic communications sector, to cover other critical information infrastructures: Article14 of the proposed NIS Directive.

The scope of Article14 of the proposed NIS directive applies to government administrations and 'market operators':

(a) providers of information society services which enable the provision of other information society services
(b) operators of critical infrastructure which is essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health.

The legal text of Article 14 can be (graphically) summarized as follows.

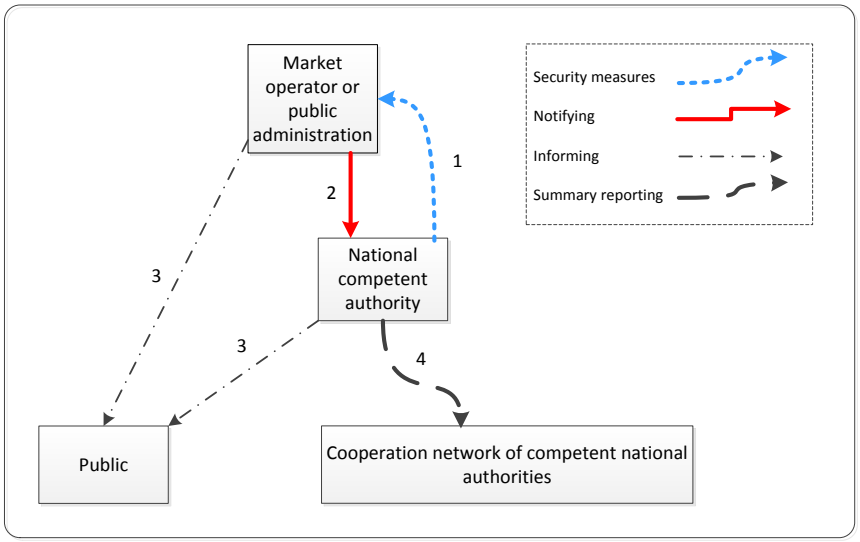

Figure 3 Information flows and actors described in Article 14

[9] The DIginotar incident underscores how an incident in one country can have an impact across the border.

The main provisions of Article14 are:

1. (blue dotted arrow) National competent authorities should ensure that public administrations and market operators take appropriate technical and organisational security measures to protect network and information systems underpinning their core services[10].
2. (red arrow) When a significant security incident occurs, the public administrator or market operator should notify the competent authority.
3. (black dash-dotted arrow) Depending on the circumstance, the competent authority might inform the public or require the market operator to do so.
4. (black dashed arrow) Annually, the competent authority should send summary reports about the incidents to the cooperation network, which includes all competent authorities across the EU.

The cooperation network should discuss about past incidents, lessons learnt, ex-post, common issues, et cetera, and agrees on a common, harmonized approach.

[10] Article 15 of the NIS Directive ("Implementation and enforcement") gives competent authorities the power to request market operators to do a self-assessment, to undergo an audit, and/or to investigate cases of non-compliance.

4 Critical cloud computing

In some settings cloud computing services can be critical. We distinguish two cases:

- Case 1: Cloud computing services which are used by operators of critical infrastructure to support the delivery of their core services, in cases where the reliability of the underlying cloud technology is itself essential to the safe functioning of the critical service.
- Case 2: Cloud computing services which are critical in themselves, i.e. if failing there would be a significant impact on health safety, security or economic well-being of EU citizens or the effective functioning EU governments.

In this section we give specific examples of settings where cloud computing services are critical.

Note that we mention names of specific customers, specific providers and specific services, but they are intended as examples. We do not intend to single out specific organisations or specific services for criticism or praise.

4.1 Cloud services which underpin critical infrastructure

Cloud services are increasingly being used in critical sectors. Below we give some example from the finance, transport and health sector[11]:

- The Air Traffic Managements solutions for the Singe European Sky (SESAR) aims at developing the new generation air traffic management system capable of ensuring the safety and fluidity of air transport worldwide over the next 30 years. SESAR is funding a project on a secure Cloud for Air Traffic Management.[12]
- In the US, the FAA released their cloud computing strategy and announced a $91 million contract for Computer Sciences Corporation (CSC) and Microsoft to create a cloud email system for the agency. The agency also announced the transition of their air traffic management systems onto cloud networks in the future.
- NASDAQ OMX FinQloud is a cloud computing platform, which runs on Amazon Web Services, to monitor compliance requirements (execution compliance and surveillance systems) for high frequency trading operators[13].
- A Slovenia-based railway operator has selected a cloud-based platform to centralize passenger, freight and logistics information systems across its rail network[14].
- A big oil company adopted a private cloud model for preproduction systems, testing environment and data processing – 60% of the company's infrastructure is virtual[15].
- Another major oil company in the United States adopted PaaS to collect and process information for early warning systems[16].
- In Luxembourg the government has issues guidelines on how to implement cloud in the finance sector. The new law enriches the Luxembourg legal framework of the cloud computing and the service industry in general.[17]

[11] Directive Annex II, critical sectors: Energy, Transport, Banking, Financial market, Health sector.
[12] http://www.sesarju.eu/programme/workpackages/wpe/research-projects-results-second-call-1304
[13] http://aws.amazon.com/solutions/case-studies/nasdaq-finqloud/
[14] http://blog.executivebiz.com/2013/08/ibm-to-help-intl-rail-operator-install-cloud-it-system-roman-koritnik-comments/
[15] http://www.computerworld.com/s/article/9225827/Shell_Oil_targets_hybrid_cloud_as_fix_for_energy_saving_agile_IT?taxonomyId=158&pageNumber=2
[16] http://www.spgindia.org/spg_2012/spgp160.pdf
[17] http://www.newsletter-nautadutilh.com/EN/xzine/information_-_communication_technology/luxembourg_le_droit_de_revendiquer_ses_donn%C3%A9es%20aupr%C3%A8s_dun_fournisseur_de_solutio

There have been incidents affecting cloud services, which impacted critical infrastructure. We give some examples below:

- In 2011, Finish IT operator Tieto faced an incident for (in some cases) several weeks, affecting 50 of the company customers in both private and public sectors. The impact was felt across Sweden[18]. Some customers suffered minimal effects over a number of days; others lost their IT services for several weeks. The causes were traced back to hardware failures. This incident had an immediate effect to the citizens, since the IT system was supporting for the process of provisioning drugs to patients all over the country.
- In 2013, the NASDAQ OMX crashed for three hours, with a major financial impact on brokers. The problem was traced to a connectivity issue between an exchange participant and the industry processor, which meant the system, was unable to disseminate consolidated quotes and trades[19].

4.2 Cloud services which underpin the digital society

Cloud computing services have become critical for the digital society as a whole, even if they are not directly supporting critical infrastructures. Some cloud services which are used by many citizens in everyday life or by many companies. In these cases major security incidents could have a large impact in society.

We give some examples of outages:

- August 2013, Amazon Web Services suffers an outage, taking down Vine, Instagram and other applications for an hour. This outage shows that no proper redundancy policy is applied correctly.[20].
- March 2013, Microsoft's email infrastructures suffered a loss of availability for nearly 16 hours affecting business critical services. The causes stemmed from a faulty software update. The number of users affected has not been disclosed[21].
- January 2013, Dropbox suffered a substantial loss of service for more than 15 hours affecting all users across the globe[22].
- October 2011, millions of Blackberry users across Europe, Middle East and Africa suffered an outage lasting three days. The company has about 70m users around the world. Speculation is that most of the global customer base may have been affected at some point during this time.

For providers it is difficult to estimate the number of end-users or organizations affected by an incident, especially when they affect IaaS/PaaS. It is also hard to assess the number of end-users and organisations depending on a cloud computing service. One reason is that knock-on effects can create cascading failures when IaaS/PaaS providers offer services to other organizations, which in turn provide services to third parties. This long supply chain makes it difficult to measure the impact of incidents or the criticality of a service in terms of the number of end-users, because the number of end-users cannot be easily estimated by the service provider.

---

ns_cloud_failli/luxembourg_the_right_to_claim_back_data_from_bankrupt_cloud_computing_providers/luxembourg_the_right_to_claim_back_data_from_bankrupt_cloud_computing_providers.html?cid=4&xzine_id=4945&aid=14382

[18] https://www.msb.se/RibData/Filer/pdf/26170.pdf

[19] http://www.bankingtech.com/161382/nasdaq-omx-connectivity-disaster-highlights-stumbling-markets/

[20] http://www.businessweek.com/articles/2013-08-26/another-amazon-outage-exposes-the-clouds-dark-lining

[21] https://www.crn.com/news/cloud/240150826/microsoft-cloud-outage-blamed-on-faulty-update.htm

[22] http://www.crn.com/slide-shows/channel-programs/240146101/5-companies-that-dropped-the-ball.htm?pgno=5

5 Perspectives on Cloud Security Incident reporting

To gain a better understanding of the views and perspectives of experts on the topic of cloud security incident reporting we conducted an online survey and several interviews with experts from industry, industry associations, government, and academia. In this section we show and analyse the responses from the survey and we discuss the highlights from the interview by including quotes from experts which are representative.

5.1 Results from survey and interviews

5.1.1 Participants and respondents

In total we conducted 15 interviews and 25 questionnaires. Figure 8 provides an overview of the different participants in the interviews and their roles respectively.

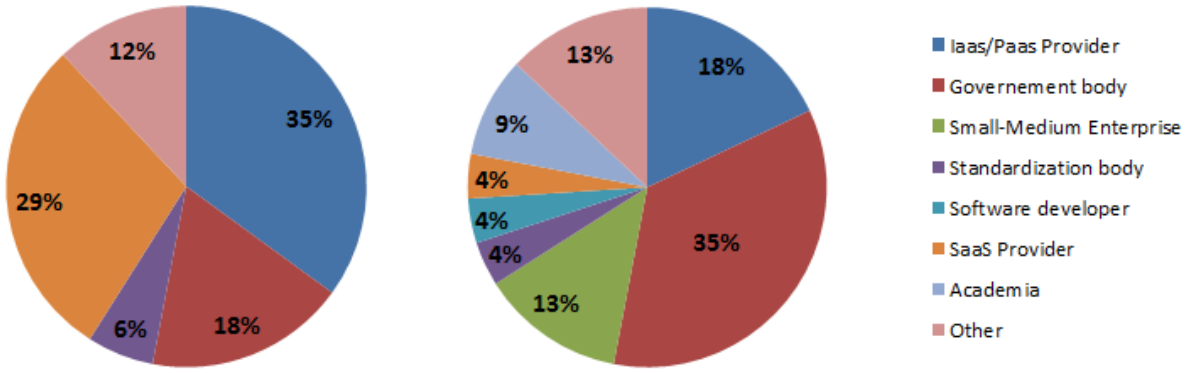

Figure 4 Overview of stakeholders participating in the Interviews and Survey

Some of the topics we included in this collection of information are:

- Incentives for reporting;
- Compulsory vs Voluntary reporting;
- Services in scope of reporting outages;
- Sectors in scope of reporting outages;
- Incidents in scope of reporting;
- Parameters to be used to measure the impact of an outage;
- Cross border incidents.

5.1.2 Services in scope

In the survey we asked participants which type of services should be in scope. Figure 9 shows the results of the survey. It shows that most respondents believe priority should be given to services that support critical information infrastructure (SaaS, IaaS and PaaS). Secondly, providers should report about incidents affecting services with large numbers of end-users or/and customers and thirdly incidents affecting services with a wide geographic spread (entire country or cross border) should be reported.

Note that respondents disagree about whether or not public or private clouds should be in scope. Half of the respondents say public clouds should not be in scope, half of the respondents say private clouds should not be in scope.

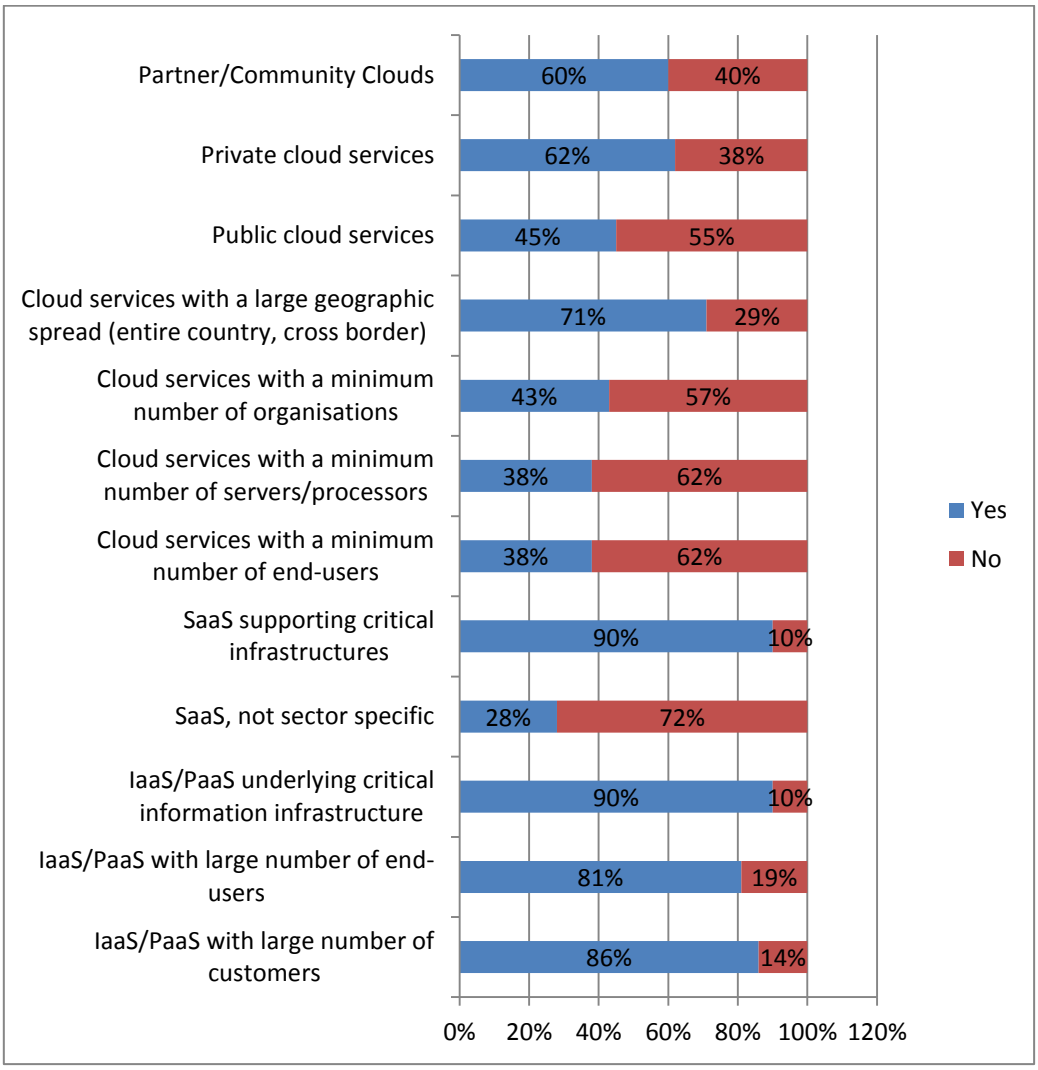

Figure 5 Services in scope

When discussing this topic in interviews experts reiterated the difficulty of making clear distinctions between IaaS, SaaS, PaaS, public and private clouds. Every cloud provider has developed their own platforms and different types of cloud resources are used in different settings:

"The distinctions between different IaaS, SaaS and PaaS architectures are less important than the impact on people. This creates problems because we, infrastructure companies, don't always know the impact of an outage on users with less tangible aspects such as trust which are key to the future development of the industry across Europe."

5.1.3 Sectors in scope

In the survey we asked respondents which incidents should be in scope. From the answers it becomes clear that incidents affecting the email services of an oil and gas company should not be in scope of reporting, unless there is an impact on core business processes (i.e. if the loss of oil and/or gas supply). Figure 10 shows the answers in more detail.

When discussing with experts in which sectors incident reporting should be mandatory, it was often mentioned that cloud computing is almost becoming a critical sector in itself. In fact, many experts currently sustain that cloud computing is becoming the backbone of the digital society:

"Cloud services are themselves part of the critical infrastructure that supports many companies in our country and across Europe."

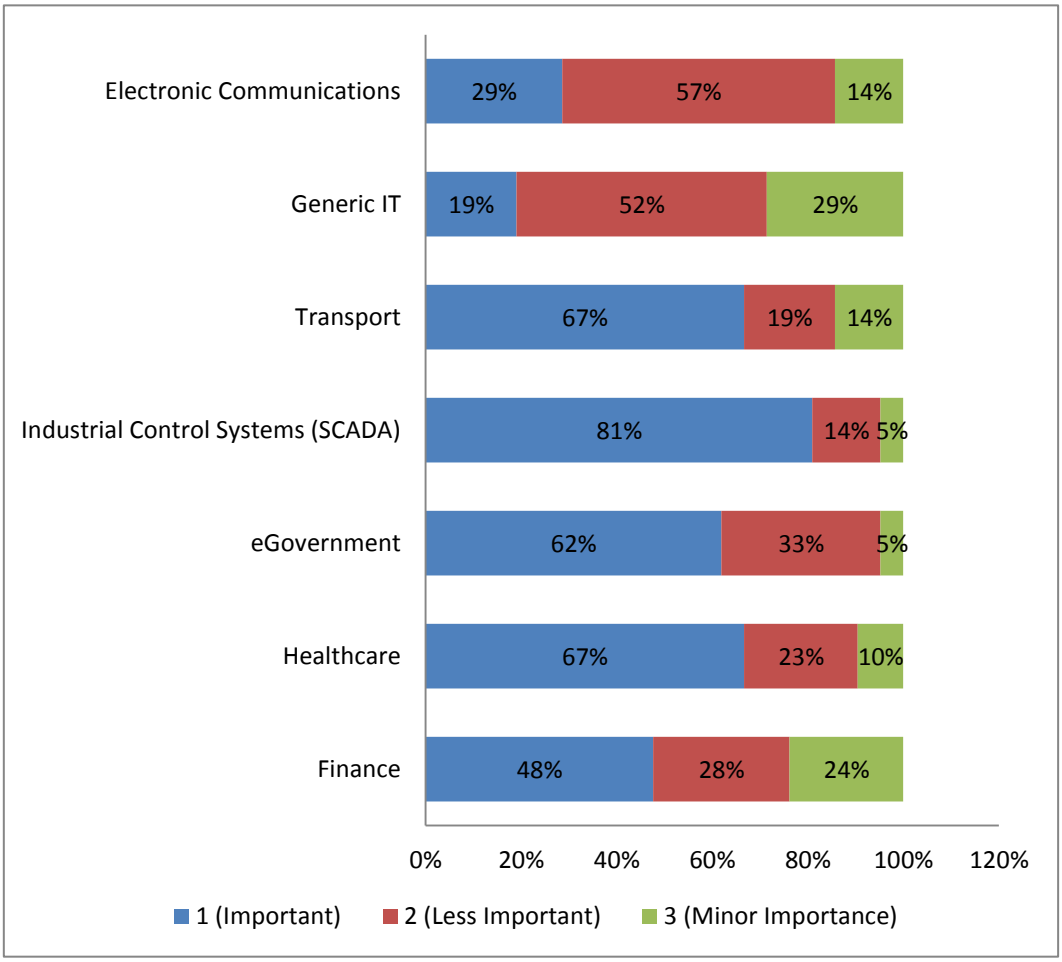

Figure 6 Sectors in scope

At the same time, one issue that was often mentioned in this context was that cloud service providers are hardly in a position to assess a-priori the criticality of their services because of the potential knock-on effect of outages. The impact of an outage depends on the kind of security measures customers took.

5.1.4 Cloud security incidents in scope

In the survey we asked respondents which incidents should be in scope of incident reporting. We first presented experts with a rough classification of the incidents according to their impact in 5 severity levels; for each level we provided one practical example. Then we asked the experts to indicate which incidents should be reported. The impact scale is presented below:

- Impact 0: Something went wrong in an exercise or a test. No impact on users.
- Impact 1: Incident had impact on assets, but no direct impact on customers.
- Impact 2: Incident had impact on assets, but only minor impact on customers.
- Impact 3: Incident had impact on customers.
- Impact 4: Incident had major impact on customers.

The answers from the respondents are summarized in figure 11. Most experts agreed that incidents with impact 3 or higher should be reported to authorities and should be the focus of information exchange across the sector and between member states.

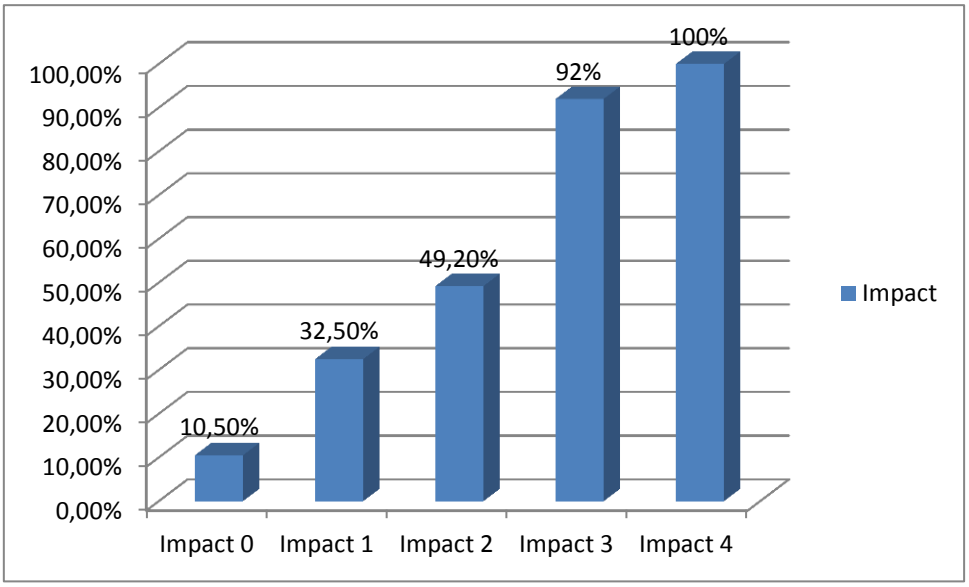

Figure 7 Impact based classification of incidents

When discussing this topic with experts, some experts remarked that often providers are not in a position to determine the severity of an incident, and/or if an incident had an impact on the core business operations of customers.

"We need to filter incident reports according to the impact but at the time an incident occurs we may not have enough information to be sure what the consequences were."

5.1.5 Incident report parameters

In the survey we asked respondents about which parameters should be included in incident reports. Figure 12 shows the responses of the experts. The most important parameter to report about is the criticality of the data or assets affected. This is in line with the fact that most experts would like to focus first on incident reporting in critical sectors. Besides this, most experts agree that incident reports should include information about the number of end users affected, the impact on customers (loss of data access, the geographic spread, and the duration of the cloud security incident.

Many interviewees said that the number of users can not be the only measure of the consequences for society; while some users might be inconvenienced by losing access to their files, for governments and other critical infrastructures the impact could be much more serious. The "significance" of an incident is something crucial to assess e.g. the temporary loss of access to an entertainment service, even if it affects many people, is very different from the risk of death due to a long-lived power outage in mid-winter, or a problem with air-traffic control. Finally, we emphasise that the impact must be significantly life-threatening for many people and/or cause or risk major long-lived economic harm.

Many experts reiterated the need to collect useful data that can be used to understand issues and increase the resilience of services, focusing on the impact of an outage. Some experts raised the issue that it is sometimes hard for providers to assess the full impact of an incident because cloud service providers do not always know the full impact of an incident in society or in critical sectors.

Most experts agreed on the fact that there is a need to share information about root causes and measures to mitigate common incidents.

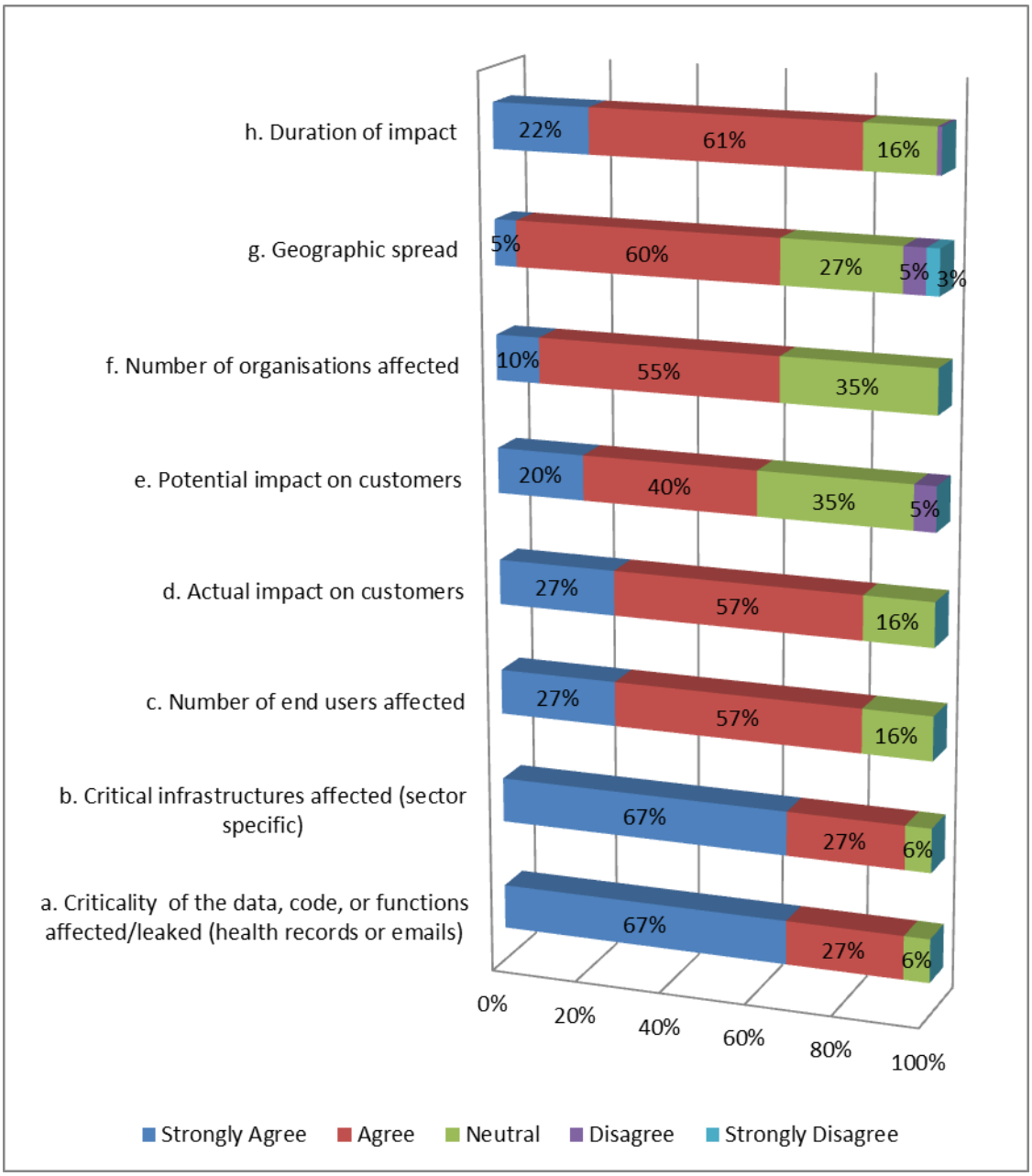

Figure 8 Parameters to measure impact on Cloud supporting CIIs

Finally, as discussed before, interdependencies across services, across society, makes it difficult to identify all the end users or customers impacted. This, in turn, makes it hard to calculate the geographic spread of an incident, for example. It seems that providers of IaaS and PaaS providers can only estimate the impact of incidents in technical terms. An estimation of the number of end-users affected can be done only at a later stage.

5.1.6 Incentives to foster incident reporting

In the survey we asked respondents about the potential incentives for providers to partake in setting up incident reporting schemes.

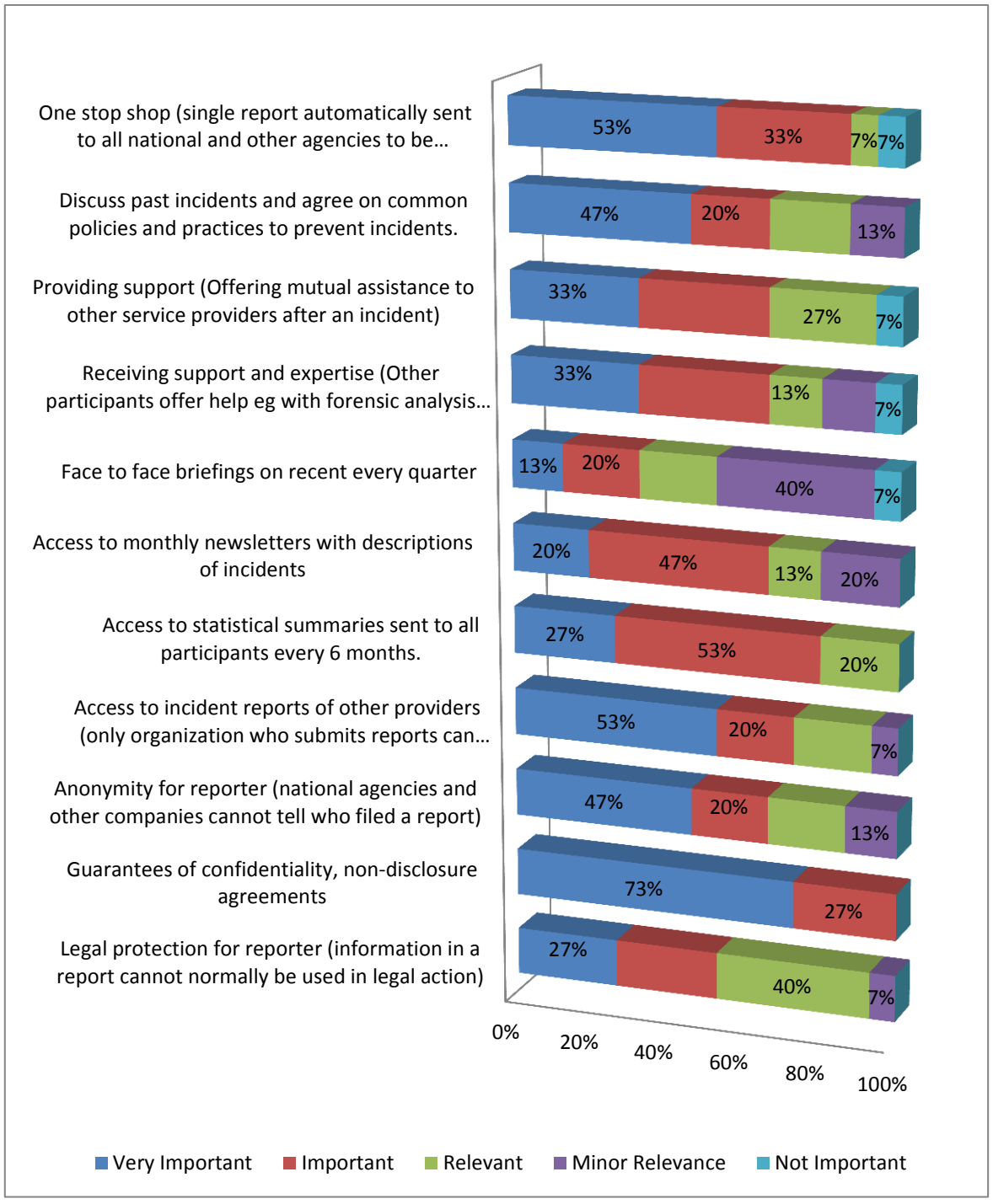

Figure 9 Incentives for incident reporting

In the interviews with experts one of the key success factors mentioned was “trust” between the information sharing parties. In competitive commercial environments, including cloud service provision, the level of trust required to support information sharing is difficult to achieve without

guarantees of anonymity and confidentiality. The main incentives for organizations to participate in a reporting scheme were considered to be:

- legal protection for the respective parties to encourage participation;
- non-disclosure agreements or anonymity for the different parties;
- ability to access the incident reports of other Cloud service providers;
- access to statistical summaries sent to all participants annually;
- a "one stop shop" – to coordinate the distribution of incident information across European, national and industry reporting systems.

Many experts were of the opinion that even if the provider is obliged to inform competent authorities, the incident reports should still be anonymised.

"[…] it is important not to disclose the identity of the organisations suffering the incident but at the same time provide sufficient detail for others to know that they might be affected. This could be more difficult for critical Clouds – where if an incident report mentioned a power company running a particular PLC then readers could infer that this might be one of two or three companies across Europe."

Most experts stressed the importance of anonymity in encouraging participation, especially in the start-up period when companies still need to gain trust in the scheme. Some experts raised the issue that in some smaller countries (with few providers) even anonymous reporting could be difficult. The main fear of providers is to lose customers if it becomes public that certain cloud services had suffered failures.

Another issue which was often raised by experts, was the fact that companies might lose a competitive advantage if other companies chose not to participate. From this perspective it seems that a legal requirement to partake in incident reporting scheme is necessary. Finally, some experts remarked that the issues of confidentiality would decrease as the reporting scheme matures and trust in the reporting scheme grows.

5.1.7 Compulsory or voluntary reporting of cloud security incidents

In the survey we asked respondents about whether or not incident reporting should be legally required or voluntary. It should be mentioned here that there are not many examples of existing voluntary incident reporting schemes.

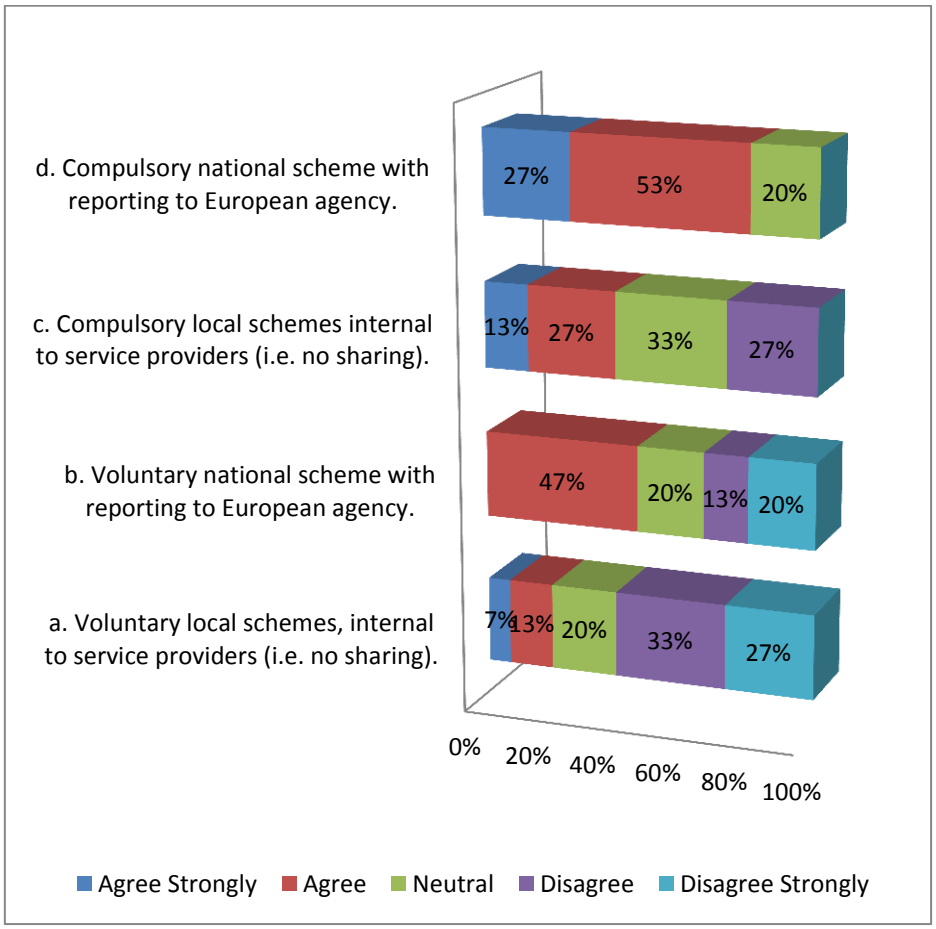

Figure 10 Ways to develop cloud incident reporting

Figure 14 shows the view of the experts. Most respondents are in favour of compulsory national schemes including the reporting to an EU agency (80%). Many respondents would also be in favour of voluntary national schemes, including reporting to an EU agency (47%). Respondents did not favour local reporting schemes, without sharing incident reports with a European agency. This is in line with the fact that most experts agree that incident reporting is most useful when the incident reports can be shared across sectors and across borders via an European agency.

In the interviews expert raised some issues with voluntary reporting schemes, expressing a concern about under-reporting. In voluntary schemes the reporting becomes biased, especially for some classes of incidents which are not directly visible outside the company. On the other hand experts acknowledged that cloud computing is still a new market and that over-regulation could stifle innovation. This could be of concern for European companies as cloud services are being developed with minimal regulatory intervention in Asia and North America.

"It is important to develop a framework that is simple rather than develop complex taxonomies or lists of incidents that would change over time. Over-regulation of a new industry needs to be avoided."

Experts also raised the concern that multiple national and international reporting schemes could make it hard for providers to comply. The experts we interviewed all strongly supported ENISA's potential role in aligning and harmonizing the different reporting schemes, particularly for small member states. The interviewees also stressed the need for Europe to act together and to develop a coherent Cloud strategy.

5.1.8 Incident reporting cross-border

In the interviews we also discussed the potential benefits and challenges with sharing incident reports across borders. Note that in the proposed NIS directive there are provisions for sharing incident reports between authorities from different countries. In the interviews the experts identified a number of further cross challenges with cross border sharing of incidents: :

1) Legislative and regulatory concerns - some governments cannot export data beyond their national borders, this may limit the submission of incident information affecting government systems in particular;
2) Jurisdictional issues – Clouds raise complex jurisdictional issues where customers are in one state, buying services from another that are implemented using systems in a third country. It can be difficult to determine where such incidents should be reported. Existing statutes establish jurisdiction in the State where a service is being purchased but the application and interpretation of the laws is often not well understood by many customers.
3) Trust across national borders –several of the interviewees mentioned the need to exclude incidents that might affect national security;
4) Integration of national and international systems. The interviewees stressed that it is important to minimise the regulatory burdens on a new and growing industry and to establish a level playing field across all member states when sharing across borders.

Larger companies that have more complex cross-border operations typically have access to legal departments that can identify their responsibilities. Smaller companies tend to have more simple operations and more straightforward obligations. One expert remarked:

"We do not have any uniform, single system for reporting incidents because there are many different companies in our group working in different member states. I get regular updates from across the group but the details are different. The development of a single European reporting system might help provide us with common reporting standards."

Other interviewees stressed the benefits to smaller member states where the costs of coordinating incident reporting could be shared. A European system for incident reporting could increase the consistency of information available within companies.

5.1.9 Statistics and post-incident analysis

We also addressed the topic off post-incident analysis in the interviews. By exchanging lessons learnt with other providers, it becomes easier for providers to address trends and issues emerging across the EU. Post-incident analysis can also help government authorities to take policy initiatives.

In responses to the survey, experts indicated they support publishing statistical information about incident reports, aggregating them across Europe. Statistical information should include:

1. Number of incidents per root cause (e.g. incidents caused by cyber-attack)
2. Percentage of users affected per root cause (e.g. 1% of Cloud users in the EU were affected by cyber-attacks)
3. Number of users affected per root cause (e.g. 50 end users were affected by an attack).
4. Total impact per service (e.g. UPS failures caused Cloud service outages of approx. 20 million user hours)
5. Percentage of impact per root cause (e.g. power failures caused 37% of the total Cloud service user hours affected by outages)
6. Percentage of incidents per root cause (e.g. half of incidents EU wide are caused by human error).

The interviewees confirmed that aggregated information would be useful to many different stakeholders. Some participants supported the development of a European system that was independent from security service vendors. Others argued that aggregate data can inform future regulatory requirements and reinforce ENISA's role in providing a bridge between EU legislation and the industry. Most experts interviewed supported the compilation and dissemination of statistical overviews. However, statistical summaries do not always provide a realistic view. It is important for regulators to supplement these overviews with additional studies into the detailed causes of incidents involving critical cloud infrastructures.

5.2 Summary of responses and interviews

- Services in scope:
  - Services (IaaS, PaaS, SaaS) supporting core systems of critical infrastructures;
  - Services that are used by large number of end users
  - Services covering large geographic spread
- Focus on critical sectors like finance, health, energy, transport and e-Government.
- Criticality of the service and impact of incidents should be analysed on a case-by-case basis.
- Incidents affecting availability, resulting to loss of services, should be reported.
- Incidents affecting data integrity and confidentiality could be reported.
- Parameters to report about:
  - Number of users affected;
  - Duration of the incident;
  - Services affected (criticality of data or services);
  - Geographic spread
- There is a need to set reporting thresholds for these parameters.
- A single reporting scheme and a single reporting template is needed for providers and operators.
- In the start-up phase the right conditions and incentives should be created (anonymity, confidentiality).
- Cross border sharing of incident reports with other authorities is crucial
  Post incident analysis and statistical information are important outcomes of pan-EU incident reporting. It is important to have bi-directional sharing schemes, where authorities feedback analysis and statistics to providers.

6 Incident Reporting Use Cases

The incidents mentioned in previous section are reality; yet, it is still a challenge to explain in each case which would be the process to report them to national competent authorities. In need of this clarification, below we depict 4 use cases of incidents, presenting the challenges in place and suggest how in each scenario, incident reporting would be realized.

6.1 Reporting Cloud security incidents by operators in critical sectors

6.1.1 Use case A: One community cloud- one critical sector

One cloud provider offers services (IaaS, PaaS) to the finance sector (critical sector); more specifically in two banks with data located in country X and in one bank with data located in country Y. The banks have built services on the top of the cloud infrastructure, supporting financial data of theirs customers and every day transactions. The **contract terms** have been specified to the customer's needs, having the banks to insist on their own standard term of secured unlimited liability for defined types of breaches or loss, notably breach of regulatory on security requirements such as breaches giving rise to regulatory fines. Same applies for in-house implementation of a private cloud in a bank.

When an incident occurs it impacts the availability of services and the datacentres of all banking organisations. The cloud provider, bonded by the contractual agreement with the client (in this case the bank), is obliged to report more information on the breach (light blue line). The reporting is based on customer specific data included in the SLA and/or contract. Currently there is no common template for all providers to use, to meet the SLA requirements of reporting.

The provider needs to report the technical data of the incident. The cloud provider is not aware of the services build on top of the IaaS/PaaS contracted, thus is not aware of the criticality of the data and/or services. In this case the report sent to the National Competent Authority (NCA), is sent by the operator, in this case the banking institutions. The operator will add more information on the impact of the breach to its core services and will need to provide this to the NCA. Since we talk about a cross border incident, each banking institution needs to send this to the NCA of the respective country. The NCA in this case could be the national finance regulatory authority. The scheme is depicted below:

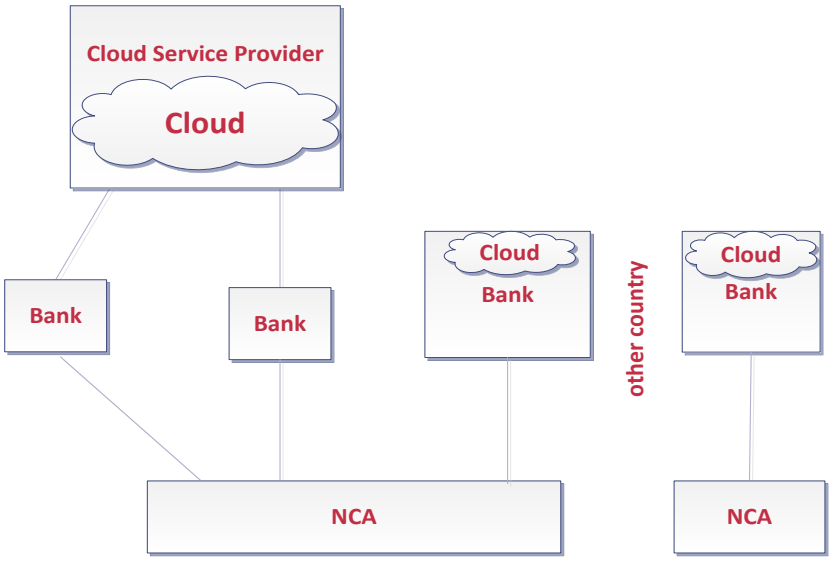

Figure 11 One community/ private cloud- one critical sector

6.1.2 Use case B: Public Cloud – Multiple critical sectors

One cloud provider offers services (IaaS, PaaS) to the finance sector and energy sector (critical sectors); the services built upon the contracted services are linked to availability of the core services to the customer (financial transactions and power supply). When a breach occurs to the cloud provider, he is obliged according to the contractual agreement or/and the service level agreement (SLA) to report the incidents to the customers (light blue line). As in the previous use case, the information included in the report is customer specific – in this case different for the banking sector and the energy sector. A common template across providers, to satisfy the reporting requirements to their customers could be a starting point in harmonising incident reporting in the cloud.

The different customers, in this case the banks and the energy supplier, since their core service has faced a loss of availability, will need to report to the NCAs. The information required by the provider, combined with the impact assessment of the operator, would be sent to the NCAs by the operator; in this specific case since we talk about two different critical sectors, the reports should be sent to the according NCAs, namely to the national finance regulatory authority and to the energy regulator. In this case we talk about "multiple-NCA". The scheme is depicted below:

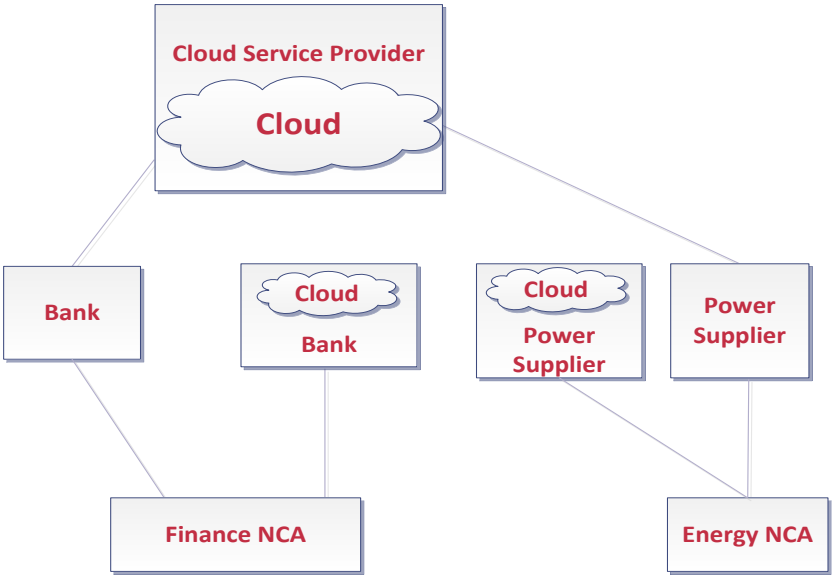

Figure 12 Public Cloud – Many critical sectors

6.1.3 Challenges of implementing security incident reporting

We analyse the challenges of security incidents reporting in the case of critical sectors:

- **Challenge 1: Definition of roles and mandate**
  Clear guidelines on how the incident reporting data flow will take place, "which will be the specific appointed NCAs", "which are the operators falling in scope", "which are the incidents in scope" need to be provided by the governmental authorities, always in conjuction with other European countries. The governemental authorities in each country need to define the roles of the different parties involved in the incident reporting framework. The NCA is the according regulatory body to receive the reports, however in each section the NCA is a different body i.e. for Banking sector is the National finance regulator, for Energy the according Energy regulator, in general the public bodies that have a regulatory mandate that includes networks and information security.

Critical service operator should report to the NCA. This means that a NCA should be defined per sector (and have the information security aspect in their mandate. In scope should fall all incidents that affect core services of the critical infrastructure and cause significant impact. To measure impact the operator needs to get metrics and classify them against specific thresholds i.e. number of citizens affected etc. The thresholds will be set by the NCAs after consulting the CII operators. This part of the reporting framework would need to be addressed by governmental authorities in order to be realized;

- **Challenge 2: Reporting clause in the contractual agreement**
  The provider needs to report to the critical infrastructures operator (a national risk assessment should take place to indicate the national critical infrastructures and investigate which of the core services are depending on cloud) according to the contract or SLA. The customer (in this case the CII operator needs to judge which critical infrastructures implemented in the cloud, are in scope). The scope of reporting incidents is determined in the contract (mandatory), and usually all incidents need to be reported or the provider operates a dashboard for the customer to monitor the service performance. This is one challenge the operator should mitigate by specifying this requirement when agreeing on the contract terms (reporting times, reporting flow, templates etc.).
- **Challenge 3: Template for reporting information**
  This report should include several technical information like: duration of breach, remediation time, systems affected, root cause, mitigation actions, addressing the positions taken on how to isolate the areas affected, remediation actions etc.; confidential information trusted only between the provider and the customer are also included in this report (name of provider, contact point etc.).
  The operator would have to share information on the type of services affected, give specific values to justify that the impact parameters measurements were over the set thresholds and provide feedback on remedial actions and lessons learnt, adding data on the impact assessment and subsequent root causes. Both reports the one from the provider and the one from the operator will need to be sent to the NCA for them to have a concrete idea of the entire incident and in the end which services affect citizens in a large scale.
  The need for a consolidated template is evident, so that NCAs will be able to collect and aggregate the data received. The reporting templates serve two purposes: a single reporting template is more efficient for providers with customers in different sectors, in different countries, avoiding the need for different reports with different content. a single reporting template makes it easier for authorities to discuss and exchange incident reports across sectors and across the EU.
- **Challenge 4: Cross border security incidents**
  An incident can affect operators in different countries causing a cross boarder incident. Operators will report the incident in their respective NCA's. However the NCA's need to have a communciation channel between themselves. The report to the NCA would need to include information on the Cloud Service Provider (CSP) and on the customer, and will need to cross check this data with the NCA of the other country affected, in order to avoid duplication of notification of incidents.
- **Challenge 5: Bi-directional flow**
  The NCA will need to send a summarized report to the collaboration network. Together with the the collaboration network, the NCA should provide feedback to the operator and the provider, i.e. providing a threat landscape overview, issuing recommendations etc. The collaboration network of authorities can support the governmental authorities in this task creating this way a benefit to the customers and providers.
- **Challenge 6: A harmonized approach**

A common reporting template for all providers could be a starting point towards harmonizing incident reporting. ENISA in this report makes a proposal on a common- flexible template to support the reporting scheme suggested.

6.2 Reporting by cloud service providers to authorities

6.2.1 Use case C: Governmental Clouds

One cloud provider (situated in country X) offers IaaS/ PaaS/ SaaS services to administrative bodies in country X (out sourced private – community cloud). The provider offers the potential of administrative institutions of the neighbour country Z to use the same services. The service provided is used by the tax offices and customers to perform tax declaration. The sector is not critical as such, but the data processed are.

In this case, as in case A, the user will insist on using his standard terms, the ones in accordance with the security requirements of the governmental authority.

The provider has signed a contract with the administrative institutions. When an incident happens, impacting the availability of the core systems of the customers, the provider will send, according to the contractual terms, a report with the technical specifications, the causes and remediation actions to the customer. Two challenges emerge in this case: which will be the NCA in this scheme; and who will need to report the provider or the operator. Since the provider is dedicated to this service, he would be able to provide a full report including impact analysis. However in the cases we have analysed until now, the operator is the one that reports to the NCA, since it is the one that collects more information on the scale of the impact (and is aware of the criticality of the services and data processed). The scheme is depicted below:

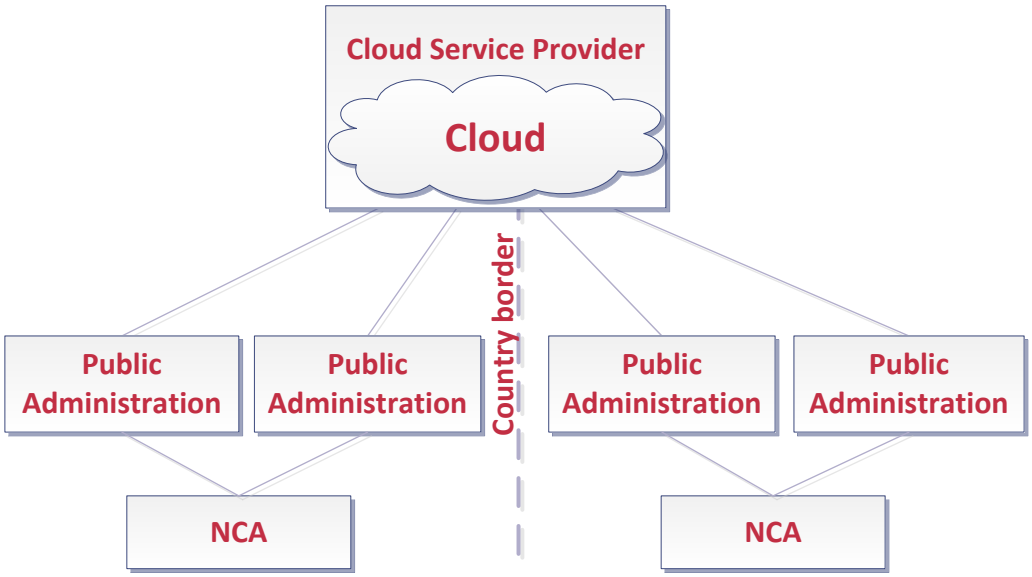

Figure 13 Governmental Clouds

6.2.2 Use case D: public cloud - non critical sectors

In this case, we describe a typical cloud provision model: a public cloud provider that offers services (SaaS, PaaS), like mailing services or applications, to many customers. The customers vary from SMEs and users, to operators that offer these services to other end users (supply chain of service provision). These customers are across different countries (the provider is not aware of their customers locations). When an incident occurs, affecting the service, the provider is obliged (if according to the contractual terms or/and SLAs) to report details of the incident.

In the case of informing the end-users, possibly a report (or a press release) would be enough to inform them of the security breach. This incident (could be business critical, meaning that could disrupt the daily operation of an enterprise) has major impact in society, causing loss of availability to a great number of users. Thus it should be reported. The appropriate party to report this incident is the provider of the services, estimating the total number of users affected. The challenge in this case is one: which the NCA involved in this scheme. The scheme is depicted below:

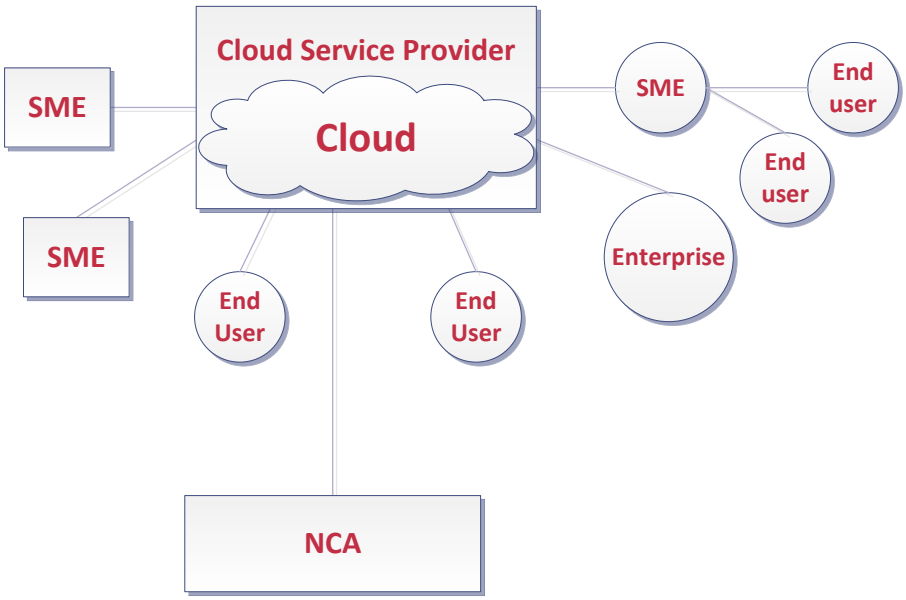

Figure 14 Public cloud - non critical sectors

6.2.3 Challenges of implementing security incident reporting

- **Challenge 1: Reporting process**
  The key difference of this use cases from the previous ones is that now the provider will be the one that needs to judge when to report a security breach to the competent authorities. Based on a case by cases analysis, the provider will need to report to the NCA on a voluntary basis. The cases, for which the provider needs to report, have to be clarified;
- **Challenge 2: Impact estimation**
  The reporting requirements for incidents having a "significant impact" could be overly broad and counterproductive when implemented by individual Member States. Cloud provider doesn't always know the precise impact, due to cascading effect and interdependencies. For this reason the NCAs should agree together with the CSP on a common approach to address the "significant impact estimation". The knowledge of CSPs would be very valuable at this

point, to explain how to measure loss of availability or continuity of a service offered and to set clear metrics i.e. CPU performance, MB loss etc.
The provider will need to indicate the parameters and thresholds according to which the incident has significant impact and needs to be reported. The thresholds need to be agreed between the NCA and the cloud provide, giving the values above which the provider will need to report;

- **Challenge 3: Information sharing**
  The provider will need to inform the respective NCA on the root causes, the impact assessed, the services affected and the users/clients affected. The information on the initial and subsequent causes should also be included; same applies for the services affected and the impact parameters.
- **Challenge 4: Scope of reporting**
  The scope of the incident reporting is not the same as in the previous cases. Large scale incidents should be reported, meaning incidents that affect many users in many different countries causing significant impact; the cloud provider might not even be aware of the exact number of users affected;
- **Challenge 5: Definition of roles**
  As in the previous case, the competent authority receiving the reports should be defined. However in this case, the problem is more complicated: where in the previous case the sector regulator that has a mandate on information security, would play the role of the competent authority, in this case there in no regulatory body to take the responsibility. Government should cooperate with the CSP to find the respective governmental authority to
- **Challenge 6: Voluntary reporting**
  Sharing aggregate data of incidents with competent authorities could also be made possible by a voluntary information sharing model of industry. Clear guidelines on how the reporting could be implemented for cloud providers need to be defined by the national authorities. Lessons learnt are the most important fact of information sharing for both governmental authorities and industry.

6.3 Summary of reporting flows

In this section we depict in one image, the reporting flows as discussed with the previous sections:

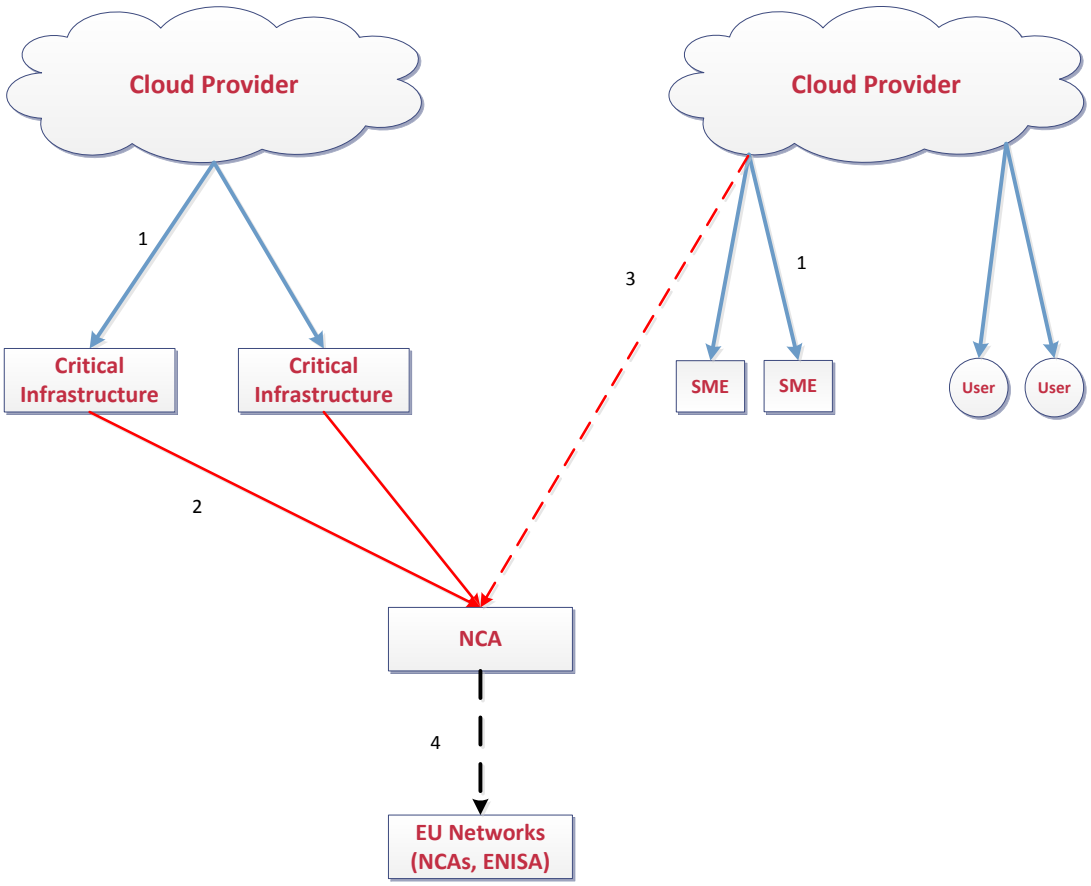

Figure 15 Cloud incident reporting scheme

We summarize the reporting flows depicted below:

1. (blue arrows) Reporting of the cloud provider to the customer as described in the contract/SLA clause. The report is customer specific and includes technical information on the incident, duration, area impacted, remediation time, systems affected that caused the incident, root cause and mitigation actions. It also includes information like provider name, contact point etc. In some cases – in the simple end-users, the provider is not requested to send an incident report but to make the incident public.
2. (red arrow) The operator of the critical infrastructure/ services reports to the National Competent Authority (NCA). In addition to the technical report sent by the provider, the operator includes specific data on the impact caused (make an impact "estimation"). The operator informs the NCA on the root causes, the impact assessed, the services affected and the users/clients affected. The operator's report contains information about the cloud services affected and the impact parameters, combined with data on the impact on its core services.
3. (dashed red arrow) The cloud provider reports an incident directly to the NCA. This reporting applies only to major NIS incidents affecting large number of users. The provider sends a report including this information to the competent authority.
4. (black dashed arrow) When relevant the national authority shares summaries of incidents' reports that occurred to a network of authorities across the EU.

7 Recommendations

7.1 General recommendations

We make several high-level recommendations about NIS incident reporting in cloud computing. We target mostly the government authorities (ministries, regulators, et cetera) tasked with ICT risk assessments and supervision of critical ICT (e.g. electronic communications, domain name registers, domains, certificate authorities, et cetera) in general, because we believe national regulators are fundamental in fostering transparency about NIS incidents and exchange of NIS practices.

- **Recommendation 1: Set scope with a national ICT infrastructure risk assessment**
  The ICT sector is rapidly changing; besides the quick changes in the traditional electronic communications services, recent years there is a wide range of other ICT services which are becoming more and more widely used, and hence more critical. Authorities should conduct risk assessments, periodically, and in this way determine the critical parts of the national ICT infrastructure. These critical parts should be targeted with specific (CIIP or other) regulation and reporting of network and information security incidents (NIS incidents) should be used by regulators to understand the state of security and resilience of this infrastructure.
- **Recommendation 2: Prioritize critical sectors and interdependencies**
  Priority should be given to the critical information infrastructure used in the critical sectors (defined by the CIP directive (2008/114/EC) – energy, oil, gas, roads, rails, air transport, waterways, shipping and ports excluding those telecoms sectors already covered by Article 13a. It is important to identify the cyclic dependencies between critical services, for example, the dependencies between the energy sector and the ICT sector. Power outages, for instance, often have an impact ICT infrastructure such as electronic communication networks. This infrastructure may also be needed to manage the power outage. In fact in some countries[23] there is a priority scheme for supplying fuel to data centres during large crises.
- **Recommendation 3: Only critical parts of cloud computing should be in scope**
  Cloud computing is now becoming the backbone of our digital society. At the same time it is not easy to identify all the cloud computing services which, if failing, could have a severe impact in society. Authorities should translate their national ICT infrastructure risk assessment to specific thresholds for specific services, and in this way target only the critical cloud computing services.
- **Recommendation 4: Use EU wide NIS incident reporting as a driver for discussing NIS**
  Incident reporting and sharing summaries of these reports nationally, with the sector and in pan-EU fora[24], lead to a better understanding of security and resilience of IT infrastructure and to a discussion about best practices. An active role needs to be played by the national authorities who need to set up national reporting schemes for NIS incidents and act as a filter for the sharing of incident reports across borders. National reporting can then be used as a basis for a better understanding of the security and resilience of large ICT infrastructures in the EU. Sharing of incident reports across borders naturally leads to
    - a common vocabulary/terminology for speaking about threats and causes, it provides a cross-check on the risk assessments (performed by companies) across the EU;

[23] Japan for instance.
[24] In interviews some experts referred to the concept of “European NIS incidents”.

- a starting point for discussion with the industry about which security measures and practices worked and if something more should be done;
- an EU wide view of common threats and common causes which can provide useful information for ICT service providers and cloud providers in particular.

- **Recommendation 5: Harmonized cloud incident reporting schemes**
  Many experts from industry and government warned for the risk of unnecessary costs due to national differences in implementing NIS incident reporting in cloud computing, especially because cloud providers often work across borders, which means that customers and regulators from several countries are involved. To allow for a level playing field and a competitive single digital market it is important to harmonize the implementation of incident reporting legislation whenever possible. There are several areas which should be addressed.
  - **Common vocabulary and format:** For the sake of efficiency authorities should agree on common vocabulary and terminology when speaking about incidents. This is important for customers, who may be dealing with multiple cloud providers, for providers, who may be dealing with regulators and customers from multiple countries, and for authorities, who may be dealing with incident reports from providers in different countries. Common digital formats for NIS incident reports (an XML scheme e.g.) would greatly facilitate the implementation of incident reporting for providers, customers and regulators;
  - **Common deadlines and procedures:** For the same reason it is important to agree on common procedures for reporting. For example, authorities across the different sectors, across the EU could agree on a two-step procedure where a brief notification is sent within hours and a full report is sent within days[25];
  - **Common terminology for causes:** One of the key goals of incident reporting is to understand the causes of incidents. By using a single terminology for (root) causes and threats authorities can more easily get an EU wide picture and understand risks in their countries better using the information about incidents which occurred across borders. In the context of the implementation of incident reporting under Article 13a ENISA introduced 5 root cause categories (Human Errors, System Failures, Malicious actions, Natural phenomena, Third party failures), which are used as a high-level classification. A vocabulary of more detailed causes (power cut, cable cut, DDoS attack) could then be used to analyse incidents in more detail;
  - **Common impact parameters:** It may be difficult to agree across the EU about common reporting thresholds because different countries have different size and different ICT dependencies. At the same time, a first step towards understanding the national differences is to agree first on a set of common impact parameters, such as the number of customers (or organisations) affected, the range of services affected, the consequences for customers affected, the geographic spread of incidents.
- **Recommendation 6: Think big, but start small**
  The field of NIS is growing and becoming more complex. There is also a wide range of different types of NIS incidents, ranging from everyday nuisances such as small power cuts affecting electronic communications, to organized attacks by criminals, severe natural phenomena affecting data centres, and so on. It may be tempting to try to address a wide range of incidents rather sooner than later, but it might be more effective to focus on a

[25] Such a set up would follow the two-step procedure described by the EC regarding the implementation of Article 4 of the e-Privacy directive, and it is in line with the two-step reporting process most EU member states use in the implementation

small subset of incidents and a small subset of cloud services first and extend scope only at a later stage. An iterative approach is particularly useful when addressing large and complex problems[26]. Useful scope restrictions could be for instance to focus only on cloud service outages, because outages are easy to detect and measure quantitatively, or a subset of services, IaaS e.g., because these services are more standardized and are used more like a utility infrastructure than other cloud services.

- **Recommendation 7: Authorities should collaborate with industry and develop voluntary reporting schemes**
  Most industry experts advocated in favour of starting with voluntary reporting schemes. Authorities should take this opportunity to collaborate with the industry and start piloting voluntary schemes, supporting this way the aforementioned idea of starting from a subset of services, and then moving to a larger one.
- **Recommendation 8: Pan-EU sharing**
  All experts were strongly in favour of reporting schemes involving pan-EU sharing of information, as opposed to more isolated national reporting schemes. By sharing summaries of incident reports with other authorities, they can discuss trends, common threats, as well as security measures and best practices. Only in this way can authorities feed-back relevant information to the industry. As a by-product, the sharing of incident reports will also contribute to harmonization, by introducing a single pan-EU terminology and vocabulary to discuss about threats, assets, and cloud security in general.

We believe national authorities should take an active role in engaging the cloud computing customers and cloud computing providers and pilot with them basic reporting schemes for NIS incidents in cloud computing. We look forward to facilitate this process and support authorities and providers with agreeing on efficient and effective reporting schemes, which provides the right information to authorities, citizens, customers and cloud providers without creating unnecessary costs for cloud providers and cloud customers.

7.2 Outlook

Security is often cited as an issue in cloud computing- partly because of general considerations arising from loss of control and lock-in of the customer and partly because data protection laws require providers to take appropriate measures, leaving security in a second place.

Cloud infrastructures now form a cornerstone of the digital society. Partly in consequence, the EU's 2012 cloud strategy aims to speed up the adoption of cloud computing as an enabler for financial and economic development. However, the increasing reliance on common technologies also raises concerns about the resilience of critical information infrastructures. It is widely acknowledged that the current lack of information about network and information security incidents can prevent government authorities and industry from taking action to mitigate the risks of future incidents. The EU's Proposal on the NIS strategy aims to address this problem by extending incident reporting obligations to a wide range of critical information infrastructures.

This report has analysed barriers and incentives for reporting incidents that involve cloud computing. We have described how the exchange of lessons learnt can help to increase the resilience of cloud computing services. The benefits of reporting incidents include: information sharing, experience exchange, identification of route causes and mitigations, data and trend analysis etc. The aim has been to provide government authorities (ministries, regulators, cyber security agencies) with an overview of issues and challenges when implementing national and pan-European

[26] It is indeed de-facto standard for software development now.

schemes for reporting incidents in cloud computing. The closing sections have also provided recommendations on the first steps that European and national agencies can take to implement future reporting scehemes.

This is just a first approach of a topic that will concern us more in depth in the future. ENISA, having the experience of a reporting scheme from been involved in Article13a reporting framework, will support all the relevant parties, competent authorities, providers and operators, to achieve a harmonised approach across all Member States.

TP-04-13-105-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

doi: 10.2824/25864

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu