Central Bank of Ireland
Outsourcing - Findings and Issues for Discussion November 2018
DVV Solutions Comment and Feedback

14th January 2019

Introduction

DVV Solutions welcomes the opportunity to respond to the Central Bank of Ireland's discussion paper "*Outsourcing – Findings and Issues for Discussion*" published on 19th November 2018.

DVV Solutions is a UK-based managed service provider of third-party risk management solutions, enhancing scalability, cost-efficiency and oversight of risk assurance frameworks and supplier due diligence programs. Our clients range from small, national and regional businesses to large, global corporations operating across banking, financial services, legal, retail and public sectors.

We are a Shared Assessments Program member and Assessment Firm with accredited Certified Third-Party Risk Professionals (CTPRP) and Assessors (CTPRA) utilising globally recognised industry-standard practices.

Key Messages

Having reviewed the discussion paper, The Central Bank of Ireland (CBoI) and its regulated firms are one of many sectors that have a growing concern around the use of Outsource Service Providers (OSPs) as most struggle to cope with the increasing demands of data handling, updated legal requirements and the resources needed to manage, store and process data securely and effectively. Outsourcing often alleviates much of the short-term burden of process management, and the immediate false sense of security is often a catalyst for systemic long-term risk development. Many organisations are unprepared for the eventual and inevitable impact of risks and particularly those which mature from deeply embedded poor practices. For businesses that are overly risk tolerant or perhaps unaware, risk management becomes a very reactive function rather than an embedded proactive process.

Success too is not without risk as organisations that undergo rapid growth particularly through acquisitions will often find themselves with processes and policies that are incompatible across business units. Individually these units may continue to function successfully yet there remains an underlying and increasingly compounded risk factor in that their internal functions do not integrate. This condition is exacerbated by the extent of supply chains and channel partners which together present a cocktail of anachronistic processes, policies and procedures.

Increasing Regulated Environments

The paper commissioned by the CBoI has gathered valuable data within in its regulated membership framework around common threats, yet these are not confined to the financial sector alone. It supports outsourcing risk trends that we see in all sectors which are being compounded by the introduction and enforcement of regulations such as the European Union (EU) General Data Protection Regulation (GDPR) and the likes of the Privacy and Electronic Communications Regulations (PECR) and the Senior Managers & Certification Regime (SM&CR) in the United Kingdom (UK).

Despite a lengthily pre-implementation period, many organizations found themselves unprepared for GDPR in May 2018 and left planning to the first quarter of the year. As such, the supporting infrastructure and policies to assure compliance with the interpreted regulations were rushed out and therefore lack the foundations on which to build an effective ISMS.

Outsourcing is traditionally justified through cost efficiencies, time to value and cost savings and was a widely accepted means to transfer or spread risk prior to the age of Big Data handling and compliance. At a fraction of the cost, the ease at which companies can procure external professional services and the false sense of security it offers drives this approach to the point whereby nearly all business functions are now under considerable pressure to be outsourced, particularly to Cloud Service Providers (CSPs). However, where data protection and security is concerned, risk can no longer be transferred or outsourced - it must be actively owned and managed by all parties concerned.

Procurement Led "Risk" Management

A fundamental flaw in outsourcing is that inadequate procurement due diligence and central monitoring is undertaken on supply chains. The complexity of dynamic components within this model makes oversight of a framework difficult to govern and report against. Lines of delineation, segregation of duties, roles and responsibilities are not clearly defined as different internal parts of the business often manage different parts of the external supply chain. While we typically see centralised and de-centralised models very frequently we have found that a federated model best meets these complex requirements. In addition to management functions, we often find that operational components such as contracts, Service Level Agreements (SLAs), Key Performance Indicators (KPIs) and specifically Key Risk Indicators (KRIs) lack substance or are absent. This risk is compounded where organisations have a framework of internal federated stakeholders, who even under the same industry regulations are independently outsourcing critical services in isolation with no broader consideration or governance. As more OSPs are onboarded, the extent of the issue becomes exponential to the point whereby the scale, scope and value of the risks are unknown. Whilst risk-based checks on specific tasks may exist within these frameworks, the time and resources needed to suitably monitor OSPs is grossly under-estimated which in turn affects budget applications creating a degrading perpetual cycle.

When considering data handling in chain outsourcing, the risks are again compounded as tracking data becomes a hugely labour-intensive and time-consuming task unless there is a dedicated central monitoring and reporting program in place. The challenge is centrally gathering and prioritising high-value outputs from seemingly low-level inputs.

Having noted in the report that monitoring deficiencies may exist within Intragroup, we suspect that this may be a result of a lack of internal stakeholder engagement when procuring third party

suppliers. Procurement systems too are fundamentally designed to manage purchase decision making processes and not the plethora of peripheral threats and risks beyond that supplier relationship.

Traditionally, onboarding is undertaken solely by procurement and is guided by cost and commercials as the primary factors. When considering the wider impacts of data on an entire organisation, there must be a mechanism and a partnership with other internal business stakeholders such as but to limited to; Information Technology (IT), Quality, Environmental, Health & Safety (QEHS), Security, Estates, Legal and Commercial in order to fully define a scope of requirements and to understand the risks associated with outsourcing. This approach will also help to develop and maintain a data processing map and define data classification standards.

Developing A Risk-Based Approach

Although all risk can be measured by financial loss, the procurement process must be led by risk as the primary factor and not by cost as financial loss is a result of risk materialising. Having identified the threats, vulnerabilities and risks, a process of monitoring needs to be standardised and applicable to context and environment in which they exist. Defining a process of assessment, monitoring, risk identification, reporting and remediation can only be done through the collation of specific data and analysis and must be done by trained and experienced professionals as dedicated assets. Even more so, this needs to be done using a process which is both repeatable and consistent and which factors in every component within the service offering. Only once a standardised benchmark is established can an organisation begin to measure risk and make meaningful comparative assessments.

There are significant factors to consider prior to outsourcing any service and must be an integral part of the Invitation To Tender (ITT) as beyond that is too late. The ITT offered to potential suppliers should include a checklist which outlines the standard requirements around data handling to assess the risk. This should not be considered as the “minimum standards approach” as this encourages cost-cutting but rather as “the standard” to define a quality benchmark. Potential suppliers must be able to demonstrate that they have the expertise, policies and processes in place in order to effectively manage data and the contracted services that support its management and processing.

Utilising Standardised Frameworks and Criteria

In addition to implementing recognised industry standards such as ISO for example, an effective way to address this is through the formation of an Information Security steering committee to oversee governance of the aforementioned issues, and specific to data protection. The members would comprise of formally appointed executives who advise and enforce policy through an Information Security Management System and Business Continuity framework. The structure of this committee must have a degree of representation from all stakeholders to mitigate any conflict of interest. It is also essential that the organisation’s Information Security Management System forms part of the Business Continuity framework using a shared risk register.

The involvement of an external third-party risk management specialists will bring an independent and impartial overview with cross-sector expertise. This too is measurable in terms of time, cost and progress as many organisations lack the resources and funds to design, build and maintain a management system which a certified specialist would provide. A collaborative approach with positive cultural change led by executives engaging with peers, industry experts and recognised standards will ensure that a sound foundation is embedded within the organisation. DVV Solutions and our technology partners have

championed such efforts across a range of sectors and our customers have experienced notably positive change in risk profile and resource efficiency.

We regard data protection and information security within the extended enterprise as the next significant growth industry within IT and will continue to maintain our position as a market leader in information assurance in the cyber supply chain.

If it would be helpful to your consideration, DVV Solutions would be happy to meet and discuss the points raised in this response.

Yours sincerely,

Bradley Horn CTPRA
Information Security Assurance Consultant
[redacted]

Sean O'Brien CTPRP, CTPRA
Managing Director
[redacted]

Detailed Response to questions for discussion:

Sensitive Data Risk

How are regulated firms ensuring that they have sufficient knowledge/ expertise within their own organisation to effectively challenge and gain assurance that their data is being managed securely by OSPs, including CSPs (how and where it is being stored, processed, used, located etc.)?

Auditing and assessments both internal and external are the only way to test the effectiveness of people, policy and process within the organisation. The biggest issues in undertaking regular testing are costs and resources, and those that have the expertise often suffer skill fade as they are not able to exercise their expertise. Implementing a dedicated auditing or assessment program to check and challenge processes is a fundamental to the success of an Information Security Management (ISMS) framework.

The ISMS policy must include a training and refresher schedule in order to maintain the program. An information security committee would typically oversee the ISMS, training and ensure that those involved are kept informed about industry, regulatory or legal changes. It is also good practice to engage with an independent external partner who can provide an impartial overview or conduct assessments.

What issues/ challenges are regulated firms encountering in gaining assurance that their sensitive business and customer data is being managed securely in outsourcing scenarios?

Procurement: There is a systemic issue that starts with ineffective pre-assessments of potential suppliers before they are invited to tender. OSPs should be able to demonstrate that they have the people, policy and processes in place to sustainably manage data and this must be measurable. This can be done at a high level by looking at what regulatory standards they exercise internally and the maturity of their information management system. Contractual agreements such as the right to audit or breach penalties are not clearly defined and are therefore difficult to enforce or to hold those in question to account. Many companies in fact are not fully aware of the extent of onward outsourcing by their supply chain and as such, poorly written agreements and KPIs are exploited by contracted suppliers.

There often also exists a misunderstanding by all parties as to who is responsible for managing data which either creates conflicting overlaps or a huge gap instance where nothing is done. Whilst companies now have data sharing agreements, these do not drill deeply enough into roles and responsibilities. Whist one of many tools, conducting regular assessments or audits is the only diligent way to seek assurances that data is being handled correctly. Outsourcing should be risk driven and not cost driven.

Expertise: Information security is still an evolving profession and similar roles would have traditionally been held under Information Technology and yet it is not a cyber specific role. InfoSec in fact touches every single component of any business and practitioners must have far greater skills than those confined just to IT. Sourcing experts who understand risk management in the wider context and particularly information security is challenging and is therefore often delegated to an individual or group who must cope with this as a secondary job role.

Culture: Proactive and effective third party risk management functions in the background and generates huge value without due recognition. It is undervalued as the benefits are only realised when a serious issue is found and a disaster is averted. Whilst many companies do undertake OPS assessments, we find this is a point in time assessment and only for specific purposes and does not factor in the wider dynamic threats and risks. Culture is by far and away the hardest thing to change in any organisation and as such it is essential that senior management sets the appropriate tone to support third-party risk management.

Concentration Risk

How are regulated firms seeking to reduce their exposure to concentration risk both from the perspective of providers and geographical locations?

We have found that many organisations do not currently record or manage concentration risk. We have found that with the implementation of GDPR, that organisations are now starting to ask their OSPs where their data resides. However, few have taken this further to examine concentration risk.

The issue is further complicated when an organisations third-party sub-contracts to a 4th or 5th party. In this instance, most organisations do not have a clear picture of where their data resides. GDPR should have forced organisations to map data process flows down through all of these nth parties and therefore organisations should have the raw material to being to map and assess concentration risk going forward.

How are regulated firms addressing concentration risk whereby they are outsourcing to OSPs who provide services for a large proportion of their sector? Of particular interest is how regulated firms are dealing with concentration risk where there are limited numbers of providers of niche services such as CSPs?

As mentioned previously, we have come across very few financial organisations who assess concentration risk at the 3rd party level, let alone the nth party level. Financial organisations are aware that they have an increasing number of eggs in the same basket, such as AWS or Azure and a limited number do assess and make some degree of judgement, but we have to date come across very few with active concentration risk policies, processes and guidelines.

Concentration risk in respect of niche providers is extremely difficult to detect and manage at an individual organisation.

Taking a step back, we would suggest that CBoI consider issuing guidelines to ensure concentration risk is assessed within the finance industry. Part of these guidelines may include the reporting of concentration risk back to the CBoI, who would then be able to assess concentration risk for niche providers and at least have an understanding of the potential risk.***Do regulated firms have views, as to how systemic concentration risk related to outsourcing, can be effectively monitored and managed by both regulated firms in all sectors and the Central Bank***

Systemic concentration risk is normally a result of poor procurement practices whereby not enough due diligence is undertaken on suppliers prior to onboarding. This issue is made worse by weak contracts and is further compounded by the lack of monitoring.

In addition to both cultural and policy changes, systemic risk can be managed out through a program of continual monitoring and/or auditing. This is akin to a change management program and needs to be fully supported and driven forward by executives. As mentioned previously, if guidelines were issued by CBoI in respect of concentration risk and third-party risk in general, the CBoI could begin to manage and steadily improve the overall OSP/CSP risk landscape for financial organisations throughout Ireland. You may wish to take a look at Shared Assessments. Shared Assessments are a third-party risk management industry body who provide complete third-party risk assessment frameworks, developed by and for the financial industry, and can be used to undertake detailed remote and onsite risk assessments of suppliers.

Offshoring and Chain Outsourcing

Given the significant volume of offshoring to the UK what preparations are regulated firms undertaking to prepare for Brexit and what related challenges are envisaged in terms of their outsourcing arrangements?

The UK will be expected to mirror EU legislation for the foreseeable future, especially given the reciprocity of markets, clients and supply chains. EU law is therefore expected to provide the de-facto standard to work to in respect of any UK-based decisions. However, incumbent upon regulators and regulated firms to maintain constant dialogue to ensure the anticipation and preparation for any possible conflict or divergence from current regulations in the medium- to long-term.

What steps are regulated firms taking to ensure they have full sight of any chain outsourcing which may be occurring within their outsourcing arrangements and how are they managing risks associated with this?

In respect of Publicly Identifiable Information (PII) data, Article 30 of the GDPR states that organisations must maintain a record of processing activities under [their] responsibility. Although the article does not define how this requirement must be met, a data flow mapping process can be used and to define information classifications. In addition to internal and external auditing, an assessment program such as the Shared Assessments should be implemented in order to verify appropriate controls are in place and track and remediate identified risks.

The organisation can also manage this risk through policies such as one which where possible bans chain outsourcing altogether within supplier contracts. As such, assessments and audits can be undertaken thus containing any prereferral risks such as those which are not immediately apparent.

How are firms ensuring that contractual rights of access are the same with all parties to a chain-outsourcing arrangement, as those granted by the primary third party OSP?

In an ideal world, chain outsourcing should be avoided to mitigate its inherent risks. However, given the interconnected nature of the cyber supply chain this is not practical or possible. The key to addressing chain-outsourcing begin with the right to audit which should always be specified within all supplier contracts as standard company policy and written in such a way that no misunderstandings can be deduced from its intended purpose.

The contract should also cover resource and financial responsibilities to ensure that nothing can prevent or hinder an audit taking place. Chain outsourcing must be subject to rigorous continuous monitoring not only be the end user, but by the chain customer. As an originating organisation in the nested supply chain, you should endeavour to utilise flow-down terms within your contracts to ensure things like right to audit, geographic location of your data, etc. The entire supply chain must adopt and adhere to the same processes, policies and procedures to ensure transparency and accountability.

Where flow down terms are not possible, then the organisation has things they can do to assess the risk of nth parties. The first is to assess/audit your third-parties, third-party risk management process and subsequent output. The second is to utilise one of the many Continuous Monitoring tools on the market today. Our advice would be to look for Continuous Monitoring tools that not only look at the cyber aspects of nth parties, but also look at the wider remit, to include brand, reputation, financial and operational risk.

Substitutability Risk

What issues/ challenges are regulated firms encountering when assessing substitutability and exit strategies? How are these being addressed?

A fundamental challenge is that contracts do not cover exit strategies in enough detail and much of the terminology is implied or open to interpretation. Whilst organisations undertake due diligence for onboarding, not enough is done for offboarding and unless there is a clear breach, the assumption is that the contract with conclude at the end of its term without issue.

Suppliers rarely go bad overnight. It is usually something that the organisation sees coming several months in advance, either through poor performance, or changes in circumstance. Organisations should consider utilising Continuous Monitoring solutions to monitor a supplier's competitors to greatly reduce the risk of jumping from frying pan to fire. The lack of suitable and affordable suppliers too prevents customers from approaching the wider competitive market as many hold monopolies and therefor indirectly hold customers to ransom. We feel that regulators could do more to enable customers by putting pressure on service providers to open their markets and incentivise innovation. This approach would perhaps encourage collaborative partnerships between regulators, regulated firms and suppliers in better defining contractual agreements and costs.

In reality, most organisations currently struggle with identifying all of their third-parties and keeping abreast of the onboarding process. A limited number manage mid-contract changes and very few have even begun to successfully manage the exit aspects of third-party risk.

As with all of these things, tone is set at the top and should result in the exit process being clearly defined through policy, process, guidelines and standards with a third-party risk management framework.

What are the risks / challenges where there is no substitutability or it is not possible to bring the service back in house? How are these being addressed?

Once a service has reached a degree of maturity and scale it becomes financially unviable to bring it back in house. Supporting the service in house requires infrastructure, resources, training, expertise and investment all of which are absorbed by the OSP and were defining reasons for outsourcing in the first instance. It is important that customers maintain a unilateral standard and relationship with suppliers but also to ensure that they do not become complacent and wholly reliant on their service.

Access to technology, funding and expertise are the primary blockers to re-establishing an in-house service. We often find that there is a lack of understanding of the scope, scale and cost of the service offering which inhibits what would otherwise have been a clear decision to bring it back in house. Many organisations only realise the risk upon its fruition and which could have been managed or mitigated through better management. Large and often stagnant OSPs hold market shares and block access by smaller innovative OSPs into markets which leads to a non-competitive environment.

- ENDS –

SFG SHARED ASSESSMENTS

DVV Solutions Limited
Grosvenor House, St. Thomas's Place,
Stockport, Cheshire, SK1 3TZ, United Kingdom
Registered in England. 3858411

Tel: +44 (0) 161 476 8700
Email: enquiries@dvvs.co.uk
Web: www.dvvs.co.uk