ASSESSING THE BUSINESS RISK OF TECHNOLOGY OBSOLESCENCE THROUGH ENTERPRISE MODELLING

Cameron Spence
Capgemini, 1 Forge End, Woking, Surrey, U.K.
cameron.spence@capgemini.com

Vaughan Michell
Informatics Research Centre, Henley Business School, University of Reading, U.K.
v.a.michell@reading.ac.uk

Keywords: Enterprise architecture, Obsolescence, Risk, Modelling.

Abstract: The problem of technology obsolescence in information intensive businesses (software and hardware no longer being supported and replaced by improved and different solutions) and a cost constrained market can severely increase costs and operational, and ultimately reputation risk. Although many businesses recognise technological obsolescence, the pervasive nature of technology often means they have little information to identify the risk and location of pending obsolescence and little money to apply to the solution. This paper presents a low cost structured method to identify obsolete software and the risk of their obsolescence where the structure of a business and its supporting IT resources can be captured, modelled, analysed and the risk to the business of technology obsolescence identified to enable remedial action using qualified obsolescence information. The technique is based on a structured modelling approach using enterprise architecture models and a heatmap algorithm to highlight high risk obsolescent elements. The method has been tested and applied in practice in two consulting studies carried out by Capgemini involving three UK police forces. However the generic technique could be applied to any industry based on plans to improve it using ontology framework methods. This paper contains details of enterprise architecture meta-models and related modelling.

1 INTRODUCTION

As the pace of technology introduction quickens and IS becomes more pervasive the rate of change of technology and the forced obsolescence has also increased (Bulow, 1986). This very pervasiveness increases the connectedness and reliance on specific technology which can quickly become obsolete (Whelan, 2000). This increases both the cost of maintaining existing and or replacing the technology (Solomon et al., 2000). Doing nothing is not possible due to risk of loss of service provision and hence the management of obsolescent technology is becoming critical. The current economic focus on austerity has increased the need for better obsolescence awareness and management as businesses seek to consolidate and reduce their costs whilst maintaining their technology competitiveness.

Much of the existing literature regarding obsolescence has focused on its definition and relationship to specific business contexts. (Lemer, 1996) has focused on evaluation of the performance and eventual failure of obsolescent infrastructure facilities (e.g. public works, sewers, pavements etc) and the need to establish reliable design service life metrics. (Solomon et al, 2000) explores the obsolescence of electronic integrated circuit components such as DRAMs, via an adapted stages of growth model that includes obsolescence. Whelan (Whelan, 2000) discusses the impact of obsolescence on stock management and the value and effective mathematical productivity of stock ranging from computers to industrial machinery and its relationship to computer usage. Feldman (Feldman and Sandborn, 2007) looked into the problems of obsolescence with respect to the parts procurement lifecycle to improve algorithms for parts forecasting and management. (Aversano et al., 2004) examined strategies for evolving existing software and included obsolescence as a factor along

Spence C. and Michell V.
ASSESSING THE BUSINESS RISK OF TECHNOLOGY OBSOLESCENCE THROUGH ENTERPRISE MODELLING.
DOI: 10.5220/0004458600610070
In *Proceedings of the First International Symposium on Business Modeling and Software Design (BMSD 2011)*, pages 61-70
ISBN: 978-989-8425-68-3

with quality, economic and data value in their metrics. Similarly (Boehm, 1999) includes technical obsolescence as a factor in a similar paper on software productivity and reuse. Little work has been conducted to develop a practical methodologies approach to finding obsolete software and related components.

Obsolescence results in an inability to meet performance criteria (Lemer, 1996), for example when the requirement has moved on, or the technology has been superseded. Our concern is with the former. We propose an approach to identifying and managing obsolescence and risk using a simplified enterprise architecture and heat map approach that can be scaled to different size companies. The approach has also been successfully trialled to identify and manage IS infrastructure obsolescence in a specific business case of a police service where low cost obsolescence risk assessment was required to support change decisions.

There are three main issues to address when considering the impact of technology obsolescence on a business: we need to define obsolescence and its impact factors; we need a way of identifying the other aspects of technology and services impacted by that obsolescence; and finally, we need a way of identifying the greatest risk to the business from those obsolete technologies and services. These three issues are addressed sequentially in the next section on approach.

2 APPROACH

2.1 Obsolescence and Impact

2.1.1 What is Obsolescence?

As Sandborn suggests definitions of software obsolescence for commercial off the shelf (COTS) products vary, as there is often a big gap between the end of the product sale date and the date of the end of the support for the product (Sandborn, 2007). The withdrawal of support however, may not lead to immediate loss or degradation, but acts as a trigger for the business to make the necessary decisions to preserve the capability provided by the technology, subject to its criticality. For our purposes we will define obsolescence as the loss or impending loss of support for technology that reduces its ability to continue to function in the organisation (Feldman and Sandborn, 2007). Whilst the date of end of production of the technology and the date of end of support is reasonable to identify, the way in which the technology will be affected by degraded or no further support is more difficult to determine and will depend on the capabilities and resources of the organisation as well as the technology being considered (Lemer, 1996).

2.1.2 The Impact of Obsolescence

Many organisations are running with a technology estate that is substantially obsolete. This causes problems of cost and risk. Increased costs are introduced by (a) the requirement for special support arrangements; (b) the extra development required to provide applications that can cope with obsolete technology (a notable case in point is the continued use of Internet Explorer 6 and Windows 2000 in the UK public sector); and (c) difficulty/high cost of obtaining support for very out-of-date technologies (both hardware and software).

Many factors may contribute to a high cost of ownership of an IT estate; it is often instructive to keep recursively asking the typical root cause analysis question “why” to determine root causes (Ginn et al., 2004). For example, high costs associated with running applications in data centres could be traced back to costs for the actual infrastructure (servers, switches etc.) and costs for the datacentres themselves (cooling, power, rent etc.) For the servers, then costs could be associated with both software and hardware – and the costs for both of these are likely to go up over time as the products on which they are based start to become obsolete and thus the subject of special (custom) support arrangements. Eventually the products involved will become unsupportable, which transforms an issue with high cost into an operational risk to the business. A root cause analysis in graphical format made this very apparent and understandable to the client (fig. 1).

The increased costs and the lack of knowledge results in increased operational risk of service failure, especially where obsolete technology is a key part of the core service delivery capability of the business. This operational risk if not attended to can then result in reputational risk where business service performance is badly impacted by IS/IT failure. With no action there is a risk of degradation of business service capability through the inability to process and disseminate quality (correct, complete and timely) data and information through the enterprise. However, it is not enough simply to identify the technology components that are subject to obsolescence. We also need to understand how the technology supports the business and specifically the processes and services delivered by it. Critically we also need to quantify the importance of the relationship between in order to understand the impact of the obsolescence.

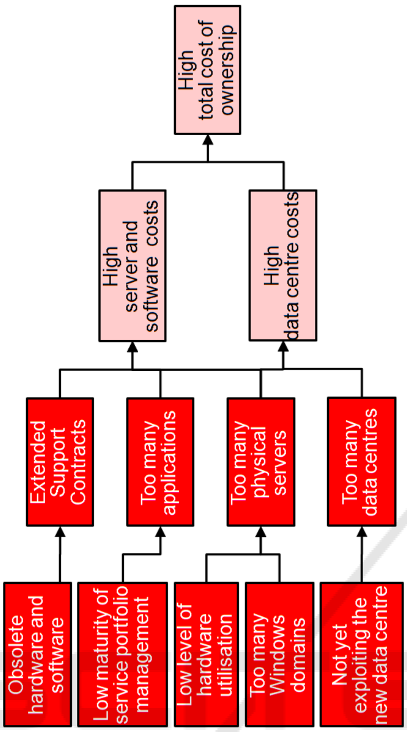

High total cost of ownership
High server and software costs
High data centre costs
Extended Support Contracts
Too many applications
Too many physical servers
Too many data centres
Obsolete hardware and software
Low maturity of service portfolio management
Low level of hardware utilisation
Too many Windows domains
Not yet exploiting the new data centre

Figure 1: TCO Root Cause Analysis.

A near obsolete IS component will be dependent on a cascade or chain of factors that determine the level of risk and impact of the obsolescence as seen in the four step chain in Figure 2.

The first factor is the proximity of the technology component to obsolescence. This will depend on both the vendor support and maintenance to allow the product to function after obsolescence. The second factor is obsolescence criticality: even if the obsolete technology is supported after obsolescence the service provided by it might be degraded, as it may not be able to provide the IS service performance of newer or competitor products. Alternatively an upgrade path may allow the degradation to be reduced. The third factor is impact of the IS component on the business service. For example is the performance and capability of the IS component critical to the business service, or does it add very little value? Finally the fourth factor is the criticality of the business service in terms of delivering value to the customer. Ideally all these factors should be taken into account on the basis of a failure mode and effect analysis (Ginn et al, 2004) but this can increase cost and complexity. Some analysis frameworks already provide useful metrics for the criticality of the business and IS service relationships (Liu et al., 2011) but these are better suited to comprehensive architecture analysis. For our purposes we propose a more simplistic risk framework based on a simplified metamodel explored in the later sections.

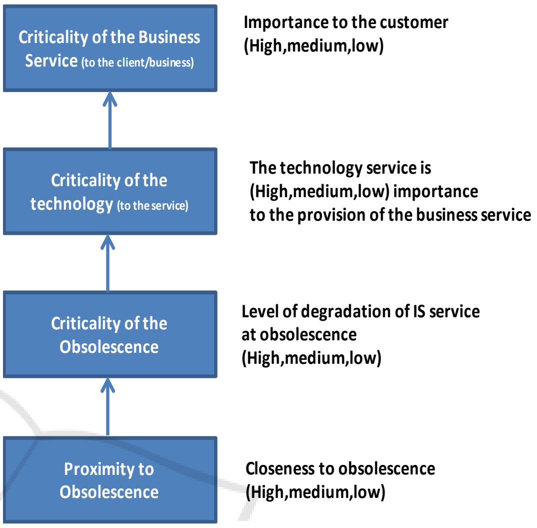

Criticality of the Business Service (to the client/business)
Importance to the customer (High,medium,low)
Criticality of the technology (to the service)
The technology service is (High,medium,low) importance to the provision of the business service
Criticality of the Obsolescence
Level of degradation of IS service at obsolescence (High,medium,low)
Proximity to Obsolescence
Closeness to obsolescence (High,medium,low)

Figure 2: Obsolescence Impact Factor Chain.

2.2 Services and Technology Impacted

2.2.1 Identifying the Services and Technology Impacted

Information-intensive industries have very large amounts of IS/IT with attendant software and technology hardware and component risks. If the maturity of the architectural and operational processes have not kept track with the size of their IT estate, then there may be a lack of understanding of exactly what technology the organisation has, who is using it, and what its vulnerabilities are.

2.2.2 Understanding the IT Estate

The term “IT Estate” is generally used to refer to the complete portfolio of technology used within a business – including applications and infrastructure. If the knowledge of such an IT Estate is not encapsulated and maintained in some kind of ‘living repository’, then the lack of corporate knowledge can be exacerbated over time by changes to personnel within the organisation, so that key knowledge as to what exists and for what purpose, is lost as people’s roles change. The federated nature of some large organisations can make this problem worse, because from the outset, no one part of the organisation ever has a complete picture of the business and technology architecture. The best that can be achieved in these circumstances is that individual parts of the organisation try to document solution architectures that capture their piece of the picture. A lack of knowledge of an Enterprise Architecture can make it hard to plan for the future, because without knowing the 'as-is' state, it is difficult to know what needs to change in order to achieve a 'to-be' state. Thus, it is possible to view the 'status quo' as a safer option, putting off the required upgrade and modernisation projects. Without knowledge of what applications are being used, by whom, and their underlying technologies, it is not possible to get a view as to the risks being posed to the business due to this obsolescence.

2.2.3 Case Studies

The aims of the first project, from the client's perspective, was (a) to understand the potential cost savings associated with rationalising the application platforms, and (b) understand the degree of risk associated with technology, and provide a roadmap for addressing it. Thus, the idea of heat-mapping the business risk is highly relevant because it provides part of the 'business case' for making the relevant upgrade / replacement projects to address the risks thus identified.

The aim of the second project, a partial merger of two UK police forces, was to seek cost savings by identifying duplicate applications. However, the heatmaps were also relevant here, both in pointing out risks to the businesses, as well as assisting in the choice of applications to retain.

2.2.4 Enterprise Architecture Meta Model

It is necessary to gain an understanding of the business technology architecture estate in enough detail so that, obsolete technology types can be traced through to the applications relying upon them, and thence through to the business services and functions that in turn rely upon those applications. Many enterprise architecture models have been developed to make sense of business and technology components found across a variety of businesses (Lagerstrom et al., 2009) and aligning business services with IT capability (Strnadl, 2005). Our specific issue requires a focused model that is easy for business and technical users to understand, but also shows dependencies between components. For this reason we have adapted and extended part of the TOGAF (OpenGroup, 2009) content meta-model to build a set of artefacts and inter-relationships that are particularly relevant to our area of interest.

Although standards exist for modelling Enterprise Architectures, it is frequently necessary to adapt those standards for different client situations. Reasons for this include: (a) the client prefers a particular standard (e.g. TOGAF or Zachman (Noran, 2003) or one of their own frameworks and (b) there are requirements for a particular engagement that demand a change to the standard model. In the first example discussed in this paper, the client was particularly interested in rationalising the application platforms rather than the applications themselves. Therefore, there was a heavy focus on infrastructure. The model used is illustrated below:

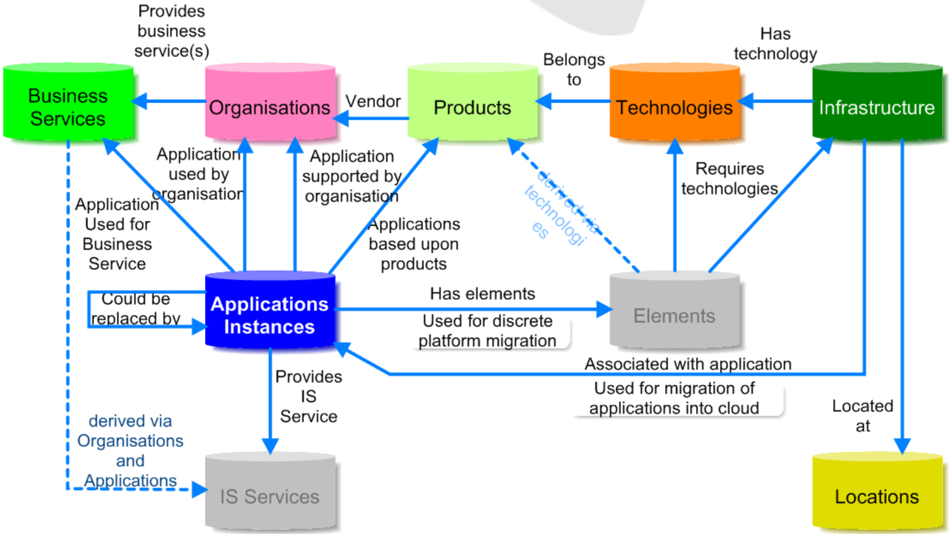

Provides business service(s)
Business Services
Organisations
Vendor
Products
Belongs to
Technologies
Has technology
Infrastructure
Application used by organisation
Application supported by organisation
Application Used for Business Service
Applications based upon products
derived via technologies
Requires technologies
Could be replaced by
Applications Instances
Has elements
Used for discrete platform migration
Elements
Associated with application
Used for migration of applications into cloud
Provides IS Service
Located at
derived via Organisations and Applications
IS Services
Locations

Figure 3: Sample Meta Model for Analysing Cost and Business Risk due to Obsolescence.

Figure 3 represents the actual model that was used to capture, analyse and report on various aspects of the IT portfolio for the first police force. With this particular client, two aspects of the model (shown in grey) were not used at the time of writing. For the other study involving two police forces, heavy use was made of the IS Services component, critical for application de-duplication.

Parts of this model had previously been used with another client to carry out an analysis of their application portfolio with a view to rationalising that portfolio (removing duplication). This gave rise to the two elements focusing on Applications (or **Application Instances**) and **IS Services** (both taken from TOGAF). By definition, any two applications that are labelled as offering the same IS Services are duplicates; and one of the aims of that study was to aim for a ‘minimum set’ of applications that gave the full range of required IS Services (functionality).Part of the business case for rationalising applications is of course the cost of running those applications, and part of the cost of an application comes from the servers hosting that application. Servers are of course a particular kind of infrastructure, which is why the model includes **infrastructure**. This infrastructure resides in physical **locations**, which are important to know for a number of reasons, especially when part of the rationalisation design includes closing one or more data centres. This has no bearing on the question of obsolete technologies, but was critical to the analysis and creation of the rationalisation design.

The servers in the IT estate for any client will have installed on it a number of software **products**, for example applications, databases, middleware, operating systems, monitoring and so on. In addition, the servers themselves are of course products from a hardware manufacturer. Thus, the products need to include a list of all software and hardware in the IT estate. In practice, the terminology used to describe a particular product may be very different to the terminology used by auto-discovery software, which sometimes goes to the extent of looking at versions of libraries installed on the servers (for example, Dynamic Link Libraries, or DLL files, on Windows platforms). Examples of this are (see table 1).

When looking up products on manufacturers’ websites, the term in the left column needs to be used. However, when auto-discovery tools are run, the terms in the right column are those that are generated.

Table 1: Sample Product-Technology Mappings.

Product	Technology
Windows Server 2003 Enterprise x64 (SP2)	Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition Version 5.2.3790 Build 3790 SP2
RDBMS 10g Release 2	Oracle Database Server 10.2.0.4.0
Solaris 10	SunOS 5.10

With this particular client, there were several thousand servers that needed to be matched up to products. Using this intermediate mapping meant that this could be done largely automatically. Once it had been calculated to which product a particular ‘technology’ corresponded, then that mapping was automatically applied to all instances of that technology.

Another reason for the use of this intermediate layer was the fact that in many cases, there were multiple pieces of software that corresponded to the same product, which were ‘discovered’ separately. For example, two separate pieces of software were discovered (“Oracle Net Services (TNS) Listener 9.0.1” and “Oracle Database Server 9.0.1.0.0”) that both corresponded to the same product (“RDBMS 9i Release 1”).This intermediate mapping of **technologies** provides the ability to cope with multiple synonyms and multiple pieces of technology that belong to a single product. The intention of the **elements** artefact was to allow the modelling of major components of the application (e.g. web tiers, database tiers, business logic tiers, storage allocations) so that they could then be rationalised. This is not relevant to the obsolescence discussion.

The final pieces of the model are both drawn from TOGAF. The **organisation** information allows us to represent the structure of an organisation, which is where the users of the applications reside. This is also useful for representing external organisations, for example the vendors of the products, or those involved in some way in supporting the applications.

The **business services** are the services provided by the business to its client. Clearly defining business services is necessary in order to be able to make a correlation between the services provided by the business and the IT that supports those services. Also the criticality of the service to the end client, will in turn affect the importance of the IT service and hence the impact and risk associated with the obsolescence of the technologies and components.

2.2.5 Populating the Model

The model was implemented using a particular modelling tool, MooD®. The functionality provided by this tool was critical to our ability to import, analyse and report on the data that was captured.

Many different information sources were used to populate this model, including but not limited to Active Directory, Tideway (auto-discovery software), a Configuration Management DataBase (CMDB) product and various spreadsheets populated manually.

The applications were populated using a combination of reports from the CMDB and spreadsheets provided by the client. The infrastructure was populated using a set of spreadsheets from various sources. The technologies were populated using spreadsheets from the auto-discovery software. The products were populated partially manually, interpreting the technology lists in the light of the team's knowledge of the marketplace, and partially using data from the CMDB.

The organisation was populated using information on the client's public web site.

The business services were populated from a generic UK police business service architecture published by the National Police Improvement Agency, called the "Policing Activities Glossary" (NPIA, 2011). This provided a hierarchical representation of the services provided by UK police forces, which we represented graphically in the modelling tool:

2.2.6 Tracing Obsolescence to Applications

Obsolescence as applied to technology (such as hardware and software products), using the definition previously offered, means "loss or impending loss of support for *hardware or software products* that reduces their ability to continue to function in the organisation". These products are produced by various organisations (vendors / manufacturers), who often specify a date beyond which support for their products will either cease, or become more restricted (and perhaps substantially more expensive). Some manufacturers specify "End of Support" (EOS) and "End of Extended Support" (EOES) dates for their products.

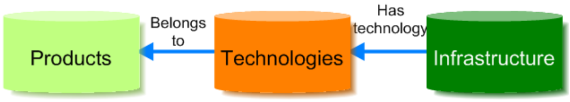


Figure 4: Obsolescence from Products to Infrastructure.

Starting from the products, therefore, and knowing that several products may relate (via the Technologies intermediate layer) to a piece of Infrastructure (a server), then it is possible to say, for each piece of infrastructure, what is the earliest EOES date for any product that relates to that piece of infrastructure. For example, if that infrastructure was based upon a server model that had an EOES date of February 2013, but ran Windows 2000 that had an EOES date of 13th July 2010, then we can say that the earliest EOES date of these is the latter – so give the infrastructure as a whole, an EOES date of 13th July 2010. In other words, there is something about this piece of infrastructure that will be difficult and/or costly to support beyond that date.

The next step is to roll this up into the application layer.

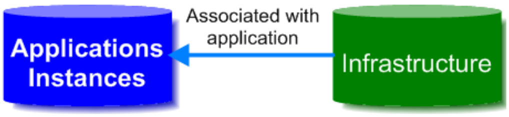


Figure 5: Obsolescence from Infrastructure to Application Instances.

Following the same approach, we can look at all the servers that are associated with a particular application (or instance of an application), and pick the earliest EOES date for each of these servers. In other words, we are saying that for a particular application, there is a particular piece of technology (software or hardware product) somewhere in the supporting infrastructure that will make application difficult and/or costly to support beyond that date.

2.3 Identifying Business Risk

An approach to identifying business risk from IT in general is discussed in (Halliday et al., 1996). This paper suggests a four-quadrant model for categorising risk, including notably the "avoid/prevent risks" which are viewed as being most critical because of the impact to the business should they be triggered, as well as the probability of them occurring. In this particular paper, we are focusing on the risk to the business from technology obsolescence that would fall within this particular quadrant. In other words, these are risks that a business can and should manage down to an acceptable level, and perhaps would if those business stakeholders were actually aware of their existence in the first place.

The use of 'heatmaps' is appropriate to demonstrate business risk, if backed up by proper evidence.

2.3.1 Algorithm for Generating a Risk Heatmap

The heat map, a colour-coded display of the intensity of a result has been used in various forms (Wilkinson and Friendly, 2009) to provide immediate visual understanding of multi-objective optimisation processes. It has been widely used in consultancy and problem solving as a means of highlighting critical obsolescence information in an easy to understand form (Miyake et al., 2004) (Detre et al., 2006).

As discussed in the risk section, whilst the Obsolescence Impact Factor Chain helps to cover a range of appropriate factors, this can quickly become complex and costly and hence we adopt a simplified approach that assumes full support is provided by the IT service and focuses only on the criticality of the service and whether the technology is deemed obsolescent as defined by the client.

Continuing the algorithm started in the IT domain, it is possible to look at all the applications used to support a particular business service, at each of their EOES dates, which in turn are rolled up from infrastructure and products. We ask the question "are there any applications required by this service where the EOES date has already passed?". Where this is true, this obviously indicates that there is a degree of risk associated with the continued operation of that business service. The mapping of applications to business services can either be done via the organisation structure (i.e. for each organisational unit, determine which applications they use; and also which business services they provide) – used for our second study with the two police forces; or in the case of first study for a single police force, they were able to provide a direct correlation between applications and business services, as shown below.

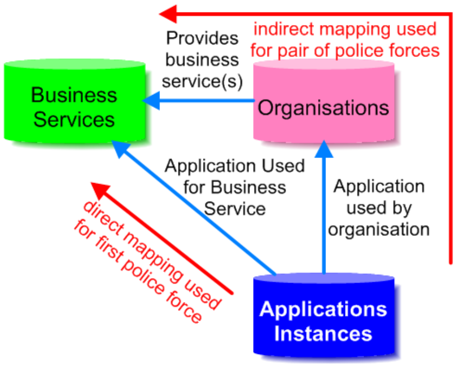

Business Services
Provides business service(s)
indirect mapping used for pair of police forces
Organisations
Application Used for Business Service
Application used by organisation
direct mapping used for first police force
Applications Instances

Figure 6: Obsolescence from Applications to Business Services.

However the mapping is done, the following algorithm was then used, which relies upon knowing the EOES dates for all the support applications, along with an indication of their criticality to the business (1 being the most important) (Fig.7).

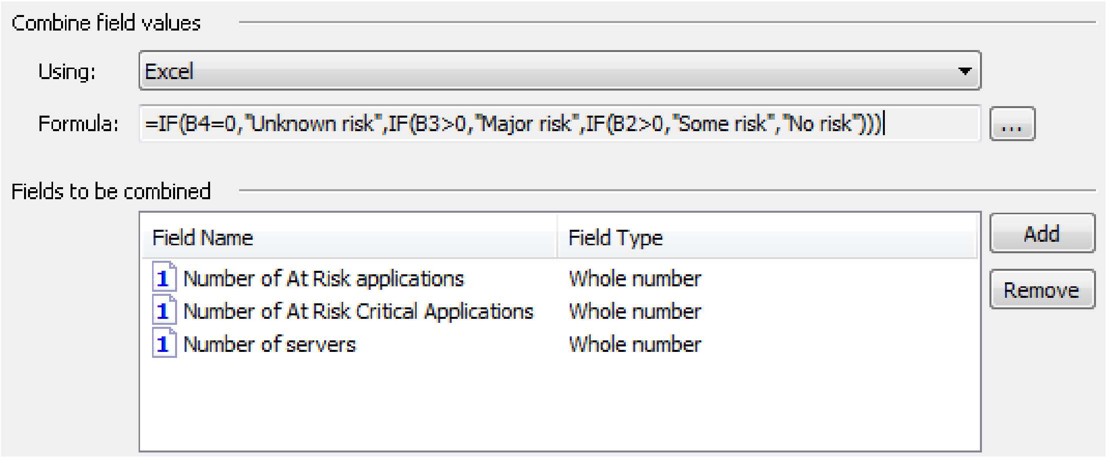
Like all of the algorithms in the model, this calculation was automated for all of the business services using the tool's ability to calculate and store intermediate results, including where necessary the ability to 'call out' to Excel. For example, the above algorithm looks like we can see in figure 8.

2.3.2 Risk Heatmap for a Police Force Requirement

By applying the above algorithm to each business service (from the PAG) in turn, it was possible to assign a risk value to each business service. The modelling tool was able to assign a colour to the business services dependent upon the risk value, and so the resulting heatmap looked like the figure 9.

```
FOR each business service
IF ∃ supporting applications of criticality 1 and EOES date in the past
THEN
       SET risk to MAJOR RISK
ELSE
    IF ∃ supporting applications of criticality > 1 and EOES date in the past
    THEN
        SET risk to SOME RISK
    ELSE
        IF we cannot associate any infrastructure with this service
              THEN
                SET risk to UNKNOWN RISK
              ELSE
            SET risk to NOT AT RISK
        ENDIF
    ENDIF
ENDIF
```

Figure 7: Algorithm for Calculating Business Risk in a Heatmap.



Combine field values

Using: Excel

Formula: =IF(B4=0,"Unknown risk",IF(B3>0,"Major risk",IF(B2>0,"Some risk","No risk")))

Fields to be combined

Field Name	Field Type
1 Number of At Risk applications	Whole number
1 Number of At Risk Critical Applications	Whole number
1 Number of servers	Whole number

Figure 8: Automated calculation of business risk using MooD®.

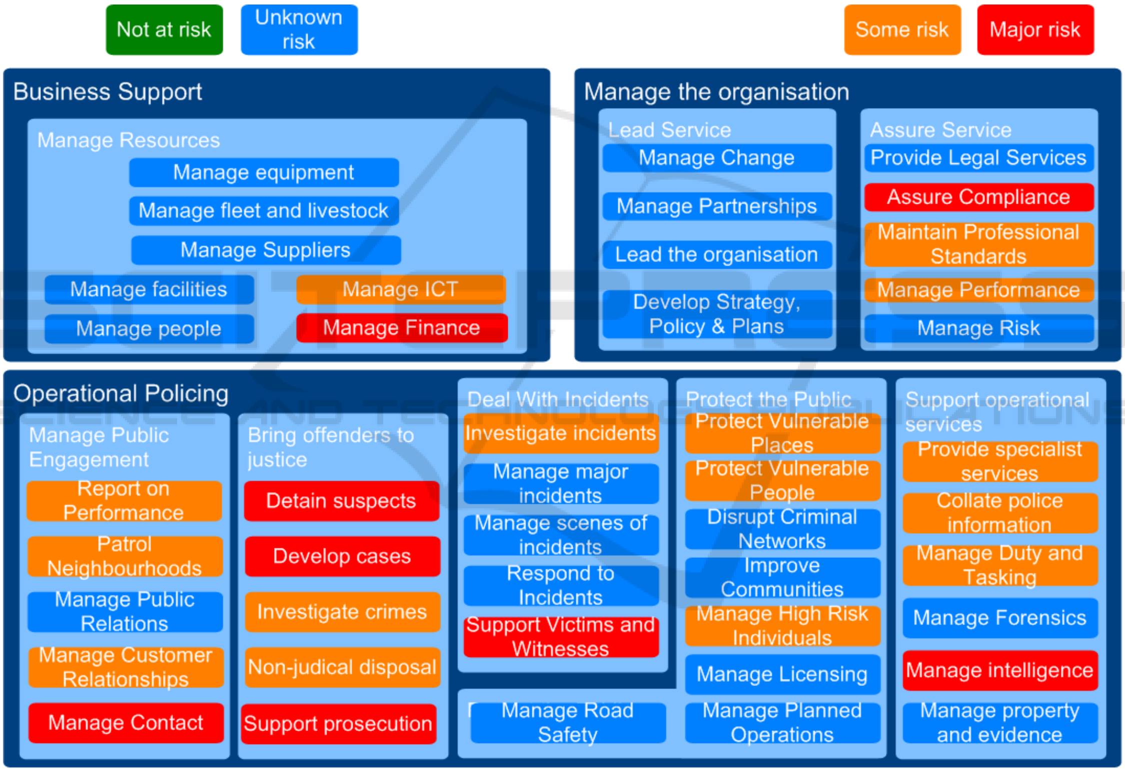


Figure 9: Police Business Services Risk Heatmap.

The value of this model lies in its ability to convey a technical concept (out-of-date products) and the link through the Enterprise Architecture model to business stakeholders in terms that are easy to understand and completely non-technical. Thus, this is a useful tool in demonstrating the risk component of the business case for making the necessary changes to the IT portfolio, to remove this risk.

3 LESSONS LEARNT

3.1 Building the Model

In order to carry out this kind of analysis, two things are needed: firstly, the raw information, with consistent terminology and all the relationships between the various kinds of information; and secondly, some kind of toolset to enable the import, analysis and reporting of that information. For organisations with a relatively mature EA function, the first of these should not present a huge challenge, however in many cases even getting the client to produce a single definitive list of applications is difficult. It is also difficult to see how this could be done without some kind of modelling and requirements capture tool. However, one approach we are exploring is the development of an ontology chart based on organisational semiotics principles. The MEASUR (Stamper, 1994) model approach offers a structured method to interview and model the ontology of an organisation and has been used in related work applying the techniques to enterprise architecture and consulting modelling frameworks (Liu et al, 2011). Excel can handle two- or perhaps three-dimensional data with the help of pivot data; complex meta-models such as Figure 3 are probably beyond the ability of such tools to handle. A more robust technology is required, ideally layered over some kind of relational database to ensure the integrity of the data. Some candidate tools can be seen in (Short and Wilson, 2011).

3.2 What We Got Out of It

The team involved in the project felt that by the end of the study, a good deal of evidence had been collected that gave a very strong business case to continue work with this client, to address the cost and risk issues identified so clearly by the work so far. In the subsequent study; a partial merger of two UK Police Forces, the approach from the first study was readily re-usable, using the easy to understand heat-map, even though the meta-model was significantly different for the merger scenario. The resulting heat-map for the pair of police forces was all red, due to a critical corporate application, used across the whole of the organisations that uses Oracle 8. This ‘all-red’ picture gave a very powerful and well-received message to the client about the urgency of the situation. The meta-model used for the second case study, built using lessons learnt from the first, omitted the infrastructure and technology catalogues, relating applications directly to underlying products. It also differed in that the linkage from applications to business services went via the organisation structure. This linkage was much simpler in the first study, going directly from applications to business services. Nevertheless, the heat-map was still able to be calculated in a similar fashion.

3.3 What the Client Got Out of It

The main deliverable being sought by the client, regarding obsolescence, was a view as to the motivation (business case) for making change. The use of the business heatmap, along with the TCO root cause analysis (shown above) and other financial information outside the scope of this paper, provided a clear business case at low cost. The approach and model are capable of being extended to accommodate increased technology and risk complexity if required.

4 CONCLUSIONS

Having used the approach successfully in two separate cases with very different meta-models, albeit both in the policing sector, we have concluded that the approach is readily re-usable.

The library of product obsolescence data captured during the first engagement was very useful in terms of shortening the research required during the second engagement to produce the obsolescence heat-map.

5 FUTURE WORK

In retrospect, the terminology used for some of the artefacts in the meta-model need further work. In particular, the word ‘technologies’ is perhaps misleading in the way it is being used in this kind of analysis. Further research is required of existing architecture frameworks and methods to identify more commonly used and industry accepted terms that enable new clients to quickly come up to speed. As mentioned we are considering ontological analysis for specific industry terminologies to identify the relevant terms (Guarino, 1998). Also we intend to review and expand the obsolescence impact factor chain and investigate how this could be embedded in developing architecture based consulting analysis frameworks, potentially using the Capgemini Integrated Architecture Framework or the BTS analysis framework (Liu et al., 2011) which has embedded structures for identifying the relationships between business services and IS services and their criticality.

TRADEMARKS

MooD is a registered trademark of Salamander Enterprises Ltd.

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle and Solaris are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

REFERENCES

Aversano, L., Esposito, R., Mallardo, T. & Tortorella, M. 2004. Supporting decisions on the adoption of re-engineering technologies. *Eighth euromicro working conference on software maintenance and reengineering (csmr'04).* Tampere, finland.

Boehm, B. 1999. Managing software productivity and reuse. *Computer,* 32, 111-113.

Bulow, J. 1986. An economic theory of planned obsolescence. *The quarterly journal of economics,* 101, 729-749.

Detre, J., Briggeman, B., Boehlje, M. & Gray, A. W. 2006. Scorecarding and heat mapping: tools and concepts for assessing strategic uncertainty. *International food and agribusiness management review,* volume 9.

Feldman, K. & Sandborn, P. 2007. Integrating technology obsolescence considerations into product design planning. *Proceedings of the asme 2007 international design engineering technical conferences & computers and information in engineering conference,* idetc/cie 2007.

Ginn, D., Streibel, B. & Varner, e. 2004. *The design for six sigma memory jogger : tools and methods for robust processes and products*, salem, nh : goal/qpc, cop. 2004.

Guarino, N. Formal ontology and information systems. Proceedings of fois'98, 1998 trento, italy. Ios press, amsterdam, pp. 3-15.

Halliday, S., badenhorst, k. & solms, r. V. 1996. A business approach to effective information technology risk analysis and management. *Information management & computer security,* 4, pp. 19 - 31.

Lagerstrom, R., Franke, U., Johnson, P. & Ullberg, J. 2009. A method for creating enterprise architecture metamodels - applied to systems modifiability analysis. *International journal of computer science and applications,* vol. 6, no. 5, pp. 98 - 120.

Lemer, A. C. 1996. Infrastructure obsolescence and design service life. *Journal of infrastructure systems*.

Liu, K., Sun, L., Jambari, D., Michell, V. & Chong, S. 2011. A design of business-technology alignment consulting framework. *Caise conference 2011.*

Miyake, M., Mune, Y. & Himeno, K. 2004. Strategic intellectual property portfolio management-technology appraisal by using the technology heat map. *Nri papers.* Nomura research institute.

Noran, O. 2003. An analysis of the zachman framework for enterprise architecture from the geram perspective. *Annual reviews in control,* 27, 163-183.

Npia. 2011. *Police activities glossary* [online]. Available: http://pra.npia.police.uk/ [accessed 7th april 2011 2011].

Opengroup 2009. The open group architectural framework (togaf 9).

Sandborn, P. 2007. Software obsolescence - complicating the part and technology obsolescence management problem. *Ieee trans on components and packaging technologies,* 30, 886-888.

Short, J. & Wilson, C. 2011. Gartner assessment of enterprise architecture tool capabilities. Gartner.

Solomon, R., Sandborn, P. A. & pecht, m. G. 2000. Electronic part life cycle concepts and obsolescence forecasting. *Components and packaging technologies, ieee transactions on,* 23, 707-717.

Stamper, R. 1994. Social norms in requirements analysis: an outline of measur. *Requirements engineering.* Academic press professional, inc.

Strnadl, G. F. Aligning business and it: the process-driven architecture model. Computer as a tool, 2005. Eurocon 2005.the international conference on, 21-24 nov. 2005 2005. 1048-1051.

Whelan, K. 2000. Computers, obsolescence, and productivity. *Ssrn elibrary*.

Wilkinson, L. & Friendly, M. 2009. The history of the cluster heat map. *The American statistician,* 63, 179-184.