

HEFCE Shared Services Feasibility Study

Proposed EMMAN Information Security Service

Final Report and recommendations



Author: Tony Brookes, University Of Derby. January/May 2008
Status: Final Report, as published to HEFCE May 2008

Table of Contents

1. EXECUTIVE SUMMARY	3
1.1. INTRODUCTION AND BACKGROUND.....	3
1.2. FINDINGS.....	3
1.3. RECOMMENDATION	4
2. BACKGROUND INFORMATION	5
2.2. STEALTHWATCH	5
2.3. EMMAN	5
2.4. INFORMATION SECURITY.....	6
2.5. METHODOLOGY	6
3. PROPOSED SERVICE DESCRIPTION	7
3.1. DEFINITION AND SCOPE	7
3.2. SERVICE NEEDS.....	7
3.3. SERVICE ELEMENTS.....	7
3.4. KEY SERVICE BENEFITS.....	9
3.5. PROMOTION	9
3.6. ORGANISATION AND SYSTEMS	9
4. CRITICAL SUCCESS FACTORS	10
4.1. INTRODUCTION	10
5. SPECIALIST TAX AND FINANCIAL ADVICE	10
6. EXISTING COMMERCIAL SERVICES AVAILABLE	11
7. FINANCIAL ANALYSIS	12
7.1. ESTIMATED COST OF PILOT AND SERVICE	12
7.2. THE KEY ASSUMPTIONS MADE IN THIS ANALYSIS	12
7.3. COST MODEL FOR AN INDIVIDUAL ORGANISATION.....	13
7.4. INFORMATION SECURITY INCIDENT COSTING	13
8. INITIATION MILESTONE PLAN	14
9. GOVERNANCE & MANAGEMENT	15
9.1. GOVERNANCE.....	15
9.2. MANAGEMENT	15
10. KEY RISKS AND CONTINGENCIES	15
11. SCALABILITY ISSUES	16
11.1. THE SCALABILITY ISSUES AND THEIR RESOLUTION, FOR THIS SERVICE ARE AS FOLLOWS:.....	16
11.2. SERVICE EXTENSION	16
12. FUNDING AND SUSTAINABILITY OPTIONS	16
12.1. FUNDING OPTIONS FOR THE PILOT.....	16
12.2. PROPOSED FUNDING OPTION	17
12.3. SUSTAINABILITY OPTIONS.....	17
12.4. SUSTAINABILITY PREFERRED OPTION	17
13. APPENDIX A FINANCIAL ANALYSIS TABLES	18
13.1. MULTI-YEAR PROFIT & LOSS FORECAST.....	18
13.2. CASH FLOW FOR PILOT BY MONTH	19
13.3. CASH FLOW FORECAST	20
13.4. DISCOUNTED CASH FLOW BY MONTH	21
14. APPENDIX B: EMMAN LTD OPERATIONAL STRUCTURE	23
15. APPENDIX C: EMMAN LTD GOVERNANCE STRUCTURE	24

1. Executive Summary

1.1. Introduction and Background

- 1.1.1. The HEFCE published the request for proposals on shared services in March 2007
- 1.1.2. The University of Nottingham submitted an expression of interest to the HEFCE for pilot funding of 72K based around the existing StealthWatch¹ capabilities in May 2007 comprising 1FTE and equipment. It should be noted that EMMAN, Nottingham Trent and Nottingham Universities are already using StealthWatch in their local networks and the MAN backbone. This existing investment is included in the financial analysis for the feasibility study.
- 1.1.3. The HEFCE then requested a feasibility study instead of a pilot, and offered funding of 25K covering a feasibility study, business plan development and specialist VAT & financial advice for EMMAN. The initial EMMAN terms of reference were agreed October 2007 with Nottingham, Loughborough, Derby, Lincoln and Nottingham Trent Universities, who had indicated their willingness to participate in the feasibility study work. In January 2008 work started on the study after Nottingham decided to participate and act as the lead Institution but was unable to lead the feasibility study, the University of Derby fulfilling that role.
- 1.1.4. Since then, De Montfort has also since participated in the study. EMMAN has provided the consultancy for the development of the business plan, with PKF providing the specialist VAT & financial advice. The FE community has also been consulted as part of the feasibility study.

1.2. Findings

- 1.2.1. All those consulted are aware that Information Security is a rapidly evolving pressure for their Institutions. By pooling their needs a shared service is likely to offer a better capability than each individual institution is able to afford.
- 1.2.2. The Information Security Shared Service for the East Midlands will help an organisation to better manage its information related risks and hence reduce the risk of significant information security failures, reduce the costs of its information security practice and increase the quality thereof.
- 1.2.3. There is strong support from all those consulted for EMMAN offering a shared information security service. It is seen as neutral and impartial and having a good awareness of academic needs by the majority of the community. Indeed the service as envisaged is innovative, combining monitoring, consultancy, sharing best practice, benchmarking, some forensic assistance and monitoring the Web to oversee the members on line reputation. (N.B. not all services will be available on the first day of operation as they will take some time to establish). The services will be supplied by a mix of subscription and consultancy model. This approach also uses the existing EMMAN management and governance structures with little additional overhead.
- 1.2.4. A combination of one or two Universities launching a similar service from their own IT departments are likely to fail as they would be initially lacking the reputation for integrity, impartiality and transparency that EMMAN already has; they would also need to develop the management and governance structures that exist in EMMAN.
- 1.2.5. The EMMAN board has agreed to support the service making it sustainable in the longer term. However the academic budget cycle means funding is unlikely to be available in the first twelve months of operation.

¹ StealthWatch is hardware and software used by EMMAN (and also Nottingham and NTU) to monitor network traffic in the backbone. Its main function is to alert the network staff to traffic that is "odd"- i.e. something failing or more sinister.

- 1.2.6. A mix of existing EMMAN facilities and HEFCE “pump priming” funding will enable the pilot service to be established. Initially the service will be provided by 2.5 FTE staff (technical/management and administrative) within the existing EMMAN structure and governance. Longer term, funding is expected to be 80% by subscription and 20% consultancy for existing EMMAN University Members. This initial mix of income streams will give a stable foundation for the shared other customers (FE Colleges, Research organisations and the wider public sector) who will have their subscription and consultancy costs and mix agreed by individual negotiation.
- 1.2.7. FE and other organisations connected via EMMAN are seen as the other natural initial service customers. It is expected that the service will grow via other educational organisations and the wider public sector initially in the East Midlands. The service is not limited to the East Midlands and might be replicated in other areas; potentially nationally.
- 1.2.8. Potential cost savings per institution have been identified comparing the costs of the shared service and that of establishing a similar facility in house. The service is expected to save approximately 20 to 60k per HEI per annum, an overall total of over 160k pa.
- 1.2.9. Other non financial benefits identified include helping service users to reduce the risks of running complex network and network dependant services; being able to demonstrate that to the auditors; benchmarking, best practice, information and learning sharing; and generally helping the organisations to protect their reputations in a fast moving technological area.
- 1.2.10. The service as envisaged is not currently available commercially from a single source especially in the East Midlands. This point is considered further in section 6.
- 1.2.11. The proposed service has natural steps in scaling up its operations (people, equipment, network limits and geographical area covered) that are considered in detail in the section on scalability issues, section 11.1. Simply put, the number of technical staff will need to increase in line with the number of service customers, the rate at which this is achieved is not at the same rate as the technology used nor the supply of the service to remote (i.e. non EMMAN connected) customers. It is straightforward to replicate onto other MANs providing they have a similar level of cooperation and trust between the members. It is possible to envisage a mixed economy (EMMAN monitoring other StealthWatch probes in remote MANs) but developing a full business plan for potential national expansion was seen as outside the scope of this report.
- 1.2.12. The full cost of a pilot/start-up phase starting in August 2008, for 15 months, is circa £250k, with the service being self-sustaining from October 2009.
- 1.2.13. If the HEFCE do not fund the pilot service, then it is considered unlikely that the service would be established as envisaged. A reduced service established later might follow if initial funding could be agreed locally.

1.3.Recommendation

- 1.3.1. The HEFCE Shared Services Group should invest a sum of £190k to “kick start” the shared service in the East Midlands, that sum being 74% of the start up costs. The rest being supplied by EMMAN as it has agreed to supply equipment and services of circa £60k (26%).
- 1.3.2. The service will provide the EMMAN community of 9 HE and circa 35 research and FE organisations with best-in-class information security services across the data network at a fraction of the cost compared to an individual organisation attempting to provide similar services for its own use. Extension of the service once established in both business terms and geographically is considered further in section 11.

- 1.3.3. Note: Should the funding not be granted then there is a medium to high risk of the individual Institutions servicing their information security needs via the commercial market. This will incur higher costs. Alternatively they could recruit their own staff or establish a reduced shared service depending upon the funding that can be provided. In any case there is likely to be a delay before any decisions are reached. The study has shown there is an opportunity to establish the shared service as outlined.

2. Background information

- 2.1.1. A short background and introduction to the main concepts, regional structures, groups and technology proposed in this report

2.2. StealthWatch

- 2.2.1. StealthWatch is a commercially available product² comprising hardware and software to allow its users to monitor network traffic to understand the traffic flows and their purpose.
- 2.2.2. The hardware device EMMAN use to monitor the MAN Traffic overall can also be used on the inside of an Institution's network to similarly monitor network traffic there (as Nottingham and Nottingham Trent Universities have done in this region).
- 2.2.3. A slightly less featured analysis of the internal network traffic of an institution can be carried out by routing the internal traffic information from the core network routers to a StealthWatch probe on the MAN. Depending upon how many Institutions decide to implement this, there is a point at which an additional probe (£32k) would be needed during the pilot phase.
- 2.2.4. EMMAN has negotiated a purchasing framework with Khipu Networks,³ the UK supplier of the system for discounted hardware, software and training that is available to all EMMAN members.

2.3. EMMAN

- 2.3.1. The East Midlands Metropolitan Area Network, is the Regional Network Operator contracted by JANET(UK) to deliver the national educational Internet service in the East Midlands.
- 2.3.2. EMMAN does not employ any staff directly; instead it contracts for a service to be delivered from one or more member Universities. At present 10 staff (6 FTE) are employed by four contracted Universities to deliver the existing EMMAN service. Often the individual staff combines EMMAN work and their employing Universities work as part of their contract of employment. It is expected that any staff needed to deliver the proposed shared service will therefore be employed by a University in the region. They will deliver a service as described in a service contract between EMMAN Ltd and that University.
- 2.3.3. EMMAN is run operationally by a group called the managing agents, drawn from Nottingham, Nottingham Trent University and others, under contract from EMMAN Ltd. It is a company limited by guarantee. It has a board of directors of whom the majority are either directors of service or Pro-Vice Chancellors. There is also a management committee comprised of senior IT managers from the members including FE representation. A technical committee meets to advise on specialist issues as well. Diagrams of the operational and governance structures are contained in Appendices C and D.

² See <http://www.lancope.com/products/> for more details

³ See <http://www.khipu-networks.com/home/default.asp> for more details.

- 2.3.4. The subscribing members who jointly established the service are the eight Universities in the area⁴. The service has since been extended to Bishop Grosseteste University College and circa 35 FE Colleges and research organisations.

2.4. Information Security

- 2.4.1. Information security is the name of that specialist area of risk management primarily focussing upon the confidentiality, integrity and availability of information. It is one of the younger areas of specialism within IT and is in the process of establishing itself as a profession. The public perception is of a highly technical area of work often with government or military overtones reflecting the history of its development.
- 2.4.2. In fact, the work ranges from the technical, as shown by the StealthWatch element of the proposed shared service, to policy and process development showing organisations how best to ensure their staff and students behave in a ways so as to minimise the chances of a loss of information or access to that information by authorised users. Sometimes, as much as 80% of the work is non technical; i.e. it is people focussed. The work frequently extends into business continuity, IT audit and risk management. University auditors are increasingly interested in the effectiveness of the information security arrangements of the organisations such is the potential impact should such work be proved ineffective.
- 2.4.3. There are many reports published world wide trying to present an overview of the state of information security today, especially in the present era of Internet everywhere, social networking and on-line business. Indeed such is the importance that HMG attach to the issue, the cabinet office sponsor a whole range of work in this area, and the BERR (DTI as was) sponsor an annual report the Information Security Breaches Survey 2008, available from⁵ as a national annual benchmark.
- 2.4.4. Within the East Midlands, EMMAN has already established a peer group of Information Security staff that meet quarterly to share experiences and best practice, this approach will be strengthened and extended as part of the shared service.
- 2.4.5. Universities have an academic role in teaching and research in this area and it is possible that some of the consultancy will be supplied from that source. At least 35% of Universities in the UK have specialist Information Security support staff in post, as an email survey found 18 months ago.

2.5. Methodology

- 2.5.1. A steering group largely made up from members of the EMMAN management committee who are mainly senior managers of IT services in the region's Universities has guided the direction of this study. The business case working group with membership from specialist technical staff from the majority of the subscribing Universities devised the services they need. An EMMAN business consultant has drawn the information together into a business case upon which this final report is heavily based.
- 2.5.2. Additionally the East Midlands Regional Support Centre facilitated a discussion with senior IT managers from regional FE Colleges about the proposed service.

⁴ The Universities of De Montfort, Derby, Loughborough, Leicester, Lincoln, Nottingham, Nottingham Trent and Northampton.

⁵ http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html

- 2.5.3. The feasibility workshop group, the feasibility project steering group and the HE board members of EMMAN are fully supportive of the initiative and have declared their willingness to participate once the pilot project has been undertaken and the budget in the 2009 academic year become available.
- 2.5.4. It has been noticeable that the carrying out of this study has promoted closer working between members in the region and it is likely that other efficiencies will follow this work particularly if the pilot scheme is funded. Examples are disaster recovery, email security and shared data centres.

3. Proposed Service Description

3.1. Definition and Scope

- 3.1.1. Objective: The purpose of this shared service is to significantly reduce the cost of operating a high quality information security service in an organisation.
- 3.1.2. The services described in this report regard StealthWatch as the technical foundation of the service funded by subscriptions, with the other work also being carried out by the two technical staff usually charged as consultancy. The best mix of work and funding will be determined during the pilot phase.
- 3.1.3. The foundation work needs to be delivered in a dependable and reliable way to customers; the elective work is best carried out as consultancy especially as the exact timing is expected to be negotiable.
- 3.1.4. Two technical staff are considered the minimum necessary to deliver the service throughout the year allowing for staff absences.

3.2. Service Needs

- 3.2.1. The services to be provided address the information security issues that give rise to common problems for a HE institution of:
 - 3.2.1.1. Cost of prevention and remedial actions considering own service provision vs collaboration vs outsource
 - 3.2.1.2. Compliance for legal and audit
 - 3.2.1.3. Protection of an Organisation’s reputation
 - 3.2.1.4. Balancing information security with Academic use
 - 3.2.1.5. Maintaining critical mass of specialist skills
 - 3.2.1.6. Visible collaboration across the sector
 - 3.2.1.7. Providing best value services

3.3. Service Elements

- 3.3.1. The information security service to be delivered will ultimately comprise the following service elements, the exact mix and proportion being determined in the pilot phase. Their likely funding mechanism is indicated by S (Subscription) or C (Consultancy).

Service Element	Purpose	S or C	Description
Monitor Network Activity	Collect network traffic data and statistics	S	System level automatic recording of traffic data and presentation of activity levels
Analysing Network Activity	Identification of abnormal network traffic and activity	S	Manual review and analysis of statistics and alerts raised

Service Element	Purpose	S or C	Description
Management Alert of activity	Ensure user management aware of abnormal network activities and possible sources/causes	S	Management reporting and escalation procedures.
Management Alert of potential issues	Prevention of security breaches from a known source/activity/configuration	C	Assessing, known threats, trends and solutions on the network. Reporting to user management as needed.
Intelligence gathering and notification	Prevention of security breaches from a known source/activity	S	Scanning for, and assessing, known threats, trends and solutions in the information security industry. Reporting to user management as needed.
Forensic Investigation	Identify causes and sources of an incident	C	Provision of specialist expertise to supplement and/or complement user investigative resources.
Incident Remediation	“Clean up” following an incident	C	Provision of suitably qualified expertise to supplement and/or complement user restoration resource needs.
Information and Security Helpdesk	Single point of contact for user operational communications and incident/issue management	C	Help desk to provide immediate answers where possible and to track progress and escalate issues to other resources/management as needed, with an audit trail.
Anonymous Performance and Benchmark Info	To enable users to understand and compare their performance to best practise	S	Collation, analysis and reporting of suitable statistics.
Web Reputation Monitoring	To identify web based information and sources that may damage the reputation of the institution	C	Scanning for, monitoring and reporting on relevant website/blog/email content
Training Info Security Staff	Maintain skills level in user community	S	Develop and deliver relevant training courses as needed
Implementation Consultancy	Provide best practice advice and support users	S	Maintain knowledge and skills to provide consultancy to users as needed
Network “Health Checks”	Provide independent network security assessment report	S	Assess and report on the information security systems, processes and procedures with recommendations for improvement.
Best Practice advice	To enable users to implement best practice in their information security systems and services	S & C	Assess, advise and/or deliver and report on the evaluation, selection, implementation and management of information security systems and services

3.4.Key Service Benefits

The key service benefits are in three main areas of information security:

3.4.1. Future Cost Reduction

- 3.4.1.1. The shared service is a lower cost alternative to individual in-house provision for each institution
- 3.4.1.2. It reduces the cost of compliance to members' and auditors' information security policies
- 3.4.1.3. It reduces the cost of forensic investigations of suspected breaches of security
- 3.4.1.4. It encourages economies of scale by demand aggregation.

3.4.2. Quality Improvement

- 3.4.2.1. Develop benchmarks using anonymous reporting, and establish best practice for dealing with and preventing such incidents.
- 3.4.2.2. The dissemination of shared learning across the membership
- 3.4.2.3. Increasing the resilience of the members Information Security service by providing a wider pool of experienced specialist staff for members to call upon.

3.4.3. Risk Reduction

- 3.4.3.1. Prevention by prediction of security threats
- 3.4.3.2. Protect organisational reputation of the members

3.5.Promotion

3.5.1. Promotion of the services will initially be targeted on the current EMMAN community of organisations and using the existing EMMAN marketing resources. Once the pilot service is established, the targeting of the wider public services community, and possibly the commercial sector, can be undertaken using the following approaches

3.5.2. Collateral

- 3.5.2.1. Brochure service details
- 3.5.2.2. Mailer content
- 3.5.2.3. Newsletter content
- 3.5.2.4. Website/Internet content

3.5.3. Marketing Activities

- 3.5.3.1. Email
- 3.5.3.2. Internet based channels (Blogs/Wiki etc)
- 3.5.3.3. Specialist interest groups initiation and contribution
- 3.5.3.4. Workshops
- 3.5.3.5. Exhibitions
- 3.5.3.6. Conferences (Organiser, Speakers and Delegates)
- 3.5.3.7. Commissioned research projects
- 3.5.3.8. Individual sales meetings
- 3.5.3.9. HEFCE sponsored Shared Services events and activities
- 3.5.3.10. UCISA and JISC events and activities

3.6.Organisation and Systems

3.6.1. To manage the proposed service, the two technical staff, (both relatively senior) have an added provision of 0.5 FTE of management and admin support. The team will report to the EMMAN Executive Director, as shown in the charts in Appendices C and D.

3.6.2. This small team approach has been created to minimise the management load on the Executive Director, and to ensure a focus is maintained on the team's role and service delivery. More detailed, second-level and top-up support for the services will be supplied under contract from the specialist information security teams that exist in some of the member organisations

- 3.6.3. Operational and administrative systems will need to be specifically put in place for the regular monitoring and reporting activities required to operate and manage the service. These systems will make use of existing systems and methods where appropriate, but some specific development/deployment will be required for the detailed specifics of delivering the services.

4. Critical Success Factors

4.1. Introduction

- 4.1.1. The following factors were identified at the start of the feasibility study by the working groups as needing to be achieved before the shared service could be considered successful. The first two can be considered to have been met.
- 4.1.2. The service must provide the quantifiable benefits that the EMMAN membership need.
- 4.1.3. Longer term sustainability of the recommended service.
- 4.1.4. The HEFCE Shared Services Group agrees to fund the pilot service.
- 4.1.5. The service elements must be attractive, in the longer term, to the wider public sector.
- 4.1.6. The service must be seen as independent, trustworthy, dependable and transparent as demonstrated by a survey in the post pilot service implementation review.

5. Specialist Tax and Financial advice

- 5.1.1. As part of the feasibility study, specialist Corporate Tax and VAT advice was sought regarding how EMMAN should account for the shared service so that any consequent Tax burden is minimised. The advice received was:-
- 5.1.1.1. That the information security shared service should be part of EMMAN, there are no tax or VAT advantages to setting up a separate or subsidiary company. EMMAN is VAT registered and therefore charges VAT on all sales.
- 5.1.1.2. VAT is, at present, chargeable on all sales to Universities and other customers. However, it may be possible for EMMAN to discuss VAT exempt treatment with HM Revenue & Customs⁶. This is an issue for the EMMAN board to follow up outside of this study as it would apply not just to this service, but also to other EMMAN services.
- 5.1.2. It should be noted that EMMAN, because of its primary status as a company limited by guarantee and engaged in mutual trading for the benefit of its members also engages in straightforward trading. This “mixed economy” is subject to corporation tax on its commercial trading activities. Should EMMAN become VAT exempt then this will alter the VAT recovery and possibly the corporation tax regimes. There is a complex interplay between these issues that will need careful consideration and it may not be beneficial to EMMAN to change its tax status. This is an issue for the EMMAN board to consider as a result of this study.
- 5.1.3. If it is possible to reduce the VAT burden on Universities and other educational organisations then that would be welcomed. However, it should be noted that EMMAN is just beginning to supply services outside the educational area and that may complicate the handling of the issue.

⁶ It should be noted that there are no clear precedents in this area of case law, hence negotiations with HMRC may be protracted and involve further advice from tax specialists.

6. Existing Commercial Services Available

- 6.1.1. No single company currently delivers the range of services envisaged in the proposed shared service, though there are a wide range of commercial activities available supporting various aspects of Information Security.
- 6.1.2. There are so many sources of information available at a detailed level that it is too easy to get overwhelmed, and one of the aims of the proposed shared service to set up a single dependable source. Some government inspired initiatives would seem to suit EMMAN, e.g. WARP⁷, and possibly⁸.
- 6.1.3. Collaborative commercial services are rare, though this model is often seen in the NHS and other public sectors.
- 6.1.4. Commercial consultancy costs are in the range of £400 per day for general consultancy (usually by hiring a contractor for a few weeks) to £2,500 per day for specialist technical services in the information security area.

Service	Commercial approach	EMMAN Shared Service
Monitoring network activity	Commercial purchase (1)	Included.
Alerting management of unusual network activity	Commercial purchase (1)	Included.
Intelligence gathering and notification of issues and trends	Commercial purchase(2) or free sources	Included.
Incident remediation (including virus mop-up etc)	Commercial purchase (3)	Included.
Providing anonymous network security performance and benchmark information	Commercial purchase (4)	Included.
Training for information security staff	Commercial purchase (5), academic courses, Professional bodies	Included.
Independent network security "health checks" to support audit requirements	Commercial purchase (6)	Included.
Analysing network activity	Commercial purchase (1)	Included.
Alerting management of potential security threats	Commercial purchase (1)	Included.
Forensic investigation support	Commercial purchase (6)	Included.
Information security and incident helpdesk	Commercial purchase (7)	Included.
Web reputation monitoring and reporting	Commercial purchase (8)	Included.
Security Implementation best practice advice and support consultancy	Commercial purchase (6)	Included.
Providing best practice advice in evaluation, selection,	Commercial purchase (6)	Included.

⁷ <http://www.warp.gov.uk/Index/indexintroduction.htm>

⁸ http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Informationsecurity/DH_4015419>

Service	Commercial approach	EMMAN Shared Service
implementation and management of information security services		

The table shows as many as eight companies could be needed (depending upon the exact mix of services offered) to supply a similar service to that proposed.

7. Financial Analysis

7.1. Estimated Cost of Pilot and Service

- 7.1.1. The total needed to set up the pilot scheme is 250k of which £190k is being requested from HEFCE and £60k from EMMAN. Appendix A contains the detailed financial analyses: a three year cash flow for the service, pilot and service cash flows, a Profit & Loss and a discounted cash flow. Section 7.3 contains a detailed list of assumptions made in this study.
- 7.1.2. In the preparation of the business plan, which is a separate document to this report, varying numbers of staff were considered. After discussion within the business plan working group, two FTE technical staff were considered the minimum number to be sustainable within the existing EMMAN community.
- 7.1.3. Remote testing of networks and services, known as penetration testing or sometimes as network health checks is beginning to be required by auditors. It is often priced at the upper end of the scale and would be offered as a separate consultancy service. To establish credibility in this area of work, it is likely that the proposed shared service will need both the staff that carries out the work and EMMAN to meet external standards. The CREST approach seems the most likely⁹ as does the use of OSSTMM¹⁰.

7.2. The key assumptions made in this analysis

- 7.2.1. The service will be self-financing by the end of the pilot
- 7.2.2. Subscription based services will be 80% of annual revenue
- 7.2.3. Call-off consultancy packages/subscriptions will be available
- 7.2.4. Subscriptions are paid annually at the start of the subscription period and synchronised with EMMAN billing schedules
- 7.2.5. The price of the services is based on balancing a cost-per-fte basis that includes all costs required to operate the services
- 7.2.6. Salaries are based upon current staff salary levels for existing university staff performing similar skilled functions
- 7.2.7. Contract staff costs are based upon member organisations' current charging rates for such skills
- 7.2.8. Hardware and software costs are based upon current EMMAN agreement discounts with relevant vendors
- 7.2.9. Helpdesk services will be within current operation of EMMAN helpdesk. EMMAN is working towards a mix of office hours and call out to cover Monday/Friday 0800 – 23.59; Weekends 0900 – 23.59, including the majority of Bank Holidays.

⁹ <http://www.crest-approved.org/Pages/RequiredMembership.html>

¹⁰ See <http://www.isecom.org/osstmm> for the Open Source Security Testing Methodology Manual

7.3. Cost Model for an Individual Organisation

7.3.1. The costs for an organisation to provide such information security for itself can be seen as follows:

Item	Description
Income	Member institutions will be able to pay after Aug 2009 (next budgeting year)
Staffing	Specialist Staff: 2.0 fte = 1 x £50k + 1 x £30k Management and admin staff : 0.5 fte = 0.5 x £40k
Staff Training	Specialist staff @ 4 weeks/person @ £2k/week
Recruitment	Circa 15% of 1st year salaries
Marketing	Activities: Setting up 2 events and attending 4 events Collateral: Informational material
Travel	Expenses @ 2.5 days/week @£20/day for each specialist = circa £6k
Office	Space: Based on small sized serviced office space charges. Equipment: Basic phones etc. Consumables: Includes technical manuals
Legal and Professional	Advice and preparation: T's & C's, Licenses, Contracts, Prof. Indemnity and other insurances (bearing in mind specialist nature of such services)
Maintenance	10% of hardware/software purchase price
Hardware Systems and Network	Central StealthWatch system £54k (Supplied by EMMAN) as an in kind contribution 2 x laptop and 2 x Desktop = £4k Upgrade to central StealthWatch system to cater for increasing traffic volume £32k
Additional Software	Standard office software to be made available under educational agreements. Specialist software: StealthWatch and Snort - circa £3k/specialist = £6k

7.3.1. An estimate of the costs that would be incurred by the EMMAN members to establish their own service would therefore be 6*(53k) or 318k pa, and 32k hardware upgrade (N.B. Two Universities already have these facilities).

7.3.2. The overall cost savings with the shared service are 161k pa longer term.

7.4. Information Security Incident costing

7.4.1. Like most risk management based incident or event based costing it would be much easier to estimate these figures in a retail environment. Never the less, an attempt at such an estimate will be made to try and quantify the cost benefits of such a service.

7.4.2. The highest impact incident is where a whole institution cannot use the IT infrastructure for a sustained period of time and many people are needed to help in the clear up afterwards. An example might be a virus infection. Thus a medium size site with 1000 staff and their PCs that are down for two weeks, that takes an hour per PC to clean up will cost: 1000 (staff) x 10 (days) x 15 (£ per hour of wasted staff time) or £150k in wasted staff time, with the tidy up being 25 (people needed to clean up PCs) x 11 (£ per hour) x 2 (weeks) x 37(hours/week) or £20,350 to ensure each PC is working. Note there has been no attempt to quantify the "cost" of the reputational damage that would also result.

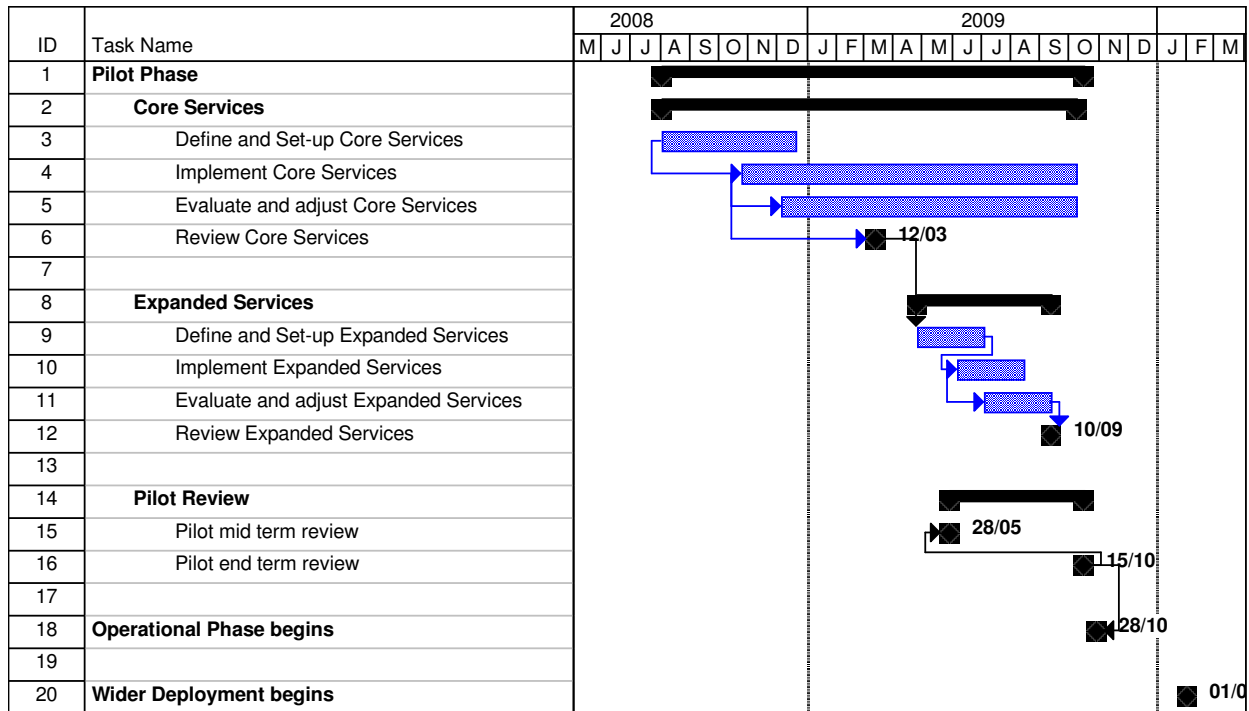
7.4.3. Trying to contain reputational damage via detrimental website comments usually takes one to two weeks of one or two staff time to identify and then deal with. This is likely to cost 5 x 400 plus 5 x 1000 or £7k.

7.4.4. A simple hacking attack, e.g. defacing a web page, if successful can involve the rebuilding of one or two web servers, and assuming external staff need to be used will cost 5 x 400 or £2k.

- 7.4.5. A more complex attack on an administration or finance system for example is likely to cost three to five times the last example (i.e. £6 – 10k) for the IT elements alone, the impact via fraud is outside the scope of this approach.
- 7.4.6. The potential forensic work envisage may have different purposes: one or two days advice to an organisation about how to proceed with such work in support of a staff disciplinary investigation and (possibly £3k if purchased commercially), or carrying out the detailed work needed to analysis exactly what has been done on that computer by a member of staff or a student most likely one or two weeks (say £15k for two weeks).
- 7.4.7. Business interruption insurance can cover the financial losses, for some of these incidents, though the insurance company will impose minimum conditions before underwriting such insurance and will most likely raise the premiums of any organisation that make repeated claims.

8. Initiation Milestone Plan

- 8.1.1. The following plan outlines the major phases, work streams and review points required to go beyond a pilot and implement sustainable and scalable shared services for the East Midlands HEFCE community.
- 8.1.2. The plan shows the start of implementing the core services following the August start of year peak for Educational sector and runs over the following year’s intake period to compare the effectiveness and impact of the service over a critical period for the HE sector.
- 8.1.3. The plan also assumes the following:
 - 8.1.3.1. Initial 3 month period to recruit staff and set up
 - 8.1.3.2. Initial 12 month contract for pilot staff
 - 8.1.3.3. HEFCE sign-off pilot and commit to initial funding by August 2008



9. Governance & Management

9.1. Governance

9.1.1. It is proposed that governance of this new service is delivered by using the existing EMMAN¹¹ structures. The current governance structure of board and focused management committees would be able to accommodate the governance of the provision of the shared information security service. Appendix C has a diagram showing this structure.

9.2. Management

9.2.1. It is proposed that the management of the shared security service also be handled within the existing structure of EMMAN. The shared information security service would be managed in the same manner as existing operational management, but with a specialist information security group reporting directly to the current executive director of EMMAN. Appendix B has a diagram showing this structure

10. Key Risks and Contingencies

Risk Description	Likelihood	Impact	Risk Rating	Mitigation
There is a risk of insufficient financial commitment from the EMMAN membership which is caused by being unable to commit the funds needed to sustain the service that will result in the service being scaled back.	Low	Very High	Medium	Will require revision of service and cost options but may result in bringing forward the broadening of the service to FE Colleges and other public sector organisations
There is a risk of being unable to recruit critical specialist skills which is caused by short term contracts being offered to staff resulting in service failure.	Low-Medium	High	Medium	Some member institutions will make staff and skills available to aid training and accelerate learning as appropriate. Also the pilot scheme has been designed to last 15 months to allow the staff contracts to be 12 months in duration.
There is a risk of service demand outstripping supply which is caused by having more work than staff. This will result in unhappy customers and a loss of confidence in the service.	Low-Medium	High	Low	Service will be managed within the constraints of the quantity of specialist resources allocated to provide the service. Additional resources will be added to match the medium to long-term forecast of demand as long as such levels are commercially sustainable.
There is a risk of the pilot not going ahead which is caused by insufficient funds from HEFCE which will result in the scheme being delayed or cancelled.	Medium	High	High	None possible in the same timescale. It may be possible to proceed with a self funded scheme scaled back from the proposed service at a later date if sufficient funds can be made available.
There is a risk that HEFCE will suffer reputational damage caused by being seen to use	Low	High	Medium	Thought unlikely as the same issue has not caused any comment with the creation of the MANs and their intended

¹¹ A company limited by guarantee.

public funding to set up a commercial company.			commercial trading. If the pilot does go ahead, then SME's and larger commercial companies are unlikely to be actively targeted (see 12.3.5).
--	--	--	---

11. Scalability Issues

11.1. The scalability issues and their resolution, for this service are as follows:

- 11.1.1. During the pilot and into the longer term operation of the service, there is a need to maintain and develop the specialist skills possessed by the two technical staff to match the demand for the service. Whilst training costs for staff have been included in the financial plan, it will be during the pilot period that a clearer picture of the actual demand and profile of the skills needed to deliver the service can be determined.
- 11.1.2. Additional skilled staff will be available to deliver consultancy. It is assumed that existing member staff already trained in some of the service elements will be made available on a contract basis to supplement and complement the EMMAN core skills.
- 11.1.3. The limiting factors of the StealthWatch technical environment are:-
 - 11.1.3.1. Server scalability to match network traffic monitoring levels
 - 11.1.3.2. Number of devices to monitor
- 11.1.4. One extra University subscription beyond the initial EMMAN members is unlikely to need extra staff or equipment, however three or four may need one additional member of staff and at approximately six extra subscriptions extra equipment will be needed. The EMMAN shared service could be extended nationally, an approach considered in the next section.

11.2. Service extension

- 11.2.1. To extend the service outside the EMMAN area can be carried out in two different ways depending upon the other regional network operators' choice.
- 11.2.2. The service can simply be replicated to another MAN area, possibly with some consultancy from EMMAN during the initial stages.
- 11.2.3. Alternatively, provided a StealthWatch probe is located within the JANET or other Internet supplier's feed of the interested Institution, the monitoring and other shared services could be delivered via EMMAN. There is a geographical limit to the distance that people can cost effectively travel to deliver on-site services.
- 11.2.4. These options have not been investigated in depth as they are considered outside the scope of this study. It should be noted that two other regional operators are considering a StealthWatch installation. Their names have been deliberately omitted as until their commercial negotiations are completed the discussions are considered confidential.

12. Funding and Sustainability Options

12.1. Funding Options for the Pilot

- 12.1.1. The financial plan has been produced on a full cost basis for a pilot project and is the basis for the funding options identified.
- 12.1.2. **Pilot Option 1 - Funded 100% by HEFCE**, with the HEFCE provide the full funding £250,000 as indicated in the financial plan for the full period of the pilot until the final pilot review. Probability – low.

- 12.1.3. **Pilot Option 2 - Funded 100% by EMMAN and its Members**, A contribution matrix of some description would need to be created to enable EMMAN members to establish and agree their ability and level of financial contribution for such a project. Budgets for 2008/09 are now set, and therefore it will be very difficult to get agreement to an increase at this point Probability – very low.
- 12.1.4. **Pilot Option 3 - Funded by The HEFCE + EMMAN and its Members** Specific contributions of equipment and facilities could be made by EMMAN and some of its members to reduce the balance of funding needed from HEFCE to make the pilot viable. With an overall cost of the pilot of circa £230,000 and a contribution from EMMAN and its members of circa £60,000, then HEFCE would need to fund circa £190,000 (76%) of the costs of the pilot. Probability medium – high.
- 12.1.5. **Pilot Option 4 - Funded by HEFCE + EMMAN + Members + Others**, similar to option 3, this option requires the availability of other styles of funding from other organisations, possibly both commercial and public sector. Commercial vendors with an interest in the project together with EMDA have been approached with no positive result to date. Probability Low.

12.2. Proposed Funding Option

- 12.2.1. The most likely option to be equitable and effective for all parties is option 3 and that is the option proposed for funding the pilot project.

12.3. Sustainability Options

- 12.3.1. These options look at how the post-pilot skill/people/technical/equipment/financial resources needed to maintain and possibly grow the service could be secured during the pilot phase.
- 12.3.2. **Sustainability Option 1 - EMMAN + EMMAN community funded.** This would require sufficient take up of the subscription and ad-hoc services by the EMMAN community to cover the costs of the service. Probability – medium
- 12.3.3. **Sustainability Option 2 – EMMAN + EMMAN community + Other HE.** This would require a “centre of excellence” style of service to be made available on a fee paying basis to other HE organisations around the country that don’t have access to the skills and facilities that this service will create in the East Midlands. Probability – medium
- 12.3.4. **Sustainability Option 3 – EMMAN + EMMAN community + Other HE + Public Sector.** This option would see the services, particularly the skills based services, being promoted to the wider public sector community within and without the East Midlands area. Probability – medium to high
- 12.3.5. **Sustainability Option 4 – EMMAN + EMMAN community + Other HE + Public Sector + Commercial.** This option takes option 3 one stage further and encompasses the potential for such specialist skills to be attractive to some of the medium to large size commercial organisations. In recognition of the risk identified to HEFCE’s reputation from the potential use of public funds to fund a commercial company, EMMAN will not actively pursue this option until after the service is established. Probability – medium to high.

12.4. Sustainability Preferred Option

- 12.4.1. The preferred approach has been identified as option 3 as this is the option most likely to succeed with the potential scope to evolve to option 4 contingent upon financial and political circumstances at the time.

13. Appendix A Financial Analysis tables

13.1. Multi-Year Profit & Loss Forecast

	Aug 08 - - Oct 08 £	Nov 08 - - Jan 09 £	Feb 09 - - Apr 09 £	May 09 - - Jul 09 £	Aug 09 - - Oct 09 £	Nov 09 - - Jan 10 £	Feb 10 - - Apr 10 £	May 10 - - Jul 10 £	Total £
TURNOVER									
Subscription Services	-	-	-	-	145,000	-	-	-	145,000
Consultancy and ad-hoc Services	-	-	-	-	-	5,000	7,000	10,000	22,000
Health Check Services	-	-	-	-	5,000	-	5,000	10,000	20,000
	-	-	-	-	150,000	5,000	12,000	20,000	187,000
DIRECT COSTS									
Specialist Staff Direct	-	19,265	19,264	19,265	20,252	20,251	20,251	20,252	138,800
	-	19,265	19,264	19,265	20,252	20,251	20,251	20,252	138,800
GROSS PROFIT	-	(19,265)	(19,264)	(19,265)	129,748	(15,251)	(8,251)	(252)	48,200
OVERHEADS									
Staff Salaries	5,007	5,008	5,007	5,008	5,191	5,191	5,190	5,191	40,793
Recruitment	15,000	-	-	-	-	-	-	-	15,000
Training	-	4,000	4,000	4,000	4,000	4,000	4,000	4,000	28,000
Marketing	3,750	1,250	3,750	1,250	4,375	1,875	6,875	1,875	25,000
Office	2,490	1,490	1,490	1,490	2,740	1,740	1,740	1,740	14,920
Legal and Professional	10,000	5,000	-	-	5,000	-	-	-	20,000
Maintenance	-	-	-	-	4,200	-	-	-	4,200
Travel and expenses	700	1,500	1,500	1,500	1,100	1,500	1,500	1,500	10,800
	36,947	18,248	15,747	13,248	26,606	14,306	19,305	14,306	158,713
OTHER COSTS									
Depreciation	3,500	3,750	4,417	5,750	4,661	4,662	4,661	4,661	36,062
	3,500	3,750	4,417	5,750	4,661	4,662	4,661	4,661	36,062
OPERATING PROFIT	(40,447)	(41,263)	(39,428)	(38,263)	98,481	(34,219)	(32,217)	(19,219)	(146,575)
NET PROFIT	(40,447)	(41,263)	(39,428)	(38,263)	98,481	(34,219)	(32,217)	(19,219)	(146,575)
CUMULATIVE	(40,447)	(81,710)	(121,138)	(159,401)	(60,920)	(95,139)	(127,356)	(146,575)	(146,575)

N.B. The income from the subscription service has been shown as a single amount rather than a monthly accrual, for the sake of clarity.

13.2. Cash Flow for Pilot by Month

	Aug 08 £	Sep 08 £	Oct 08 £	Nov 08 £	Dec 08 £	Jan 09 £	Feb 09 £	Mar 09 £	Apr 09 £	May 09 £	Jun 09 £	Jul 09 £	Total £
RECEIPTS													
VAT	-	-	2,077	-	-	5,558	-	-	3,065	-	-	1,445	12,145
	-	-	2,077	-	-	5,558	-	-	3,065	-	-	1,445	12,145
PAYMENTS													
Invoiced Costs	-	1,681	12,256	5,971	23,301	976	8,908	5,676	5,971	976	7,733	976	74,425
Specialist Staff Direct	-	-	-	4,204	4,203	4,204	4,203	4,204	4,203	4,204	4,203	4,204	37,832
Staff Salaries	1,178	1,178	1,177	1,178	1,178	1,178	1,178	1,177	1,178	1,178	1,178	1,177	14,133
Hardware - Systems and Network	-	-	54,000	-	-	-	-	-	-	-	32,000	-	86,000
Software	-	-	-	7,050	-	-	-	-	-	-	-	-	7,050
PAYE/NI	-	491	492	491	2,710	2,709	2,709	2,710	2,709	2,709	2,710	2,709	23,149
	1,178	3,350	67,925	18,894	31,392	9,067	16,998	13,767	14,061	9,067	47,824	9,066	242,589
NET CASH FLOW	(1,178)	(3,350)	(65,848)	(18,894)	(31,392)	(3,509)	(16,998)	(13,767)	(10,996)	(9,067)	(47,824)	(7,621)	(230,444)
OPENING BANK	250,000	248,822	245,472	179,624	160,730	129,338	125,829	108,831	95,064	84,068	75,001	27,177	250,000
CLOSING BANK	248,822	245,472	179,624	160,730	129,338	125,829	108,831	95,064	84,068	75,001	27,177	19,556	19,556

13.3. Cash Flow Forecast

	Aug 09	Sep 09	Oct 09	Nov 09	Dec 09	Jan 10	Feb 10	Mar 10	Apr 10	May 10	Jun 10	Jul 10	Total
	£	£	£	£	£	£	£	£	£	£	£	£	£
RECEIPTS													
Invoiced Sales	-	117,500	-	52,875	5,875	-	-	5,875	5,875	-	8,225	11,750	207,975
VAT	-	-	-	-	-	-	-	-	1,181	-	-	-	1,181
	-	117,500	-	52,875	5,875	-	-	5,875	7,056	-	8,225	11,750	209,156
PAYMENTS													
Invoiced Costs	976	11,551	9,319	4,295	5,676	976	4,060	5,676	9,935	976	8,760	976	63,176
Specialist Staff Direct	4,385	4,386	4,386	4,385	4,386	4,385	4,386	4,386	4,385	4,386	4,385	4,386	52,627
Staff Salaries	1,215	1,214	1,214	1,214	1,214	1,214	1,214	1,214	1,214	1,214	1,214	1,214	14,569
PAYE/NI	2,710	2,881	2,881	2,881	2,881	2,881	2,882	2,881	2,880	2,881	2,881	2,882	34,402
VAT	-	-	14,244	-	-	7,118	-	-	-	-	-	1,378	22,740
	9,286	20,032	32,044	12,775	14,157	16,574	12,542	14,157	18,414	9,457	17,240	10,836	187,514
NET CASH FLOW	(9,286)	97,468	(32,044)	40,100	(8,282)	(16,574)	(12,542)	(8,282)	(11,358)	(9,457)	(9,015)	914	21,642
OPENING BANK	19,556	10,270	107,738	75,694	115,794	107,512	90,938	78,396	70,114	58,756	49,299	40,284	19,556
CLOSING BANK	10,270	107,738	75,694	115,794	107,512	90,938	78,396	70,114	58,756	49,299	40,284	41,198	41,198

13.4. Discounted Cash Flow by Month

EMMAN Discounted Cash Flow Forecast

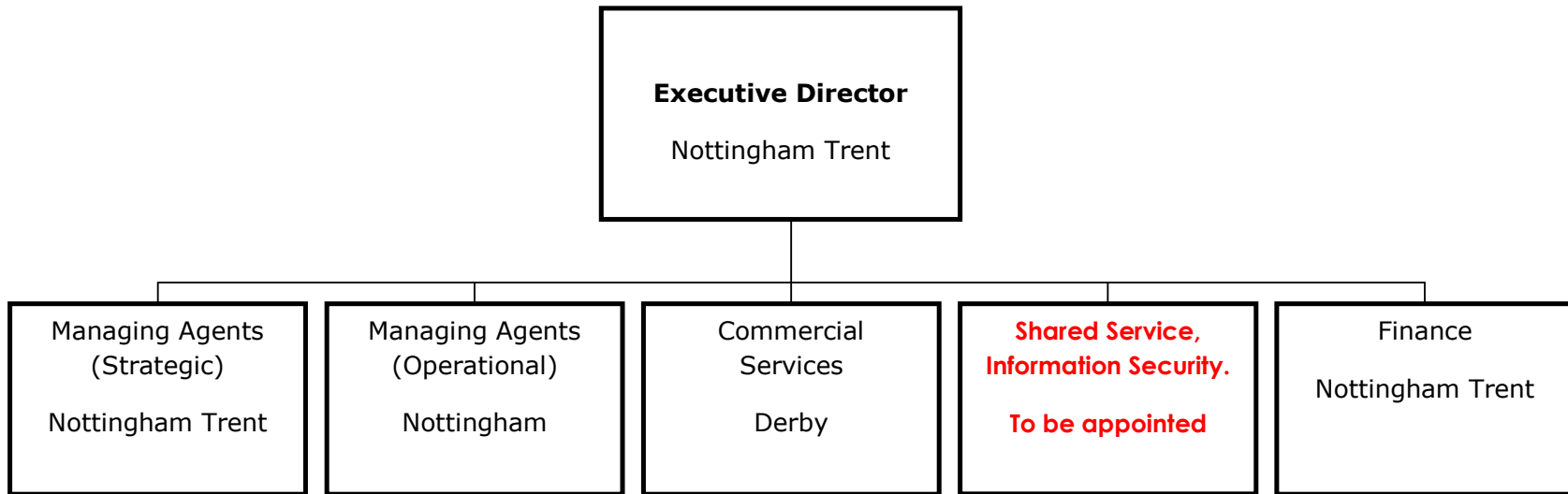
	Discount Rate												7%
	Month												
	1	2	3	4	5	6	7	8	9	10	11	12	Year
NET CASH FLOW	-£1,178	-£3,350	-£65,848	-£18,894	-£31,392	-£3,509	-£16,998	-£13,767	-£10,996	-£9,067	-£47,824	-£7,621	-£230,444
DCF	-£1,171	-£3,311	-£64,709	-£18,459	-£30,492	-£3,389	-£16,320	-£13,141	-£10,435	-£8,555	-£44,860	-£7,107	-£221,950
	Month												
	13	14	15	16	17	18	19	20	21	22	23	24	Year
NET CASH FLOW	-£9,286	£97,468	-£32,044	£40,100	-£8,282	-£16,574	-£12,542	-£8,282	-£11,358	-£9,457	-£9,015	£914	£21,642
DCF	-£8,610	£89,846	-£29,367	£36,537	-£7,502	-£14,927	-£11,230	-£7,372	-£10,052	-£8,321	-£7,886	£795	£21,910

EMMAN Discounted Cash Flow Forecast

HEFCE Shared Services Feasibility Study, Information Security Management, Final Report

		Discount Rate 7%											
		Month											
	1	2	3	4	5	6	7	8	9	10	11	12	Year
NET CASH FLOW	-£1,178	-£3,350	-£65,848	-£18,894	-£31,392	-£3,509	-£16,998	-£13,767	-£10,996	-£9,067	-£47,824	-£7,621	-£230,444
DCF	-£1,171	-£3,311	-£64,709	-£18,459	-£30,492	-£3,389	-£16,320	-£13,141	-£10,435	-£8,555	-£44,860	-£7,107	-£221,950
		Month											
	13	14	15	16	17	18	19	20	21	22	23	24	Year
NET CASH FLOW	-£9,286	£97,468	-£32,044	£40,100	-£8,282	-£16,574	-£12,542	-£8,282	-£11,358	-£9,457	-£9,015	£914	£9,642
DCF	-£8,610	£89,846	-£29,367	£36,537	-£7,502	-£14,927	-£11,230	-£7,372	-£10,052	-£8,321	-£7,886	£795	£21,910

14. APPENDIX B: EMMAN Ltd Operational Structure



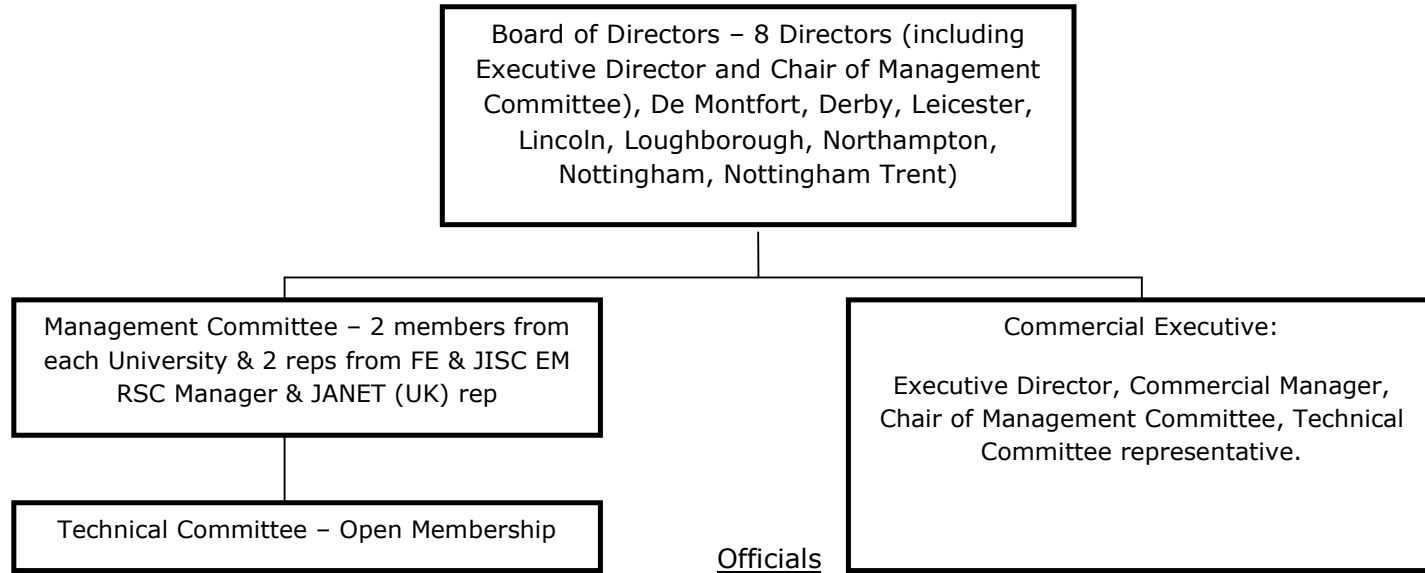
Key Individuals

Technical Manager (Strategic)	John Cheesbrough	Nottingham Trent
Technical Manager (Operational)	Phil Harrison	Nottingham
Commercial Manager	Pete Darby	Derby
University of Nottingham Manager	Richard Smeeton	Nottingham
Technical Support	Roger Browne	Nottingham Trent
Technical Support (FE)	James Higham	Loughborough/Nottingham Trent
Accountant	Jo Frith	Nottingham Trent
Bookkeeper	Rob Thirlby	Heathfield
EMMAN Executive Director	Ian Griffiths	Nottingham Trent

N.B. Most of the staff mentioned combine EMMAN work with other things.

15. APPENDIX C: EMMAN Ltd Governance Structure

Company Limited by Guarantee



Chair of Board of Directors	Richard Maccabee	Derby
Chair of Management Committee	Tony Brookes	Derby
Chair of Technical Committee	Dave Roberts	Leicester
Minute Secretary to Board of Directors	Richard Smeeton	Nottingham
Secretary to Management Committee	Dave Temple	Loughborough
EMMAN Executive Director	Ian Griffiths	Nottingham Trent
Auditors	Donald MacDuff	PKF (UK) LLP
Company Secretary	James Kindell	David Venus & Co Ltd
Company Solicitor	Michael Longden	Irwin Mitchell