



## Migration Lifeline

White Paper 2009

A guide to managing a successful  
infrastructure migration



certainty / confidence / agility



## Overview

Consolidating the management of your infrastructure to a single provider can dramatically reduce your IT operations expenditure and, in some cases, by up to six figures. However, the process of migrating critical infrastructure can be complex and risky.

Based upon our experience of managing over 150 migrations for some of the UK's leading blue chip companies, retailers and financial services organisations, Attenda has compiled the Migration Lifeline as a guide and sample project plan to manage a successful infrastructure migration.



## Table of Contents

1. Executive Summary.....	4
2. Planning a migration project .....	7
1) Ensure every project is clearly defined .....	7
2) Ensure a defined beginning, middle and an end .....	7
3) A project must have a clear organisation.....	8
4) A project must have clearly defined communication plans .....	8
5) A project must have a documented (and agreed) plan .....	8
6) Every project must have management buy in.....	8
3. Managing the migration .....	10
1) Project initiation stage .....	10
2) Relocating your solution.....	12
3) Preparing for service restoration .....	13
4) Re-commissioning.....	13
5) Testing.....	14
6) Go live .....	14
7) Security .....	14
8) Establishing operational services and monitoring.....	15
9) Documentation .....	15
10) Project closure .....	16
4. Glossary.....	17
5. A Managed Approach .....	19



## 1. Executive Summary

The need to drive greater cost efficiencies into IT operations will again dominate the agenda of many IT departments this year. Accounting for up to 80% of an IT system's lifecycle costs, operations continues to come under intense scrutiny as an area in which IT spend can be significantly reduced.

Some IT departments have realised significant reductions in operations expenditure by migrating their entire infrastructure to the management of a single, trusted provider. By merging multiple business applications such as ERP, Messaging & Collaboration, Thin Client and Web Applications to a single architecture, enterprises are able to save the time and costs involved in managing multiple infrastructures, networks, suppliers, contracts and SLA's. In fact, some organisations have cut **six figure sums** from their budgets.

However the market is volatile; finding a suitable supplier is difficult and the migration process itself is complex and risky. A more typical preference has been to 'spread the risk' – operating infrastructure within multiple locations, paying a premium in infrastructure management costs and suffering inconsistent service levels.

Yet, if an organisation is confident that it can mitigate the risks of a complex migration and find a trusted operations partner, then a migration to a consolidated infrastructure becomes a highly attractive option, its potential to improve service levels and reduce costs outweighing the risks. Importantly it will allow your in-house specialists to concentrate on the higher value activities that drive competitive differentiation, knowing with complete confidence that your vital applications are available and secure

This guide seeks to help IT departments and project managers do exactly that – to reduce the likelihood and impact of the many risks inherent in taking on a complex migration project. It is based on a real migration undertaken by Attenda and comprises a sample project plan containing detailed, real life project stages, tasks, resource allocations and timescales for a typical migration project, with an extensive body of knowledge held in the notes allocated to each task. It is accompanied by this commentary that seeks to highlight those factors most likely to make or break a project of this complexity.



## Your provider

This plan addresses a number of migration scenarios for an organisation 'lifting and shifting' its hardware from one Data centre to another, whether between third party suppliers, telcos or managed services providers, or from an external provider to an in house operations centre.

Whilst the plan provides guidance on some of the key considerations for a migration, it assumes that the decision over the most suitable operations partner has been made. If you are in the process of selecting an operations partner, you may wish to consider the points overleaf.

1. Do the skills exist to manage the complexity of your application or will you need to supplement them with your own resource? Have you allocated additional budget for this?
2. Are you confident in the financial stability of your new provider? Are they cash generative and debt free?
3. Are they locally based or a satellite of a larger global organisation?
4. What impartial validation of their service management exists? ISO 20000 IT Service Management System, ISO 27001 Information Security Management System, ISO9001 Quality Management System or vendor recognition such as HP signature partner, Microsoft Gold, SAP Hosting Partner, SunTone or VMware Hosting Partner.
5. What experience do they have of running a migration? Can client references be obtained?
6. What best practice standards do they adhere to? Are their processes ITIL or MOF compliant? Are they using PRINCE2 as their project management methodology?

To assess the service levels you are likely to achieve, you will need to examine the provider's operational infrastructure, that is the processes, people and technology they have in place to provide consistent service levels. This is especially important if the complexity of your applications and infrastructure, or its management requirements, have outgrown the capabilities of your existing operations partner or in house operations team and requires more specialist support.



## Avoiding the pitfalls

Irrespective of the scenario, a migration constitutes a highly complex and potentially risky project and it is common for organisations to fall foul of common yet avoidable errors and increase the risks of an already complicated project. Yet, if well planned and well managed, such a project can be successfully executed to time and to budget reducing the associated risks.

This guide provides a detailed sample project plan and commentary that will provide a valuable insight into some of the pitfalls inherent in a complex infrastructure migration. It highlights the key tasks, project stages, resources and timescales common to all projects, regardless of impetus for migration or size and complexity of infrastructure. Whilst there is no substitute for an experienced team, this project plan was originally written for an Attenda client who approached us to manage their migration. It contains the combined experience and expertise of our team of qualified project managers, technical architects and solutions consultants.

*! Although this paper can provide a useful starting point for your planning, every migration project is different – with different drivers, risks and technical scenarios. So it is essential that you consider carefully the specific requirements of your project.*

Whether you wish to limit your infrastructure management expenditure by consolidating your infrastructure, establish superior levels of service and support for mission critical applications, or you just want to mitigate the risks of running a project of this complexity, the guide will provide you with an important understanding of how to put together and execute a successful migration project.

*A note for readers:*

*Part one of this guide is devoted to project management. Whilst it is always worth reiterating the essential aspects of best practice project management, if you are an experienced project manager, you may wish to skip this section and move on to Part Two.*



## 2. Planning a migration project

Almost any activity that involves carrying out a non-repetitive task can be described as a project. However, there exist significant differences between a simple project involving one or two people and one that requires the involvement of a complex mix of people, organisations and tasks. Careful planning becomes especially important when the result of a project is as critical as the successful migration of an application that is vital to your business.

A number of structured methodologies have been developed to provide a formal approach to project management. This document and the attached plan is based on PRINCE II project methodology which Attenda uses for all client projects. More details of this method can be found on the official Web site: <http://www.ogc.gov.uk/prince2/>

Outlined below are some of the key elements common to all project management methodologies and central to project management best practice.

### 1) Ensure every project is clearly defined

Each project must have a clear objective and deliverables, which are agreed and documented.

### 2) Ensure a defined beginning, middle and an end

It may sound obvious but many “projects” skip the beginning and therefore fail to reach the end, often as that end is not clearly defined. Every project should have at least three stages:

- The initiation stage, where objectives are defined, business cases are developed, senior management buy in is obtained, the project team and project board are appointed and the project plan is developed.
- The implementation stage, which may be divided into several stages with different, clearly defined variables. During this stage, the project plan is actioned and deliverables produced.
- The project closure stage, where the project is assessed for success against the original objectives and any outstanding tasks or issues are noted.



### 3) A project must have a clear organisation

Each project should have a named project manager, and as importantly, a project sponsor who should be a senior level employee to ensure the project is supported and represented at the highest level. Without this high level support, few projects will succeed in meeting their objectives.

In addition, the project team should be clearly defined, and responsibilities formally agreed and documented by every team member. Within the project team there should be at least one project client and one project supplier representative.

Finally the project should have a project board, which is usually made up of the project sponsor, the client and the main supplier. Key decisions will be escalated to the project board for sign off. In effect, the project board act as executive decision makers within the project team.

### 4) A project must have clearly defined communication plans

As project teams are often “virtual” teams communication can be difficult to manage. During the initiation stage, a communications plan should be drawn up, formalising the frequency and type of communication both within the project team and from the team to the wider organisation.

### 5) A project must have a documented (and agreed) plan

Usually completed during the initiation stage, this is the detailed list of tasks, which indicates specific responsibilities, required timescales and dependencies of different tasks. By indicating timescales and dependencies between tasks, a critical path can be mapped out.

When planning your project, it is very important to be realistic. Make sure your project team consider the implications of what they are being asked to do, especially in parallel with their other day-to-day responsibilities. One of the biggest problems with projects is resource planning. You may wish to include a contingency into the planned timescale, or explicitly question whether resources will be available. Get it right during the initiation stage and set expectations appropriately.

Providing these basic principles are followed, your migration project should be able to be managed in an efficient and effective way. However, remember that there is one more very important factor to consider that will ensure your project is completed to time and to budget.

### 6) Every project must have management buy in

Without commitment from the management, no project can succeed. Management commitment ensures that not only monetary resources will be made available, but also that human resources, which are often



required from various departments, will be made available as and when required. Management commitment is often formalised by the development of a business plan, developed during the initiation stage, which defines the cost (both in terms of resource and capital expenditure) and the benefits of the project.



### 3. Managing the migration

Appendix A of this paper provides IT departments and project managers with a sample project plan for the migration of a typical Internet application. This is based on an actual plan written for an Attenda client who successfully migrated their Web infrastructure on time and to budget. It has been adapted to provide a general guide to planning and executing your own successful migration project.

The plan includes a detailed breakdown of key project stages and tasks, sample timescales, suggestions on resource allocation and a substantial body of notes - hard earned insights and tips from our experience of managing the migrations of critical, blue chip Web applications. Those sections that have the greatest impact on the successful delivery of a project of this kind have been highlighted in the sections below.

In this plan, it is assumed that the equipment is being “lifted and shifted”. That is, taking the existing infrastructure and re-deploying it in a new location, without adding servers or changing the configuration or the site itself. In some instances, migration strategies involve commissioning new equipment prior to de-commissioning the old to limit the potential for downtime during the migration, but as ‘lift and shift’ is the most complex, we have focused on this approach. Attenda can advise on the most cost effective strategy.

The plan also assumes that the business plan has been completed and signed off with the project objectives clearly defined and agreed.

The objective of this project can be summarised as follows:

***“To complete the migration of an existing application, from its current location to a new Data centre, within the stated timescale and the agreed budget, using a “lift and shift” strategy.”***

*! When planning your own migration, it is important to review this plan in the light of your own specific objective and strategy for migration.*

#### 1) Project initiation stage

Without a carefully managed project initiation stage, it is highly unlikely that the project will truly achieve its objectives and be completed within the specified budget and timescales. During this stage, all partners should attend a risk assessment workshop.



## Personnel

The appointment of a project manager and project sponsor will take place during this stage. Ideally, the sponsor will be a senior member of staff. Without this seniority to drive the project, it is unlikely that it will reach its successful completion.

## Due diligence

A period of due diligence should take place before any other activity commences, to provide the necessary time to obtain, collate and verify all documentation relevant to the project.

Documentation should not be more than one week old to ensure that all the latest patches and updates are taken into account. It should include details of any firmware and software license keys, full technical architecture documentation (including cabling) and details of monitoring regimes, scheduled tasks and user passwords.

## Application health check

It is important to assess at the initial stages of the project any potential impact the migration may have on the application itself. This will include checks for hard coded IP addresses that will not work within the new Data centre location.

Also examine the security model of your new operations provider. If security specifications differ from those which the application was originally built for, there can be implications for the way in which you access or connect to your solution.

## Back up

A full back up of the solution must be obtained and verified before any preparatory work on the solution commences. Restores should be fully tested to ensure the back ups have been completed successfully.

*! Don't rely on a single back up as tapes and files can corrupt.*

## Suppliers

Another key area that often receives insufficient attention is the process of supplier engagement. Suppliers you are likely to require will include the new operations provider (who should have proven knowledge and experience of all the technologies used within your application), the application developer and the physical removals company.



*! Verify that your insurance company will cover your equipment during the removal from one Data centre to another. It is also wise to contact your leasing company at this stage, if you use one.*

Once you have chosen suppliers, you must ensure that you have signed contracts that detail the agreed roles and responsibilities, as well as schedules.

*! Double check that all parties agree and understand these terms to avoid unnecessary delays or cost escalations during the project.*

Only once each of these tasks is performed and documented should you kick off the project. The final schedule and escalation paths should be confirmed and the risk and issue logs updated. These logs document and assess the likelihood, impact and mitigation strategy for any identified risk or issue.

NB: If you have a staging solution it may be wise to consider moving this first as a pilot project.

## 2) Relocating your solution

How much downtime is acceptable?

### 24 hours

In the example provided, the solution migration is estimated to take around 24 hours, and this was considered an acceptable level of downtime to incur. How you manage the changes to IP addressing and associated DNS record changes will dictate the downtime likely to be experienced. DNS changes generally take around 48 hours to propagate so, in advance of the migration, the time to live of the Zone Records is reduced to 1 hour. This means that the DNS changes will propagate more quickly (closer to 24 hours), and reduce the time the site is unavailable.

### Zero downtime

If no downtime is acceptable, there are two options:

- 1) To redirect old, public IP addresses to a holding page, only making the final DNS record changes shortly before the migration is complete (or even once the solution has been completely relocated and tested to limit risks). In any scenario, it is always good practice to have a holding page available, in case of problems with the migration. However, this means that the full functionality of the site is not available, so you may wish to use the staging or BCP sites temporarily instead.



- 2) The alternative is to leave a reduced infrastructure in place that provides complete functionality but with diminished performance or load capabilities. The DNS record changes are made once the new solution is complete and tested.

### Final checks before de-commissioning

Before removing the solution from its current racks, it is recommended best practice to ensure that:

- Hardware spares for all key components are available and that all hardware and cabling is labelled and logged in an asset register.
- All copies of relevant software are available and passwords for all devices, software and user accounts are known and documented.
- The service is fully operational prior to decommissioning.
- That any communications links (e.g. VPN, leased line etc) required at the new location will be available at the required time and date.

When all of these preparations have been made, devices can be shutdown and un-racked. All devices should be marked off on the asset register before the authority to transport should be given.

### 3) Preparing for service restoration

Before the equipment can be re-racked in its new location, ensure the relevant preparatory work is carried out in the new Data centre. This will include setting up the racks and configuring the local rack networking infrastructure and bandwidth. The new public IP allocation & private IP addressing should already be assigned and mapped to the old public and private IP addressing.

If sufficient resource is available or time is of a premium, these tasks can be carried out concurrently with the de-commissioning process in the old Data centre.

### 4) Re-commissioning

Once all the preparation is complete, the re-commissioning process can start. At this stage, all the devices should be re-racked, cabled and documented in the asset register. The devices can then be powered up, new IP addressing can be configured and you can check that all services are running appropriately. Finally network connectivity can be confirmed.



## 5) Testing

During the initiation stage of the project criteria should be agreed for testing the solution following re-commissioning. Without rigorous testing a faulty application could be put live, or could fail soon after.

Testing will usually involve both the new operations partner to test network connectivity and the application developer who will test application functionality.

*! It is a good idea to ensure that the team that will manage the solution on an ongoing basis is available to attend these tests, as the issues raised can be helpful in planning operational requirements.*

## 6) Go live

Once testing is complete (and signed off officially), the solution can Go live. Going live means all DNS changes have been propagated and that the site is available to browse from the Internet.

***! Prepare a checklist during the initiation stage to enable you to check for functional readiness before Go live.***

## 7) Security

Following the deployment, it is of utmost importance to verify that the integral security of the solution has not been compromised in any way. Migrating a solution entails making multiple changes to security settings, such as firewall or operating system configurations and a thorough audit will be required to ensure that the application remains secure.

A security audit may be provided by the new operations partner, or a third party. At the very least the following areas should be tested:

- Existing firewall OS and/or configuration may require updates to ensure protection against latest vulnerabilities or compliance with operations provider standards. To avoid unnecessary risk the firewalls changes should be restricted to the required IP changes and any additional work scheduled for once the migrated solution is stable.
- A vulnerability scan should be carried out prior to Go live, usually by the hosting provider, to ensure that all the latest patches are applied and that changes to configurations during the migration have not opened up new security risks.
- Check your existing anti-virus solution is compatible with the new operations provider standard offering.



## 8) Establishing operational services and monitoring

A site migration requires a reassessment of its operational requirements which must be explored and agreed with the operations provider.

Key elements to consider, agree and document include:

- Monitoring requirements, escalation paths and responsibilities for fault management
- Reporting requirements (including frequency and level of detail required)
- Frequency and availability of back ups and restores, as well as the process for monitoring for back up success
- General administrative requirements including
- Scheduled maintenance
- Housekeeping
- Specialised fault management tasks
- Key contacts

## 9) Documentation

Once operational requirements are agreed they should be clearly documented in an operations manual, which should be stored with other key documents in a commonly accessible area.

Without clearly defined and documented operational procedures and responsibilities, the system availability and performance can be easily compromised through grey areas of responsibility.

All technical architecture documents must be verified and updated to ensure that those responsible for ongoing maintenance of the solution will have all the information they need to meet the SLA.

Taking time to ensure the complete documentation set is available at handover will ensure the operational staff have all the information about the solution, as well as a fully functional site. This will be important when maintaining application availability as when problems occur, the operations team need access to all the latest technical and operations documentation.



## 10) Project closure

Project closure is often forgotten, but in a migration it provides an important time to transfer responsibility for the system to the operations team who will be looking after it.

At this stage the success of the project is measured against key objectives, and importantly, any outstanding tasks or issues can be documented and passed on to ensure that they are completed (and not forgotten).



## 4. Glossary

Project	A set of tasks, carried out in order to achieve a specified, common goal
Project manager	The person responsible for coordinating the activities of the project team
Project sponsor	A member of the project team who acts as a representative of the company's senior management
Project team	A group of people who are responsible for ensuring the completion of the tasks identified for the project
Project client	A member of the project team who represents the interests of the beneficiaries of the project deliverable(s). This project client may be internal or external
Project supplier	A member of the project team who represents the interests of an organisation supplying products or solutions for the project
Project board	The executive team responsible for making final key decisions for the project. Usually made of the project sponsor, project client and project supplier
Project plan	The document which details the tasks required to complete the project, their dependencies, responsibilities for these tasks and schedules
Critical path	The tasks which affect the final date of delivery for the project
Initiation stage	The planning stage of the project
Implementation stage	The action stage of the project
Closure stage	The review stage of the project
Risk log	An ongoing document where all identified risks can be noted, with analysis of the impact and likelihood, as well as mitigation strategies



Issue log	An ongoing document where all identified issues can be noted, together with decisions on actions required and carried out
Vulnerability scan	A scan which checks that basic security settings remain in tact
Security audit	A complete audit of solution security, including both logical and physical security



## 5. A Managed Approach

### About Attenda

Attenda, the Always On Managed Services company, manages those vital enterprise, web and messaging & collaboration applications that every business relies upon today to function effectively allowing our clients to selectively outsource their IT operations and re-focus on using IT to add strategic value to their business.

Through a commitment to operational excellence, we manage, secure and optimise the performance of business critical applications, irrespective of the physical location of the infrastructure.

With over 8 years' investment into Attenda M.O., Attenda's operations platform, we provide the people, process and technology to deliver exceptionally high service levels, but at a cost that is amortised across Attenda's entire client base - currently 134 of the UK's leading companies.

Attenda is VMware EMEA Hosting Partner of the Year 2008 and 2009 and provides VMware virtualised solutions for dedicated Windows or Linux, or heterogeneous operating systems environments, the Attenda Real Time Infrastructure and Cloud Services.

Attenda pro-actively monitors and manages IT infrastructures 24 x 7, identifying problems before they occur. ISO 20000 certification reinforces Attenda's commitment to delivering the very highest service levels in IT Service Management and ISO 27001 certification ensures that these systems are highly secure.

Attenda an HP SP Signature Partner, a Microsoft Gold Certified Partner, a SAP Adaptive IT Hosting Provider, and a SunTone accredited managed service provider.

### Contact Us

Attenda Limited  
One London Road  
Staines, TW18 4EX

T: +44 (0)1784 211 100  
F: +44 (0)1784 211 200  
E: [info@attenda.net](mailto:info@attenda.net)