



MindGrove Checklists
Application Service Providers

Revision 2 - January 06

MindGrove Ltd
 PO Box 729
 Warrington
 CHESHIRE
 WA4 4WZ

Tel: +44 1925 732 757
 Fax: +44 1925 732 756

Email: enquiries@mindgrove.co.uk
 Website: <http://www.mindgrove.co.uk>

Note: The MindGrove website has additional useful working and training materials on its resource pages.

| Document | | | |
|---|--------------|-----------------|------------|
| Document | | Template | Size |
| MindGrove Checklists for Auditors - Application Service Providers | | Manual 2005.dot | 165376 |
| Status | Final | Version | Format |
| Issue | 1 | 26 | A4 |
| Change History | | | |
| Author | Component | | Date |
| MnD | This version | | January 06 |
| If you find this checklist useful then please tell others about this website and why not send one of your checklists to MindGrove at checklists@mindgrove.co.uk and we will publish it for the good of all. | | | |

ASPs – 11 major risks to the organisation ...

Organisations are routinely outsourcing non-core business. And one of the more common outsourcing operations involves contracting out facilities to an ASP.

An ASP is an application service provider that hosts software systems, such as Payroll, HR, or Accounts, on your behalf. This avoids you having to get involved in software configuration, licensing, deployment and hosting; avoids you having to employ specialist staff; and potentially allows you to take advantage of reduced costs due to the large scale of operations hosted by the ASP.

However, you do need to consider the need for additional security facilities to ensure that you can connect securely and privately to your ASP, and you will have some new contractual issues to consider ...

Use MindGrove’s checklists to help make sure you’ve considered and covered, at least, these 11 major risks.

| There may be a risk to the organisation because of: | These are the countermeasures and controls that we will deploy... |
|---|--|
| <p>The nature and execution of the contract...</p> <ol style="list-style-type: none"> 1. Failure to draw up a proper contract <p>Technology and security</p> <ol style="list-style-type: none"> 2. Failure to secure the privacy of the link between your organisation and the ASP <ul style="list-style-type: none"> ▪ Have you considered the need for an encrypted link, for using a VPN or for using tunneling protocols? 3. Failure to provide an effective identification and registration process for all ASP system users <ul style="list-style-type: none"> ▪ Have you considered how the ASP is going to uniquely identify your staff? ▪ How will the ASP register your staff on and off the system? ▪ What about temporary hires or contractors who might need to use the system – how will you be able to distinguish them from permanent staff? ▪ How will changes in staff numbers be managed – for example, how will the registration system enable you to deal with leavers, including terminations? | <p>Retrieve MindGrove’s Contract Checklist and ensure all common contract risks are properly thought through and covered see http://www.mindgrove.co.uk/tools.htm</p> |

| There may be a risk to the organisation because of: | These are the countermeasures and controls that we will deploy... |
|---|---|
| <p>4. Failure to properly authenticate users of the ASP service</p> <ul style="list-style-type: none"> ▪ What strong, single entry point, authentication process will be used to guarantee that only your nominated, identified and pre-registered staff get access? ▪ What process will prevent authentication session replays, guarantee unique session identities, and negate the possibility of spoofing of sessions? <p>5. Failure to properly authorize users of the ASP service</p> <ul style="list-style-type: none"> ▪ What mechanism will guarantee that all authenticated users will work only in the context of an appropriate and authorized “need-to-know” data and application access profile? ▪ Who defines users’ roles, who decides on the correct granularity of access, who modifies users’ roles and authorizations, who monitors user role creation, modification, deletion and day-to-day administration? <p>6. Failure to properly set up network hosts</p> <ul style="list-style-type: none"> ▪ Do you know who sets up, owns, configures and administers security hosts such as routers, gateways, proxies and firewalls between you and your ASP’s application servers? ▪ Have you an assurance that the absolute minimum number of TCP/IP Protocols, Services and Ports are deployed by your ASP in the provision of your service? ▪ Have you an assurance that all the hosts deployed by the ASP in the provision of your service are using hardened software, to which service packs, patches, corrections and fixes are routinely and obsessively applied? ▪ Do you know if the ASP routinely performs internal and external vulnerability scanning and external penetration testing of their own services to ensure that the site that hosts your services is as secure as possible? ▪ Has your ASP had their security architecture independently inspected and accredited? Would it meet ISO: 17799? | <p>Retrieve MindGrove’s router checklist from http://www.mindgrove.co.uk/tools.htm</p> |

| There may be a risk to the organisation because of: | These are the countermeasures and controls that we will deploy... |
|--|---|
| <ul style="list-style-type: none"> ▪ Who sets the rules, defines the procedures and implements security policy and change management to protect both your domain and that of your ASP? <p>7. Failure to properly set up client software on your side of the network</p> <ul style="list-style-type: none"> ▪ Have you proof that someone has configured all staff ASP access software agents and browsers correctly? ▪ Do you know if you've configured all client-server packet exchanges to use digital signatures or packet signatures to ensure authenticity and non-impersonation of transactions? ▪ Who has arranged that all transient data images: in memory, in storage, as cookies, or in intermediate hosts are scrubbed at the end of sessions? <p>8. Failure to properly set up logging and journalisation controls</p> <ul style="list-style-type: none"> ▪ Would you be able to link users to sessions and reverse engineer back to their physical locations? ▪ Have you considered the type and amount of evidence that you will need to check and keep to provide the ability to investigate anomalies and trace the source of system activity? ▪ Who is going to examine logs and journals to ensure that processing was as intended? ▪ Has the ASP arranged for intrusion detection facilities and log monitoring? <p>Communications and Service</p> <p>9. Failure to provide for effective MIS reports from the system</p> <ul style="list-style-type: none"> ▪ Has your organisation thought about and clearly set down what MIS you are you going to need about who, why, when and where your staff, temporary staff, contractors and ASP staff, get access to your system and modify its data or transactions? | |

| There may be a risk to the organisation because of: | These are the countermeasures and controls that we will deploy... |
|--|---|
| <ul style="list-style-type: none"> ▪ Have control reports been designed that prove that all data input, transformed, updated and deleted are complete and correct in amount, precision, and total number and value; that changes cannot be repudiated and capable of being independently verified? ▪ Has a process been specified to allow for independent system and data interrogation so that queries can be processed, trails pursued, and forensic evidence determined? <p>10. Failure to set up a usable service level agreement</p> <ul style="list-style-type: none"> ▪ Has your organisation negotiated a clear and unambiguous contract that makes provision for the definition and measurement of availability and robustness of service? ▪ Is it obvious who puts things right when they go wrong and how issues will be escalated until they are resolved? ▪ Have you made it clear who has ownership of your data whilst it is resident on your ASP's hosts or storage media? ▪ Who will handle incidents and take responsibility for intrusions into your data? ▪ What rights of access do you need as an organisation to inspect or audit the ASP service? ▪ Have you clearly thought through issues concerning Business Continuity Planning, Contingency, Backup and Recovery, and Disaster Preparation connected with the applications that you are having hosted by your ASP? ▪ Has your ASP clearly demonstrated their ability to meet your service level, performance and bandwidth, and business continuity requirements? ▪ Are you aware of any Proof-of-Concept benchmarking and the results? ▪ Do you have the right to withdraw from the service if you perceive the service to be inappropriate or poor in quality, or will your organisation be locking itself into a straight jacket? | |

| There may be a risk to the organisation because of: | These are the countermeasures and controls that we will deploy... |
|---|---|
| <p>Return on Investment (ROI) and the Law</p> <p>11. Failure to properly evaluate financial and legal matters</p> <ul style="list-style-type: none"> ▪ Has your organisation completed a proper ROI calculation that considers all aspects of the ASP service and all positive and negative impacts on your existing business? ▪ Will you have to buy new software licences, will this be done by the ASP, will your discount structure be carried through to the ASP, could you benefit from reverse licencing by the ASP? ▪ Are you prepared to negotiate and review tariffs charged by the ASP for providing your services on a regular basis. Will you undertake a competitive review from time to time? ▪ Could your processing be shifted to another ASP or back to your own organisation to improve your ROI? ▪ What would happen to your data and processes if your ASP went into insolvency, bankruptcy or liquidation? ▪ How much knowledge are you going to lose as an organisation: will you have to buy back information about your own processes; will you have to pay extra for knowledge mining from your own data; might you end up at a competitive disadvantage because you cannot easily change your business processes? ▪ Are both you and the ASP aware and prepared for any legislative regulations concerning privacy and data protection? | |

If you find this checklist useful then please tell others about this website and why not send one of your checklists to MindGrove at checklists@mindgrove.co.uk and we will publish it for the good of all.