neupart
The ERP of Security

Security assessment for use when choosing an IT outsourcing supplier

	Yes/No Can also be a weighted score from 1-5	Comment
General assessment of supplier		
If the supplier has any subcontractors: What do they outsource? *Do they outsource any critical data or functions?*		
Are the organisational roles and the responsibilities for the security assignments clearly defined at the supplier *Does the defined cover IT-strategies, policies and organisation of information security*		
Is the supplier dedicated to working in accordance with IT-governance principles? *Examples of this are ITIL processes, Cobit and ISO 27001 for security management*		
Is the supplier certified against relevant standards such as ISO 27001 or PCI DSS?		
Service level goals and reporting		
Are the conditions surrounding fines/penalties for non-compliance with safety requirements and/or service level clarified?		
Has reporting on agreed service level goals been satisfactorily considered *Includes the KPI or similar metrics and service level goals the supplier can be compared with*		
Is the option for a periodical IT-audit of the supplier been available? *Includes access to the suppliers internal/external IT-audit reports or outsourcing reports on internal IT-controls (SSAE16)*		
Is the supplier determined to work in accordance with relevant safety standards such as ISO 27001/ISO27001 or PCI DSS?		
Does the supplier produce a yearly risk analysis and is it available?		
What is the suppliers maturity level in relation to knowledge on IT-security in the organisation? *This includes awareness programs and the execution of periodic training of relevant employees at the supplier*		
Exit strategy		

Has a position been taken on how a possible migration of systems/data, in case of a supplier change, would go down? *This includes safe return of assets in physical, electronic form and migration of data in useable formats*		
Is the ownership distribution of systems and source code been clearly defined?		
Has the processes for (safe) destruction of data been agreed upon with the supplier?		
Handling of assets		
Does the supplier have a formal process for the life cycle of data *Includes creation, registration, changes and deletion/destruction of assets*		
User administration		
Does the supplier screen employees who are given access to customer systems and data		
Is the allocation of responsibilities for employee safety clearly defined?		
What is the suppliers maturity level for user administration? *This includes processes for creation, dismantling and periodical review*		
Is the physical security at the supplier sufficient?		
Operating settlement procedures		
Is the allocation of responsibilities for change management and Patch Management clearly defined?		
What is the suppliers maturity level for change management and Patch Management?		
Is the allocation of responsibilities for configuration management and monitoring of performance defined?		
What is the suppliers maturity level for configuration management and monitoring?		
Backup		
Is the distribution of responsibility for backup processes defined?		

What is the suppliers maturity level for backup processes?		
Network security		
Is the distribution of responsibility for network security defined?		
What is the suppliers maturity level for network security?		
This includes appropriate logical/physical separation of customer network/administration network/DMZ, perimeter protection, encryption, firewalls, use of secure protocols, etc.		
Access management		
Is the allocation of responsibilities for conditional access/rights defined?		
To what extent are processes for access management implemented at the supplier?		
This includes, among others, requirements for the use of personally identifiable profiles and logging of user profiles with enhanced rights		
Logging and monitoring		
Is the allocation of responsibilities for logging/monitoring defined?		
To what extent are processes for logging and monitoring implemented at the supplier? *This includes selection of logs, recording, monitoring, escalation, follow-up and reporting to security incidents*		
Acquisition, development and maintenance		
Is the allocation of responsibilities for acquisition, development and maintenance of software defined? What is the suppliers maturity level for systems engineering processes? *This includes the use of best practice frameworks for safe development and security testing in connection with development or procurement of systems and applications*		
Vulnerability management		
Is the distribution of responsibilities for vulnerability management defined?		

What is the suppliers maturity level for vulnerability management? *This includes completion of periodic testing of (web) applications and network in the form of vulnerability scans, application testing and potentially penetration testing*		
Management of security incidents		
Is the distribution of responsibilities for monitoring and reporting of security incidents defined?		
What is the suppliers maturity level for security incidents? *This includes identification, registration, escalation and remediation of security incidents*		
Contingency management		
Is the allocation of responsibilities for contingency management processes defined?		
Has the supplier established a contingency organisation and concrete plans? *This includes contingency plans, distribution of responsibilities for contingency assignments and periodic testing.*		
CSR demands		
Does the supplier comply with international standards for CO2 or have any environmental objectives?		
Does the supplier have a commitment to an ethical treatment of the workforce, pay the minimum wage or above, doesn't use child labour or pollute the environment?		