WATSON HALL

Watson Hall Ltd

London 020 7183 3710
Edinburgh 0131 510 2001

info@watsonhall.com
www.watsonhall.com

CHECK LIST

Information security due diligence

web applications and websites

Identifying information security risk for web applications requires a comprehensive and thorough analysis. This checklist includes information and documents which would typically form a request at the start of a due diligence investigation. The check list is not necessarily complete – depending on the situation, the application, the company or what is identified it may lead to further areas of investigation.

Terms of use

This check list is provided free of charge and without any warranty. Use of this check list is subject to the terms of use displayed on our website at http://www.watsonhall.com/terms/

Each check list should be amended and added to for the particular project requirements and environment.

References

The latest links to details of information security related legislation, codes of practice, organisations, initiative and standards can be found on the Watson Hall website at http://www.watsonhall.com/security/

Check list summary

Attribute	Text
Company	
Department	
Web application	
Completed by	
Comments	

Development and testing

Item	Required	Completed
Logical and physical diagrams of the development, testing and staging environments	□	□
Description of methodologies and techniques used for software development of the application	□	□
Description of methodologies and techniques used for security testing of the web application and subsequent changes and enhancements	□	□
Copy of configuration management and change control procedures	□	□
Copies of all change control requests relating to the application in the last 2 years	□	□
Schedule of audits and reviews undertaken in the last 2 years	□	□
Web application metrics and performance testing details	□	□

Network and hardware

Item	Required	Completed
Logical and physical diagrams	□	□
List of remote access methods and protocols	□	□
List of any hardware implemented components used within the web application which do not form part of the base system	□	□
Application hosting and connectivity		
List of agreements and contracts including dates and details of all parties	□	□
Service level agreements and actual performance in the last 2 years	□	□
Bandwidth guarantees and limits, and actual usage in the last 2 years	□	□
Availability (uptime) guarantees and limits, and actual performance in the last 2 years	□	□
Monitoring agreements and support contracts	□	□
Disaster recovery agreements	□	□
Schedule of all ongoing or planned hardware and network development projects that affect the application or its environment	□	□
List of other services, applications, protocols, ports and other software installed on the network and hardware which are not directly used by the web application or are used for other purposes	□	□

Software

Item	Required	Completed
Description of user groups, roles, geographical locations and permissions	□	□
Description of access control, authentication and session management mechanisms	□	□
Data collection, storage, sharing and dissemination policies and procedures	□	□
List of internal security policies (organisational, issue and system) that relate to the operation or use of the web application and its systems	□	□
List of purchased and developed software and their authors and other creators including information whether the author/creator made their contribution as a company employee under their employment contract, outside their employment, as a consultant or as an independent contractor	□	□
Software licences, assignments, contracts, beta testing agreements, warranties and guarantees	□	□
Application	□	□
Components within application	□	□
Third party click-wrap agreements required for the application to operate	□	□
Support and/or maintenance contracts	□	□
Product documentation and manuals	□	□
Third party software embedded	□	□
Other intellectual property embedded	□	□
Schedule of all ongoing or planned software, databases and related systems development projects that affect the application or its environment	□	□
List of agreements relating to third party website links, advertising, affiliate, co-branding, promotional, content provider, electronic data interchange, syndication, consumption and other agreements	□	□
List of any other capital or expense agreements not included in the item above	□	□
Details of application software escrow agreements or similar concerning source code access or use	□	□

Intrusion detection and prevention

Item	Required	Completed
List of routers including locations, manufacturer, model and rules	□	□
List of firewalls including locations, manufacturer, model and rules	□	□
List of access control policies, mechanisms and network segmentation	□	□
List of intrusion detection systems including manufacturer, model and rules (including network and host based detectors)	□	□
List of intrusion prevention systems (not included above) giving locations, manufacturers, model and rules	□	□
Product documentation and manuals for the previous four items	□	□
Patching policy and schedule for the last 6 months	□	□
List of logging systems and storage locations	□	□
Schedule of vulnerability assessments, penetration tests, code reviews and audits		
Dates and scope	□	□
Results	□	□
Risk mitigation undertaken	□	□
List of anti malware systems including locations, licences, update policy, incident reports and activity logs	□	□
Schedule of actual known information security breaches, exposures and other incidents relating to the web application for the last 3 years – identify countermeasures adopted	□	□
Copy of incident management procedure and details of any automates remediation capabilities	□	□

Domain names and certificates

Item	Required	Completed
List of domain names used by the web application or associated with any hardware of software used by the application (e.g. email domains and aliased domains)	□	□
List of tag holders, domain name servers and expiry dates for the above domain names	□	□
List and description of certificates (e.g. SSL and PKI) used by the web application	□	□

Intellectual property

Item	Required	Completed
List or prior ownership for technology in the preceding items	□	□
List of all names and abbreviations of the web application (including trading names if appropriate)	□	□
List of databases and locations	□	□
List of UK, EU and foreign trade names, brand names, service marks, trade marks, logos, strap lines and slogans associated with the application (registered and issued) - provide copies if applicable	□	□
List of UK, EU and foreign patents, patent rights, designs and innovations associated with the web application (registered and issued) - provide copies if applicable	□	□
List of copyright associated with the web application - provide information if applicable	□	□
List of wholly or jointly owned or proprietary technology necessary for the web application (including software, databases and other systems)	□	□
Copies of application terms of use, privacy statement, trademark usage guidelines, click wrap agreements (if applicable) and any policies (e.g. content, abuse, acceptable use)	□	□
Full details of people responsible for application, maintenance and protection of intellectual property rights and copies of correspondence from third parties regarding potential infringement of intellectual property rights of others	□	□

Partners

Item	Required	Completed
List of other companies, partnerships, individuals or other entities who are stakeholders in the web application	□	□
List of agreements with other companies for provision of or consumption of products and services – provide copies of the agreements if applicable	□	□
List of confidentiality and non-disclosure agreements relating to the web application to which the company is bound or imposes on others – provide copies if applicable	□	□
List of agreements or arrangements with company employees and shareholders or with any organisation they have a relationship with – provide copies if applicable	□	□
List of data sharing, distributorships, marketing agreements, co-packaging, reseller, franchises and referral agreements associated with the web application	□	□
Lists of any resellers and distributors of the application – if applicable provide copies of the written agreements.	□	□
List of data streams and formats provided to downstream third parties from the application including details of those third parties and the agreements	□	□

Customers and users

Item	Required	Completed
List of the application’s 20 largest customers (if applicable) in terms of sales and a description of purchases in the last 2 years	□	□
Schedule of unfulfilled orders	□	□
List and explanation for any major customers lost over the last 2 years	□	□
Description of security awareness training and services (if applicable) provided to users of the web application	□	□
Description of methods customers and users can report security issues including phishing	□	□
List of areas where user supplied content is republished or recorded	□	□
List of overdue payments including costs and timescales	□	□

Employees, other staff and sub-contractors

Item	Required	Completed
List of key employees who work on the application for development, testing, operation or security and an organisation chart showing line management and functional relationships	□	□
Number of employees and other staff (temporary, voluntary, supporters, etc) by department and by functional area associated with developing, operating and securing the application, including an indication of the percentage of their work that this involves	□	□
Contracts including information on confidentiality or non-competition agreements to which employees etc are subject to	□	□
List of specific agreements with employees, independent contractors or other third parties relating to the application’s development and operation such as indemnity agreements – provide copies if applicable	□	□
List of any other benefits in kind (relating to the web application) being provided	□	□
For each current and former consultants who work on the web application, a copy of their consulting agreement and confidentiality and agreement	□	□
Description of security awareness training provided and evidence of delivery over the last 2 years	□	□

Legislation, codes of practice and standards

Item	Required	Completed
List data controllers related to the web application, their registration numbers and describe the type of data held	□	□
Describe how the Distance Selling Regulations are implemented and enforced if applicable	□	□
List any mandatory compliance schemes (e.g. Payment Card Industry Data Security Standard PCIDSS, Committee of Advertising Practice CAP) the web application needs to comply with	□	□
List any optional compliance schemes (e.g. Fairtrade), standards (e.g. W3C, WAI), codes of practice (e.g. National Statistics, banking), accreditations (IDIS, ISIS) the web application complies with	□	□
List other business sector specific legislation which the web applications needs to comply with for the (e.g. Freedom of Information, Pressure Systems Safety Regulations, etc)	□	□
Evidence of compliance with all above items in this section	□	□
Copies of governmental licences or permits to operate in business sector of application, if applicable (e.g. Financial Services Authority)	□	□

Insurance and risk transfer

Item	Required	Completed
List and copies of all insurance policies of the company covering property, liabilities and operations relating the development, operation and securing of the web application	□	□
List of any special conditions imposed by insurers in respect of the web application	□	□
List of any other insurance policies in force related to the web application such as indemnification policies, business interruption, cyber insurance or product liability policies	□	□
Schedule of insurance claims history relating to the web application for past 3 years	□	□
Copy of the business continuity plan and schedule of tests undertaken	□	□
Copy of data backup and verification policies and procedures	□	□

Litigation, investigations and other disputes

Item	Required	Completed
List and description of actual, pending or threatened litigation, claims and other disputes relating to the web application	□	□
List and description of local or national government and their agencies of regulatory investigations, requests for information or enquiries relating to the web application	□	□
Correspondence relating to the matters requested in the two items above	□	□
Complaints by users about the web application	□	□
Legal guidance and opinions given to the company concerning the web application in the last 2 years	□	□
Correspondence and dealings concerning the company's rights or ownership of internet domain names, patents, trade marks, logos, copyright and other intellectual property associated with the web application	□	□
Any settlements, decrees, orders and judgements of courts or government agencies in the last 3 years	□	□
List of claims under any warranties provided through the application or its use, and the resolution of any such claims	□	□
List of data protection subject access requests	□	□
Press releases relating to the web application for the last 2 years	□	□

Why Watson Hall?

Watson Hall is an independent third party for review and consultation, undertaking web application security due diligence as a dedicated task or part of larger due diligence exercise.

To discuss any security matters in confidence and without obligation, telephone us on 020 7183 3710 or use the enquiry form on our website at http://www.watsonhall.com/form/

Watson Hall Ltd is a limited company registered in England no 6004969 at North Bastle, Gatehouse, Northumberland, NE48 1NG, United Kingdom.