



Helping you piece IT together

Computer Security Assurance Checklist



Copyright Notice

© 2005 BH Consulting IT Ltd. trading as BH Consulting, All rights reserved. This whitepaper is protected by copyright. Any reproduction of material of this whitepaper must be requested and authorised in writing from BH Consulting. Authorised reproduction of material must include all copyright and proprietary notices in the same form and manner as the original, and must not be modified in any way. Acknowledgement of the source of the material must also be included in all references. BH Consulting reserves the right to revoke such authorisation at any time, and any such use must be discontinued immediately upon notice from BH Consulting.

Disclaimer:

BH Consulting has made every reasonable effort to ensure that information contained within this document is accurate. However no representation or warranty, expressed or implied, is given by BH Consulting as to the accuracy or completeness of the contents of this document or any information supplied. Recommendations outlined in this document are based on accepted industry best practises.

The information contained in this document has been provided by BH Consulting for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate BH Consulting gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of BH Consulting will be corrected as soon as possible.

Any views, opinions and guidance set out in this document are provided for information purposes only, and do not purport to be legal and/or professional advice or a definitive interpretation of any law. Anyone contemplating action in respect of matters set out in this document should obtain advice from a suitably qualified professional adviser based on their unique requirements.

The information in this document may contain technical inaccuracies and typographical errors. The information in this document may be updated from time to time and may at times be out of date. BH Consulting accepts no responsibility for keeping the information in this document up to date or any liability whatsoever for any failure to do so.

BH Consulting are under no obligation to update this document or correct any inaccuracies or omissions in it which may exist or become apparent.

Table of Contents

1. Computer Security Assurance Checklist	4
2. Contact Us	5

1. Computer Security Assurance Checklist

The following checklist will help you obtain better assurance regarding the information security risks facing your company. An incomplete or negative response to any of the following items means that area of risk needs to be addressed.

People	Check Item	Answer
Responsibility	Does a director, or equivalent, have responsibility for information security?	
Employee Buy-in	Have all members of staff given written acknowledgement that they have read, understood and accepted the information security policy?	
Employee awareness	Do all users on your computer systems receive regular training on their security responsibilities and how to identify and deal with various security threats?	
Training	Do staff members with specific security responsibilities receive proper and regular training to support their role?	
Computer security policy	Have you a documented security policy, with associated operating procedures, signed off and fully supported by senior management?	
Non-disclosure agreements	Does senior management authorise third party access to confidential and/or commercially sensitive information pending completion of appropriate confidentiality forms?	

Process	Check Item	Answer
Audits	Are critical systems such as firewalls and routers regularly tested for vulnerabilities and are computers checked to ensure no copies of illegal software are present?	
Incident Planning and response	Are documented and frequently tested plans in place, with clearly defined roles and responsibilities, to ensure the company can respond to any security breaches such as a virus attack, fraud or natural disasters such as fire?	
Passwords	Are all default passwords on all systems reset from the default vendor installed passwords? Are users forced to use complex and hard to guess passwords?	
Software patches	Is there a mechanism to ensure that critical security patches are deployed to systems in a timely and audited fashion?	
Data Protection	Are systems and databases that store personal data secured properly to ensure compliance with regulatory and legal requirements such as the Data Protection Act?	

Technology	Check Item	Answer
External Network Security	Are external connections, such as to the Internet, authorised by senior management, properly documented and secured using Firewalls and Intrusion Detection Systems?	
Anti-Virus	Are all computer systems protected with the most up to date anti-virus software? Are users educated on how to identify and deal with suspect files that may contain computer viruses?	
Content Monitoring	Do you properly monitor the content of emails and Internet browsing activity to protect your company from computer viruses, SPAM, or litigation due to the nature of the content?	
Monitoring	Are the log files of important security devices actively monitored to detect potential security breaches?	
Physical security	Are critical IT resources, such as file servers, secured in a secured area that is protected from unauthorised access?	

2. Contact Us



Helping you piece IT together

If you wish to contact us or provide any feedback on this whitepaper you may do so using the following contact details.

Telephone : +353-(0)1- 4404065
Website : <http://www.bhconsulting.ie>
Email : info@bhconsulting.ie