



## RISK MANAGEMENT GUIDE

### TERRORISM RISK ASSESSMENT QUESTIONNAIRE

	Yes	No	Comments / Actions required
Terrorism risk assessment completed and documented			
Risk assessment regularly reviewed and updated			
Risk assessment takes account of the possibility of:			
(i) a direct attack			
(ii) an attack on others in the neighbourhood			
(iii) an attack on suppliers or business partners			

<b>Security Awareness</b>	Yes	No	Comments / Actions required
Embedded in the company's culture			
Board level responsibility			
Terrorism awareness training for all staff			
Regular staff briefings and updates to notice boards			
Specific awareness and procedures training for security staff, receptionists, mail room staff, call handlers, etc			
Staff instructed to report any unusual or suspicious activity			
Staff advised to store within their mobile telephone address books: "In Case of Emergency (ICE)" contact numbers (See <a href="http://www.icecontact.com">www.icecontact.com</a> for details) The Anti-Terrorism Hotline number (0800 789 321)			

<b>Emergency Planning</b>	Yes	No	Comments / Actions required
Emergency plan completed, documented and circulated			
Emergency plan regularly reviewed and updated as necessary			
Emergency evacuation pack prepared and always readily available			
Staff emergency contact numbers kept up to date			
Plan covers communications: i) into the business from security authorities (public service broadcasts and city-based warning systems) ii) within the business to alert staff and activate emergency plan			
Roles and responsibilities clear and absences of key players addressed			
Training, including refresh and succession, addressed			
Search plans, evacuation routes, assembly areas, bomb shelters etc. carefully determined and clearly defined.			
Evacuation and assembly exercises carried out at suitably frequent intervals			
Scenario-based tests and exercises (desk-top and/or full-scale, as considered appropriate) carried out at suitably frequent intervals			

<b>Housekeeping / supervision</b>	Yes	No	Comments / Actions required
External and internal public/communal areas kept clean, tidy and uncluttered to assist surveillance and reduce opportunities for concealment			
Rooms and cupboards kept locked when unattended			
Clear desk / clear floor policy			
Thorough perimeter security checks at beginning and close of day			
Regular security patrols of car parks and open yards			

<b>Access control</b>	Yes	No	Comments / Actions required
All entry points to buildings continuously locked or directly supervised			
Tight control over entry to car parks and loading areas			
High profile security presence immediately apparent to visitors			
Strictly enforced policy on management and supervision of visitors and contractors			
Staff identity badges and visitors'/contractors' passes worn at all times			
Bag and belongings searches if premises are a "front line" target			
Electronic access control systems maintained in good condition and regularly audited. Lost and non - returned cards deleted from system			

<b>Physical security &amp; electronic surveillance</b>	Yes	No	Comments / Actions required
Doors and windows maintained in good condition and adequately secured			
Windows and other glazed areas suitably protected with anti-shatter film / bomb-blast curtains if indicated by risk assessment			
Gates and fences maintained in good condition. Gates adequately secured			
Adequate external security lighting installed and regularly checked			
All potential unauthorised entry points and high risk or vulnerable areas protected by intruder alarm system and CCTV cameras			
CCTV images adequately monitored and continuously recorded			
Intruder alarm and CCTV systems regularly audited for coverage and performance. Systems maintained by approved contractors			
Regular security audits to ensure security arrangements meet changing environment and threat level			

<b>Information security</b>	Yes	No	Comments / Actions required
IT security policy reviewed with regard to the terrorist threat, and compliance audited on a regular basis			
IT security policy clearly communicated to all staff. Staff understanding checked. Non-compliance a disciplinary matter			
Robust and rigorously observed password protocols			
High quality anti-hacking and anti-virus protections installed and updated as necessary			

<b>Mail-handling procedures</b>	Yes	No	Comments / Actions required
Post and delivery handling procedures regularly reviewed and audited			
Clear guidance developed and communicated in regard to receipt of suspicious packages or mail			
Suitable mail scanning equipment in use and bomb-bins installed if the business is an obvious "front line" target			

<b>Staff recruitment</b>	Yes	No	Comments / Actions required
Staff recruitment policy reviewed with regard to the terrorist threat, and compliance audited on a regular basis			
References checked before employment is confirmed			
Close supervision of newly appointed employees, and of casual and agency staff			
Terrorism awareness training included in induction course			

<b>Business continuity</b>	Yes	No	Comments / Actions required
An impact analysis made of key business/operational processes and resources			
An assessment of vulnerabilities made and appropriate resilience to operational/business interruption put into place			
Continuity management strategy and Business Continuity Plan (BCP) in place capable of responding to the impact of a terrorist incident			
Roles and responsibilities clear and absences of key players addressed			
Training, including refresh and succession, addressed			
Scenario-based tests and exercises carried out (desk-top and/or full-scale, as considered appropriate) at appropriately frequent intervals			
Review and maintenance programmes in place			

Information set out in this document constitutes a set of general guidelines and should not be construed or relied upon as specialist advice. Therefore **MORE TH>N** accept no responsibility towards any person relying upon these Risk Management Guidelines nor accept any liability whatsoever for the accuracy of data supplied by another party or the consequences of reliance upon it.