

CRIME AND FRAUD EXPOSURE

SCORECARD

As a leader within your organisation, you want to trust your employees and the people you do business with. However, the sad reality is that no organisation is immune to the threat of crime and fraud. Indeed, some experts estimate that the private sector, including both SMEs and large enterprises, loses a total of £144 billion per year due to fraud. Making matters worse, the average time before organisations discover that fraud has occurred is 18 months, long after the damage has been done.

Unfortunately, the need for commercial crime insurance is often overlooked, with many organisations assuming that they have little to no risk at all. And, while maintaining strong internal controls should be a priority for any organisation, crime insurance provides an important safeguard against the actions of dishonest individuals.

With crime insurance, organisations can protect themselves against financial loss arising out of dishonest and fraudulent acts committed by their employees as well as the actions of non-employees.

To help organisations understand the level of risk they face on a daily basis, Bollington Insurance Brokers has developed the Crime and Fraud Exposure Scorecard.

INSTRUCTIONS: Please answer the questions below. After you have completed all of the questions to the best of your ability, add up your score and determine your organisation's level of risk by utilising the chart at the end of this document.

The following points will be assigned for each response:

- **YES:** 0 points
- **NO:** 3 points
- **UNSURE:** 3 points

Hiring and Employment Procedures

	YES	NO	UNSURE	SCORE
1. Does your organisation conduct prior employment checks, contact references and verify the educational credentials for all new employees?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2. Does your organisation conduct background and credit checks for all new employees?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3. Does your organisation periodically conduct background checks on current employees or when employees are promoted or transferred to sensitive positions?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Internal Controls

4. Does your organisation reconcile all bank accounts on at least a monthly basis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5. Are bank accounts reconciled by someone not authorised to deposit, withdraw or write cheques, or otherwise transfer funds from those accounts?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6. Are systems designed so that no single employee can control a transaction from beginning to end (eg, approve a voucher, request and sign a cheque)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7. Does your organisation require counter-signatures on all cheques over a certain amount?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
8. Are all incoming cheques stamped 'for deposit only' upon receipt?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

9. Does your organisation have procedures in place to approve expenses before issuing reimbursements to employees?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
10. Is a physical check and a count of inventory and equipment made on a regular basis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Audit Procedures				
11. Does your organisation have an audit department or a person who is responsible for internal audit procedures?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
12. If weaknesses are discovered by an internal auditor, are they required to be reported directly to the owners, partners, members or board of directors?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
13. Does your organisation have its financial statements audited by an outside firm on an annual basis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
14. Have all recommendations made by outside auditors been adopted?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
15. Do internal auditors have the authority to audit any record at any time?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
16. Do internal audits include all internet, IT and fund transfer functions?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
17. Does your organisation follow an auditing cycle that includes audits on both a regular and surprise basis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Computer Systems Controls				
18. Does your organisation have software in place to detect fraudulent computer usage by employees?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
19. Does your organisation require all passwords and access codes to be changed at regular intervals?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
20. Does your organisation immediately remove system access for inactive and terminated employees?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
21. Are passwords required in order to access sensitive information?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Supplier and Purchasing Controls				
22. Does your organisation maintain and utilise a list of approved suppliers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
23. Does your organisation have a system or set of processes for detecting payments to fictitious suppliers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
24. Are background checks performed on all suppliers to verify ownership and financial capability prior to conducting business with them?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
25. Is the responsibility for authorising suppliers, approving invoices and processing payments segregated among different employees?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Policies and Procedures				
26. Does your organisation have fraud, code of ethics and conflict of interest policies in place?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
27. Does your organisation have procedures that allow employees to confidentially report suspected fraud or theft?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
28. Are employees required to complete conflict-of-interest disclosure forms annually?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Physical Security				
29. Are former employees denied access to your organisation's property immediately upon termination?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
30. Does your organisation have physical controls (eg, an alarm or surveillance system) in place to restrict and monitor unauthorised access to your property?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

SCORE:	
---------------	--

MODERATE RISK: 0-18 points

HIGH RISK: 21-60 points

ESCALATED RISK: 63-90 points