CRIME AND FRAUD EXPOSURE SCORECARD

HORST INSURANCE

As a leader within your organization, you want to trust your employees and the people you do business with. However, the sad reality is that no organization is immune to the threat of crime and fraud. In fact, the Association of Certified Fraud Examiners estimates that organizations around the world lose approximately 5 percent of their annual revenue to illegal acts. Making matters worse, the average time before an organization discover that fraud has occurred is 18 months, long after the damage has been done.

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

With crime insurance, organizations 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 organizations understand the level of risk they face on a daily basis, Horst Insurance 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 organization's level of risk by utilizing 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 organization conduct prior employment checks, contact references and verify the educational credentials for all new employees?	☐	☐	☐	
2. Does your organization conduct background and credit checks for all new employees?	☐	☐	☐	
3. Does your organization periodically conduct background checks on current employees or when employees are promoted or transferred to sensitive positions?	☐	☐	☐	
Internal Controls				
4. Does your organization reconcile all bank accounts on at least a monthly basis?	☐	☐	☐	
5. Are bank accounts reconciled by someone not authorized to deposit, withdraw funds, write checks, or otherwise transfer funds from those accounts?	☐	☐	☐	
6. Are systems designed so that no single employee can control a transaction from beginning to end (e.g., approve a voucher, request and sign a check)?	☐	☐	☐	
7. Does your organization require counter-signatures on all checks over a certain amount?	☐	☐	☐	
8. Are all incoming checks stamped "for deposit only" upon receipt?	☐	☐	☐	

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

SCORE:	

MODERATE RISK: 0-18 points

HIGH RISK: 21-60 points

ESCALATED RISK: 63-90 points