Deloitte.

Fraud and Corruption Risk Assessment

Empowered lives.
Resilient nations.

Prevention Mechanisms and the Essential Skills Required for their Enhancement within the Context of the Jordanian Anti-Corruption Strategy

Stephen Crowe
Director - Deloitte Forensic, Dubai

10 June 2014

Arab Anti-Corruption and Integrity Network

Contents

To be updated

International Best Practice 3

Terminologies 4

Fraud and Corruption Control Plan 5

Risk Assessment Fundamentals 6

Fraud and Corruption Risk Assessment

- Overview 7
- Base Methodology 8
- Planning 9
- Corruption (Fraud) Risk Factors 10
- Control Effectiveness 11
- Determine and implement Treatment Action 12
- Fraud and Corruption Risk Matrix 13
- Risk Treatment Plan 14

Practical Exercise 15

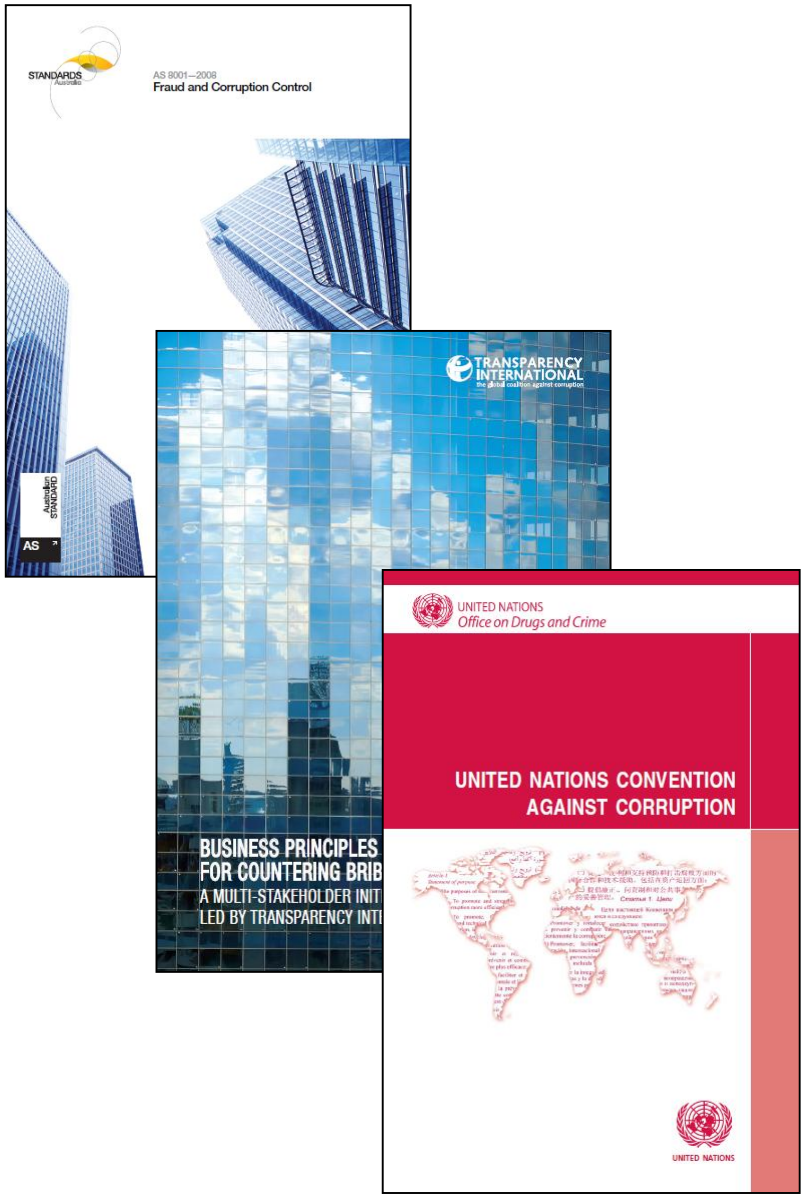
Fraud and Corruption Risk Assessment

International Best Practice

- Australian Standard (AS) 8001-2008 (Fraud and Corruption Control)
- AS/NZ ISO 31000 – 2009 (Risk Management Principles and Guidance)
- United Nations Convention Against Corruption (UNCAC)
- Transparency International's booklet titled 'Business Principles for Countering Bribery — TI Six Step Process'

Other guiding regulations

- Jordan National Anti-Corruption Strategy (JNACS, 2008 -2012)
- U.S. Foreign Corrupt Practices Act of 1977 (FCPA)
- U.K. Bribery Act
- 1997 Organization for Economic Co-operation and Development Anti-Bribery Convention
- U.S. Sarbanes-Oxley Act of 2002



Fraud and Corruption Risk Assessment

Terminologies

To be updated

Inherent Risk Rating (IRR)

- The assessment of a FCRA Scenario by *probability* (likelihood to occur) and *consequence* (magnitude of impact) prior to the consideration of controls.

Control Effectiveness Rating (CER)

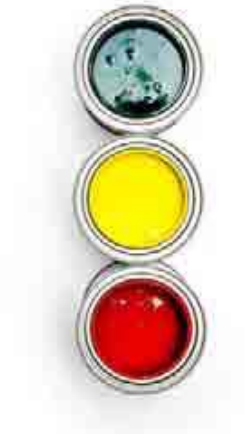
- Represents the overall design effectiveness of internal controls that mitigate the risk.

Residual Risk Rating (RRR)

- The risk remaining after factoring in the inherent risk rating and control risk rating for each identified Fraud scenario.

Risk Treatment Plan

- text



Fraud and Corruption Control Plan

Overview

It is important that to view the Fraud and Corruption Control Plan as an integral part of an overall risk management plan on the premise that fraud and corruption are business risks that are controlled by the application of risk management principles.

A Fraud and Corruption Risk Assessment is only a small, but important element within a Fraud and Corruption Control Plan.

Planning and Resourcing		
○	1.1	Fraud and corruption control planning
○	1.2	Review of the fraud and corruption control plan
○	1.3	Fraud and corruption control resource
○	1.4	Internal audit activity in the control of fraud and corruption

Prevention		
○	2.1	Implementing and maintaining an integrity framework
○	2.2	Senior management commitment
○	2.3	Line management accountability
○	2.4	Internal control
○	2.5	Assessing fraud and corruption risk
○	2.6	Communication and awareness
○	2.7	Employment screening
○	2.8	Supplier and customer vetting
○	2.9	Controlling the risk of corruption

Detection		
○	3.1	Implementing a fraud and corruption detection program
○	3.2	Role of the external auditor in detection of fraud
○	3.3	Avenues for reporting suspected incidents
○	3.4	Whistleblower protection program

Response		
○	4.1	Policies and procedures
○	4.2	Investigation
○	4.3	Internal reporting and escalation
○	4.4	Disciplinary procedures
○	4.5	External reporting
○	4.6	Civil action for recovery of losses
○	4.7	Review of internal controls
○	4.8	Insurance

Key

- No evidence of compliance
- Partially compliant
- Compliant
- Not Assessed

Source: AS 8001-2008: Fraud and Corruption Control

Risk Assessment Fundamentals

Probability and Consequence

An example of a risk assessment matrix; to assign the Inherent Risk Rating (IRR)

Probability							
	Expected to occur in most circumstances	**Almost Certain**	Medium	High	High	Very High	Very High
	Will probably occur in most circumstances	**Likely**	Medium	Medium	High	High	Very High
	Could occur at some time	**Possible**	Low	Medium	High	High	High
	Not expected to occur	**Unlikely**	Low	Low	Medium	Medium	High
	May occur only in exceptional circumstances	**Rare**	Low	Low	Medium	Medium	High
			Negligible	**Minor**	**Moderate**	**Major**	**Severe**
			Consequence				
			Impact on the function, or its objectives is negligible. Routine procedures would be sufficient to deal with the consequences. Minimal resource impost.	Would threaten an element of the function. May cause small delays or have minor impact on quality.	Would necessitate significant adjustment to the overall function and require corrective action. May have a negative impact on objectives	Would threaten goals and objectives; requires close management.	Would stop achievement of functional goals and objectives.

Fraud and Corruption Risk Assessment

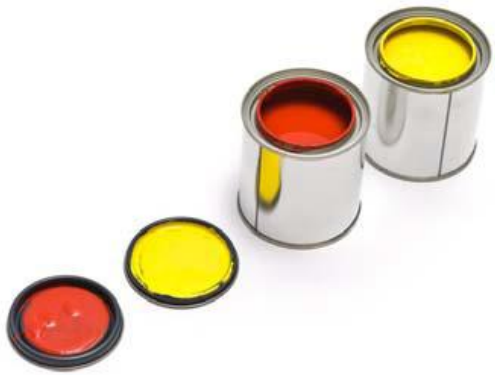
Overview

What is a Fraud and Corruption Risk Assessment ("FCRA")?

- ✓ An FCRA is a scheme and scenario based assessment that considers the various ways that fraud, corruption, and misconduct can occur within and against an organization, and is a crucial part of an entity's broader risk assessment process. An FCRA provides management with insight into potential fraud scenarios.
- ✓ It considers internal and external factors that contribute to fraud and corruption risk, and the effectiveness of existing controls.
- ✓ The output of an FCRA is a Fraud and Corruption Risk Register prioritizing identified risks from the most serious to least serious; and a Risk Treatment Plan with action items aimed at treating the risks.
- ✓ The Fraud and Corruption Risk Register should be a 'live document', and subject to full review every two years.

An FCRA does not:

- × State whether fraud or corruption has occurred or not occurred; or
- × Prevent fraud or corruption from ever occurring in the future at the Subject Entity.



Fraud and Corruption Risk Assessment

Base Methodology

Step		Approach
1	**Establish the Context and Identify / Evaluate Fraud and Corruption Risk Factors**	▪ Conduct fraud and corruption awareness sessions to selected company management to enhance their understanding of related risks, concepts, and scenarios; ▪ Conduct kick-off presentation to the leadership team, identify and evaluate fraud and corruption risk factors ▪ Conduct interviews and workshops with key executives, nominated section heads, managers and employees.
2	**Identify Fraud and Corruption Risk and Possible Scenarios and Schemes**	▪ Distribute FCRA survey and evaluate results ▪ Conduct interviews, workshops and walkthroughs to identify fraud and corruption risks and schemes ▪ Apply derived scenarios into a working risk matrix.
3	**Analyze Fraud Risks, Schemes and Scenarios and Identify and Evaluate Mitigating Controls**	▪ Define and determine probability and consequence criteria and apply to identified fraud risks to deduce an Inherent Risk Rating (“IRR”) for each risk; ▪ Facilitate the evaluation of control design and implementation through workshops and group discussions; ▪ Validate the evaluation of controls with process owners; and ▪ Determine the Control Effectiveness Rating (“CER”) for each control.
4	**Evaluate and Prioritize Residual Fraud Risks**	▪ Establish criteria to determine residual risk level and apply to each risk; and ▪ Evaluate Fraud and Corruption Risk Assessment results and prioritize residual risks.
5	**Create Fraud and Corruption Risk Profile and Develop Action Plans**	▪ Report on gaps in existing anti-corruption practices ▪ Construct Remediation plan for policy, procedure and system enhancements to improve fraud awareness, detection and prevention, enhance controls and minimize the risk of fraud and corruption

Fraud and Corruption Risk Assessment

Planning

To be updated and split

Information sources: -

1. **Stakeholder interviews:** Who are the people you need to canvas for risk factors and context?
2. **Process walkthroughs:** What processes are vulnerable to fraud and corruption risk?
3. **Workshops:** What functions / areas / levels are best represented; Team based brainstorming.
4. **Incident registers:** What has previously been reported? Scheme type and mechanisms.
5. **Previous risk assessments:** What were the identified risks? What has changed?
6. **Policies and procedures*:** Are these constructed within a Fraud and Corruption Control Plan?
7. **Industry research (peer reviews):** What are the prevalent risks encountered by peers / competitors?
8. **Employee / partner surveys:** What are the perceptions of your employees / partners?
9. **Data analytics**
    i. Financial / transactional data
    ii. Vendor / supplier data
    iii. Employee data
10. **Control environments**
    i. System based (access, permissions, audit logs)
    ii. Physical access
    iii. Procedural controls (e.g., segregation of duties)
    iv. Management controls (reviews and oversight; internal audit)
    v. External controls (external audit, regulatory, legislation)

Corruption Risk Assessment Methodology

Corruption (Fraud) Risk Factors

Typically, these may include:

- Corruption / Fraud has occurred before
- Allegations of Corruption / Fraud previously
- High level of market competition
- High level of cash transactions

The risk factors identified in the JNACS were:

- Inefficient anti-corruption measures caused by the spread of Nepotism “Wasata” and tolerant attitude of the society towards this phenomenon.
- Drop of Jordan’s rank on CPI.
- Inefficient asset recovery measures which enabled perpetrators of corruption acts to benefit financially from corruption, which consequently encouraged more wrongdoers to commit other types of crimes.
- Inefficient information exchange between public and private sector weakens asset recovery and affects investigation of corruption.
- Inefficient international cooperation at the operational level weakens asset recovery and investigation of corruption as a whole.

Fraud and Corruption Risk Assessment

To be updated

Control Effectiveness

In assessing the effectiveness of a control, the following three questions should be asked:

- Does the control address the risk effectively?
- Is the control officially documented and communicated?
- Is the control in operation and applied consistently?

Scoring…

Fraud and Corruption Risk Assessment

To be updated

Determine and implement Treatment Action

- **Avoid** the risk when it is considered too great a threat to the performance of a function or objective. This may involve modifying the function or objective; ie no longer operating a vulnerable line of business. This approach must be considered, and is rarely taken.
- **Accept** the risk because risk level is low and the existing controls are sufficient.
- Institute **treatment controls** or enhance existing controls to minimize as far as possible the probability and consequences of the risk when avoidance is not possible.
- **Transfer** the risk, for example through fidelity guarantee insurance and or business disruption insurance.

Control Treatments may include preventative measures such as:

- Enhanced tender / bidding processes
- Segregation / Rotation
- Due diligence
- Awareness program and enhanced communication
- Benchmarking prices / costs within industry and other external measures.
- Security and surveillance
- Employee screening
- ……further to be populated

Avoid generic recommendations. The treatment plan should have a level of detail that presents a action plan

Fraud and Corruption Risk Assessment

Risk Matrix - Example

Risk Ref #	Fraud Category	Fraud Description	Fraud Risk Scheme / Scenario	Inherent Risk 4 - HIGH 3 - MODERATE 2 - MINOR 1 - INSIGNIFICANT	Actual Controls identified	Control Risk EFFECTIVE PARTLY EFFECTIVE INEFFECTIVE	Additional comments	Residual Risk HIGH MODERATE MINOR INSIGNIFICANT
1	Information leakage	Leakage of information / theft of intellectual property	**Employee sells confidential or strategic information to an external party in return for a bribe.**	HIGH	Information Security User Policy Information on intellectual property is classified as restricted information within the Companys' Information Security Users Policy. Restricted classification applies to strategic business information, which is most critical and intended strictly for use within the Company (e.g. Merger and acquisition plans, Business plans, trade secrets, customer data, information security data, dealer pricing strategy, Strategy Documents.). Sharing of any information classified as restricted is not permitted. Relevant controls: 1) Users shall take necessary precautions actions to ensure privacy and confidentiality of the Company data contained in laptop hard disk. 2) Employees are not permitted to bring any personal information storage media. 3) All official media containing sensitive corporate information should be accounted for with an audit log. 4) All e-mail messages are considered as company records. Secure printing identifies what and when information is being printed, through employee access card.	PARTLY EFFECTIVE	**Recommendations:** a) Perform an EDP audit to ensure that controls as described in the policy are effective. b) Review of access permissions to documents / folders containing sensitive documents, employing a 'need to know' principle. c) Review policies on personal email and social networking to personnel. d) Consider disabling access to external devices on a needs considered basis. e) Ensure print logs maintained / archived in searchable format for an appropriate period of time (e.g. 6 months). f) Ensure secure printing is fully deployed and used by staff. g) Perform periodic / adhoc reviews on audit and print logs to identify irregular activities (IT Security).	SIGNIFICANT
6	Corruption	Corrupt Payments - Government Officials	**Government employee seeks a bribe from Government Relations staff.**	HIGH	Other than the Code of Conduct, there is no Government Relations policy / procedure prohibiting bribery of government officials.	INEFFECTIVE	**Recommendations:** a) Create a specific code of conduct for Government Relations staff, to include an annual acknowledgement on their understandings of anti-bribery and corruption regulations within the Company b) Create a Government Relations SOP that outlines the procedures relevant to dealings with government departments and officials.	SIGNIFICANT
2	Leasing Scheme	Illegal usage of properties	**Tenant uses residential premises for illegal use, pays look-away payment to security / leasing staff.**	HIGH	Residential contract specifies that the tenant must comply with all laws and regulations . We are advised that periodic audits and spot checks are conducted by Group Security. This risk carries significant reputational risk, in the event that personnel are perceived as being complicit in illegal or criminal activities within leased premises.	PARTLY EFFECTIVE	**Recommendations:** a) Ensure that this risk is captured as a reputational risk. b) Review incident reporting processes, to ensure that appropriate actions are followed in the event of reported illegal activity.	MODERATE

Fraud and Corruption Risk Assessment

Risk Treatment Plan - Example

Ref no:	Category of fraud:	Fraud Scenario:	RRR:	Reason for treatment:	Recommended Action:	Person Responsible:	Due by:	Revised Residual Rating:
1	**Bypass controls**	Item with insufficient technical specification is incorrectly categorized as "Out of policy" process in order to initiate exceptional/urgent items, thereby bypassing controls.	**HIGH**	Potential method of fraudulently obtaining goods	Establishment of a post - event reconciliation process, which would review the justification, and effect the retrospective compilation of required documentations.			
2	**Approval level avoidance**	Splitting of purchase orders to ensure each individual invoice would remain beneath an approval threshold.	**HIGH**	By passing authority levels for inappropriate reasons	SAP detective control to identify multiple transactions near authority limits. Analysis on repetitive / sequential bids from the same supplier.			
3	**Bid rigging**	Contractors or vendors collude to set artificially high prices to the detriment of the Company.	**HIGH**	Potential third party fraud against Company	Develop Industry knowledge of pricing. SAP analysis of pricing history			
5	**Conflict of Interest.**	Employees of Company use silent partnerships/equity arrangements with suppliers in order to receive benefits.	**MEDIUM**	Potential for bribery and corruption	Update policy and procedure manual to provide specific policy tailored for buyers			

Fraud and Corruption Risk Assessment

Practical Exercise – Explanatory Note

Pending

The practical exercise (pending) will involve syndicating the attendees into three groups. They will have 3 tasks, each to take about 10 minutes. They will be provided with a basic profile of an entity which they are conducting an FCRA on.

Step 1: In the first 10 minutes, each group will be provided with two corruption descriptions, they will be asked to:-

- Categorize the risk
- Compact into a clear 'corruption risk scenario'
- Consider the 'probability' and 'consequence' and assign an Inherent Risk Rating

Step 2: In the second 10 minutes, each group will be provided with the controls identified to the presented risks. From this, they will:-

- Assess the Control Effectiveness Rating
- Calculate the Residual Risk Rating

Step 3: In the last 10 minutes, each group will compile a treatment plan:-

Work on the scenarios is continuing…

Notes

Notes

Notes

Notes