

LOCATION:

DATE: 24 January 2003

		<u>Comments or cross reference to working papers</u>	<u>AFI X ref</u>
<b>1.</b>	<b><u>CONTROL ENVIRONMENT</u></b>		
1.1	<p><b>Risk: Organisational structure does not help maximise operational efficiency.</b></p> <p>Consider:</p> <ul style="list-style-type: none"> <li>◆ Organisation structure is appropriate for the size, operating activities, and location of entity.</li> <li>◆ Duplication of responsibilities/tasks does not exist in the current organisational structure.</li> <li>◆ Management review and modify (when necessary) the organisational structure in light of changed conditions.</li> </ul>		
1.2	<p><b>Risk: Lack of knowledge, skills and experience among staff.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ Standard procedures exist for hiring, training, motivating, evaluating, and developing staff.</li> <li>◆ Appropriate training and mentoring programmes exist. The training includes instruction in relevant laws, regulations and internal policies.</li> <li>◆ Periodic job performance evaluation and review is performed for each employee.</li> <li>◆ Clear and measurable personal objectives are set, which are related to business objectives.</li> <li>◆ Staffing is appropriate, particularly with regards to knowledge and experience.</li> <li>◆ Written job descriptions and reference manuals exist</li> </ul>		

LOCATION:

DATE: 24 January 2003

		<u>Comments or cross reference to working papers</u>	<u>AFI X ref</u>
1.3	<p><b>Risk : Management and/or staff undertake unethical or unauthorised actions and commitments.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ Management have access to and are familiar with GPDs.</li> <li>◆ Procedure is in place to provide a framework within which the expectations in GPD HR 401, Core Values (e.g. re commitment to diversity and equality, and re standards of conduct) are met reliably and consistently.</li> <li>◆ Core Values are communicated to all management and employees (e.g. Code of Conduct is provided to all employees; and understood by them.)</li> <li>◆ Managers are seen to lead by example and set high standard of conduct, without an unduly relaxed attitude to risk and control issues.</li> <li>◆ Employees recognise their personal responsibility for the practical application of the Core Values.</li> <li>◆ There is evidence that management act on signs of inappropriate practices and/or violations of the code of conduct.</li> <li>◆ Staff do not cut corners to meet short-term targets.</li> <li>◆ Commitment to integrity and ethics is communicated effectively throughout the organisation, both in words and deeds.</li> <li>◆ The Human Resources department takes up references for new employees, particularly those with access to sensitive functions or data.</li> <li>◆ Summary of Authority Limits is in place, and covers key requirements (e.g. those in current Group Policy Documents).</li> <li>◆ Internal delegation of Summary of Authority Limits is in place.</li> <li>◆ Delegation of authority is established, current and is in compliance with corporate policy.</li> </ul>		
1.4	<p><b>Best practice in financial and administrative matters is not followed.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ The Departmental Manager or other management supervise the function effectively.</li> <li>◆ Key staff (identify) are qualified, experienced and committed.</li> <li>◆ Staff turnover is not excessive, especially at manager and supervisor level.</li> <li>◆ BU Policies &amp; Procedures Manual (where appropriate) is available, up to date, and understood.</li> <li>◆ The policies and procedures are clear, communicated, updated and revised on a timely basis.</li> <li>◆ Internal Policies &amp; Procedures Manual is available and up to date.</li> <li>◆ ISO 900x certification or alternative is in place where applicable and up to date.</li> </ul>		

LOCATION:

DATE: 24 January 2003

		<u>Comments or cross reference to working papers</u>	<u>AFI X ref</u>
1.5	<p><b>Risk : Best practices are not shared with other businesses.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ Proactive methods exist within BU to share best practice.</li> <li>◆ BU contributes to cross-BU and cross-Portfolio best practice sharing.</li> <li>◆ Management (are required to) proactively identify best practices that would be worth adopting in similar businesses.</li> </ul>		
1.6	<p><b>Risk: Non-compliance with legislation.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ Policies and procedures are in place to ensure local laws and regulations are identified and complied with.</li> </ul>		
<b>2.</b>	<b><u>BUSINESS OBJECTIVES AND RISK MANAGEMENT</u></b>		
2.1	<p><b>Risk: Business objectives are not effectively identified or achieved.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ Business identifies objectives which are specific and measurable, but which still address the fundamental strategies / requirements for its success. (Objectives may be defined in conjunction with the Annual Plan, or otherwise).</li> <li>◆ Business's objectives are effectively communicated to staff, so that employee commitment is obtained.</li> <li>◆ Business objectives are translated into effective, specific activity-level objectives relevant to all significant business processes.</li> <li>◆ Critical success factors are identified (and, or hence, objectives are prioritised).</li> <li>◆ Achievement against objectives is adequately (objectively) monitored and reported.</li> </ul>		
2.2	<p><b>Risk : Human resources are inappropriate to achieve business objectives.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ Management believe business's headcount and quality of staff are adequate to achieve objectives. Key staff support objectives.</li> <li>◆ Organisation structure changes dynamically in line with changes in the business or industry environment.</li> <li>◆ Succession planning has been adequately addressed.</li> </ul>		

LOCATION:

DATE: 24 January 2003

		<u>Comments or cross reference to working papers</u>	<u>AFI X ref</u>
2.3	<p><b>Risk : Key risks are not identified and where possible mitigated or managed.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ The entity is involved in the annual, BU risk assessment performed in accordance with the guidelines issued by the Director, Reporting and Control, in such a way that risks critical to the entity's success are identified and given necessary attention.               <ul style="list-style-type: none"> <li>The assessment should consider risks as per Turnbull Committee guidance, i.e. those "related to market, credit, liquidity, technological, legal, health, safety and environmental, reputation, and business probity issues".</li> </ul> </li> <li>◆ The risk assessment is translated into appropriate risk management strategies visible at entity level. (These should evaluate the risk significance, the likelihood of that risk occurring, and the most effective way of managing or mitigating it).</li> <li>◆ Other entity-level mechanisms exist to identify changes in risks from external and internal sources, and to anticipate, identify and react to routine events or activities that affect achievement of business or activity-level objectives.</li> </ul>		
2.4	<p><b>Risk : Recovery from a disaster is delayed.</b></p> <p>Confirm that :</p> <ul style="list-style-type: none"> <li>◆ An adequate business continuity plan is in place and that it has been prepared in accordance with the 'Disaster Recovery Plan - Notes' issued by the Chief Information Officer on 26/9/01.</li> <li>◆ The plan addresses the four 'areas of concentration' (general areas of exposure) identified in the notes, namely:               <ul style="list-style-type: none"> <li>-Risk to staff, contractors and visitors.</li> <li>-Loss of communications capacity (voice, fax, data).</li> <li>-Loss of computer processing capacity.</li> <li>-Loss of primary workspace or vital facilities.</li> </ul> </li> <li>◆ The plan covers the normal life cycle of a disaster set out in the notes               <ul style="list-style-type: none"> <li>-Emergency Response for damage containment.</li> <li>-Interim plan - alternative actions</li> <li>-Restoration of normal operations.</li> </ul> </li> <li>◆ There is a named individual responsible for maintaining the plan and improving it (refer Characteristics of a Disaster Recovery Plan per the notes).</li> <li>◆ When the plan was last updated</li> <li>◆ The plan covers all of the business locations</li> <li>◆ The plan is tested regularly</li> </ul>		
3	<b>CONTROL ACTIVITIES</b>		

LOCATION:

DATE: 24 January 2003

		<u>Comments or cross reference to working papers</u>	<u>AFI X ref</u>
3.1	<p><b>Risk : No marketing Strategy / Inadequate information for marketing strategy</b></p> <p>Consider:</p> <ul style="list-style-type: none"> <li>◆ Marketing plan / strategy available.</li> <li>◆ Sufficient marketing knowledge and experience for technical and commercial employees.</li> <li>◆ Sufficient employees in sales / marketing department.</li> <li>◆ Market research are conducted and other relevant information are properly structured (economic, customer and industry trends – customer preferences, competitive products, technical innovations of competitors, development in demand in total market, market shares, quantity /margin/ price developments).</li> <li>◆ Legal / regulatory issues are monitored.</li> </ul>		
3.2	<p><b>Risk : Poor communication to market</b></p> <p>Consider:</p> <ul style="list-style-type: none"> <li>◆ Advertising campaigns are evaluated</li> <li>◆ Brochures are up-to-date.</li> <li>◆ Pricing strategy are evaluated through comparing with competitors.</li> </ul>		
3.3	<p><b>Risk : No optimum match with customer need</b></p> <p>Consider:</p> <ul style="list-style-type: none"> <li>◆ Customer needs are communicated to ensure product are not excessively expensive.</li> <li>◆ Production has direct contact with customer to understand more customer needs.</li> <li>◆ Sales department has adequate product knowledge (product awareness).</li> <li>◆ Actual customer information system is in place (plan to expand, history record of previous orders, changes in production etc.)</li> </ul>		

<b>4.</b>	<b>INFORMATION AND COMMUNICATION</b>		
4.1	<p><b>Risk: Significant internal and external information is not properly identified, captured and reported on a timely basis.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ The format, content and frequency of reported information has been determined and scheduled.</li> <li>◆ Information is fit for purpose.</li> <li>◆ No redundant data is reported.</li> <li>◆ Management identify missing and untimely information.</li> </ul>		

LOCATION:

DATE: 24 January 2003

4.2	<p><b>Risk: Internal communication process is inefficient.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ Regular departmental meetings are held to discuss and review relevant issues. Minutes of these meetings are made.</li> <li>◆ Policies and procedures are available to facilitate and control the communication process.</li> <li>◆ Management provides various communication channels (e.g. suggestion box scheme) to promote a free and open environment for employees to raise issues, opinions etc.</li> </ul>		
4.3	<p><b>Risk: Unreliable information as a result of poor IT systems.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ Approve service level agreements with information processing service providers are in place.</li> <li>◆ Processor and network resources are sufficient to enable adequate on-line response and timely processing.</li> <li>◆ Ongoing technical support is adequate to resolve problems quickly and effectively.</li> </ul>		
5.	<p><b><u>MONITORING</u></b></p>		
5.1	<p><b>Risk: KPIs and objectives are not monitored.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ Clear set of KPIs are in place.</li> <li>◆ Management regularly review standard against actual and deviations are analysed and reported.</li> <li>◆ Detailed action plan is available with complete indication of the responsible person, due dates, follow up. Periodic monitoring is made.</li> <li>◆ Processes exist to monitor that company adjusts controls effectively when objectives or the business environment change.</li> </ul>		
5.2	<p><b>Risk: No system of monitoring of material risks arising from all significant payroll activities.</b></p> <p>Consider :</p> <ul style="list-style-type: none"> <li>◆ Procedures are in place to periodically evaluate the effectiveness of internal controls, to report deficiencies to appropriate personnel and to modify policies and procedures.</li> <li>◆ Departmental plans are regularly reviewed and when necessary revised to meet changing external conditions.</li> </ul>		

LOCATION:

DATE: 24 January 2003

5.3	<b>Risk : Known areas for improvement are not addressed.</b>  Consider : <ul style="list-style-type: none"><li>◆ Management monitor to ensure that agreed actions from reports by internal &amp; external bodies (e.g. Audit, ISO 900x auditors, Health &amp; Safety examinations) are implemented.</li><li>◆ Adequate internal monitoring (e.g. internal quality audits) occurs, and identified areas for improvement are addressed.</li></ul>		
-----	---	--	--