Collaborative Assurance & Risk Design™ ("CARD®")

Advanced Level

Paisley Consulting is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be addressed to the National Registry of CPE Sponsors, 150 Fourth Avenue North, Suite 700, Nashville, TN, 37219-2417. Website: www.nasba.org.

Collaborative Assurance & Risk Design™

Advanced

2655 North Sheridan Way, Suite 150
Mississauga, Ontario, Canada, L5K 2P8
Tel: 905 823 5518 / Fax: 905 823 5657
www.paisleyconsulting.com

COLLABORATIVE ASSURANCE & RISK DESIGN™ ADVANCED

WORKSHOP OUTLINE & CONTENTS

Tim J. Leech, FCA·CIA, CCSA, CFE, MBA

Tim J. Leech is Principal Consultant & Chief Methodology Officer with Paisley Consulting, the world's leading provider of integrated business accountability software and training solutions. From 1991 to 2004 Tim was CEO and founder of CARD®*decisions*, a global pioneer in the ERM and CRSA areas. Paisley Consulting acquired CARD®*decisions* in June of 2004. Other positions he has had include Managing Director of a subsidiary of the Hambros Bank, Director Control & Risk Management Services with Coopers & Lybrand Consulting, and a range of comptrollership and internal audit roles with Gulf Canada. Tim was elected Fellow of the Institute of Chartered Accountants Ontario in 1997 in recognition of distinguished service to the auditing profession.

Leech's responsibilities include providing design advice on all Paisley Consulting software products; consulting and training services related to Sarbanes-Oxley, Basel operational risk management, enterprise-wide risk and assurance management; Collaborative Assurance & Risk Design™ ("CARD®") training and software development; control and risk self-assessment ("CRSA") training and implementation services; specialized litigation support services; business ethics advisory services; internal audit training and consulting; and control/risk governance consulting services. He has provided training for public and private sector staff located in Canada, the U.S., the EU, Australia, South America, Africa and the Middle and Far East. Leech has received worldwide recognition as a pioneer and thought leader in the fields of enterprise risk and assurance management and control and risk self-assessment.

Some of Leech's experiences and achievements include:

- pioneering and developing Collaborative Assurance & Risk Design ("CARD®") an integrated, enterprise-wide risk and assurance management and reporting approach that has been recognized globally as a leading edge corporate governance best practice;
- developing workshops and e-learning training modules on ERM, Sarbanes-Oxley, Basel and Internal Audit skills;
- numerous T.V. appearances, a national radio show, and scores of articles in professional journals on risk management, internal control, business ethics, and fraud related topics;
- authoring technical papers in response to exposure drafts of risk and control governance studies and frameworks in the U.S., the U.K., and Canada including Sarbanes-Oxley regulations and reports by the Treadway Commission, COSO Committee, Cadbury, and CoCo internal control research projects;
- contributing technical material related to CSA/CRSA including the IIA report CSA: Making the Choice and the IIA research study CSA: Experience, Current Thinking and Best Practices;
- co-author of an FEI Research Foundation research study Control Deficiency Reporting: Review and Analysis of Filings During 2004, and a new book published by Risk Books - Sarbanes-Oxley: A Practical Guide to Implementation Challenges and Global Response;
- delivery of expert witness services and testimony during civil and criminal actions related to fraud, secret commissions, conflict of interest, breach of contract, and officer/director due diligence;
- member of the IIA's ERM & CSA Conference Advisory Panel since the conference's inception and author of a practice exam for CSA specialist certification;
- Primary author of CARD *map* software - the world's first Collaborative Assurance and Risk Design™ groupware. At Paisley Consulting Tim has responsibility for providing input and advice on the design and features available in all Paisley Consulting software and training products including the company's flagship product, Risk Navigator, as well as CARD *map*, Focus, and AutoAudit;
- served as a board member of the Canadian Centre for Ethics and Corporate Policy, authored a column titled Duty of Care and has written a wide range of articles and made presentations on ethics related issues;
- provides expert opinion responses to SOX questions for Compliance Week's Remediation Center; and
- Contributor to articles on Basel II and SOX to the U.K. publication Global Risk Regulator and the National Post in Canada.

Bruce McCuaig, CA·CIA, CCSA
Principal Consultant - Collaborative Assurance & Risk Design, Paisley Consulting

Bruce's experience as an assurance professional, business executive and consultant spans over 30 years. Bruce is an award winning author, workshop leader and frequent speaker on risk management, professional audit standards, internal audit practices and governance issues. He recently completed the ICD Directors Education Program at the Rotman School of Business.

At Paisley Consulting, Bruce's practice area involves providing consulting, training and strategic implementation advice related to Sarbanes-Oxley (and related Canadian legislation), Basel II Operational Risk, Enterprise Risk Management, corporate governance practices, and control and risk self-assessment.

In this capacity, Bruce is actively and creatively integrating Paisley Consulting's extensive body of domain knowledge, propriety intellectual property and conceptual tools in the field of risk management and assurance and related methodologies with the Paisley Consulting's acclaimed assurance software solutions.

Prior to joining Paisley Consulting, Bruce held senior executive positions with Gulf Canada in Calgary and Toronto and Gulf Oil Corporation in Houston, Texas.

Bruce's work experience includes extensive audit and financial management in the oil and gas industry, both upstream and downstream, as well as exposure to the mining and banking sectors.

WORKSHOP OBJECTIVES

This training workshop has been designed to provide work unit and assurance personnel with state of the art skills and knowledge in control and risk design and assessment. Participants will be equipped to:

1. Define, assign and prioritize risk and assurance universes.
2. Identify and rank risks that threaten the achievement of business objectives.
3. Design high impact, lowest possible cost control portfolios that reflect organizational risk tolerance and support cost reduction initiatives.
4. Drive out clear descriptions of residual risk status to improve risk management decision making, increase work unit ownership and drive continuous improvement.

This training workshop has been designed to provide work unit and assurance personnel with state of the art skills and knowledge in control and risk design and assessment. Participants will be equipped to:

5 Knowledgeably assess the strengths and weaknesses of various control and risk models, approaches and assessment tools.

6 Develop user requirements for risk management and assurance information systems and more knowledgeably evaluate software options currently available.

7 Provide world class collaborative assurance and risk design services.

OUTCOMES FROM WORLD CLASS COLLABORATIVE ASSURANCE & RISK DESIGN™

1. Increased confidence and likelihood business objectives will be achieved.
2. More conscious and knowledgeable risk management decisions at all levels including more defensible decisions on capital allocations.
3. The Board of Directors and senior management have greater confidence that management at all levels is prudently managing significant risks and reporting candidly on the state of control and risk.
4. Greater confidence that the cost of control is optimal - i.e. the lowest level possible given the organization's risk tolerance.
5. More tangible value and payback from all assurance spending including the money allocated for internal audit, external audit, safety, environment, quality, risk and insurance and others.
6. Higher overall levels of customer satisfaction with the work done by specialist groups such as internal audit, external audit, safety, environment, risk and insurance and others.

COLLABORATIVE ASSURANCE & RISK DESIGN™

Traditional Auditing

Self-Assessment

Assurance Specialist(s)

Examines, documents and verifies controls and/or risk status

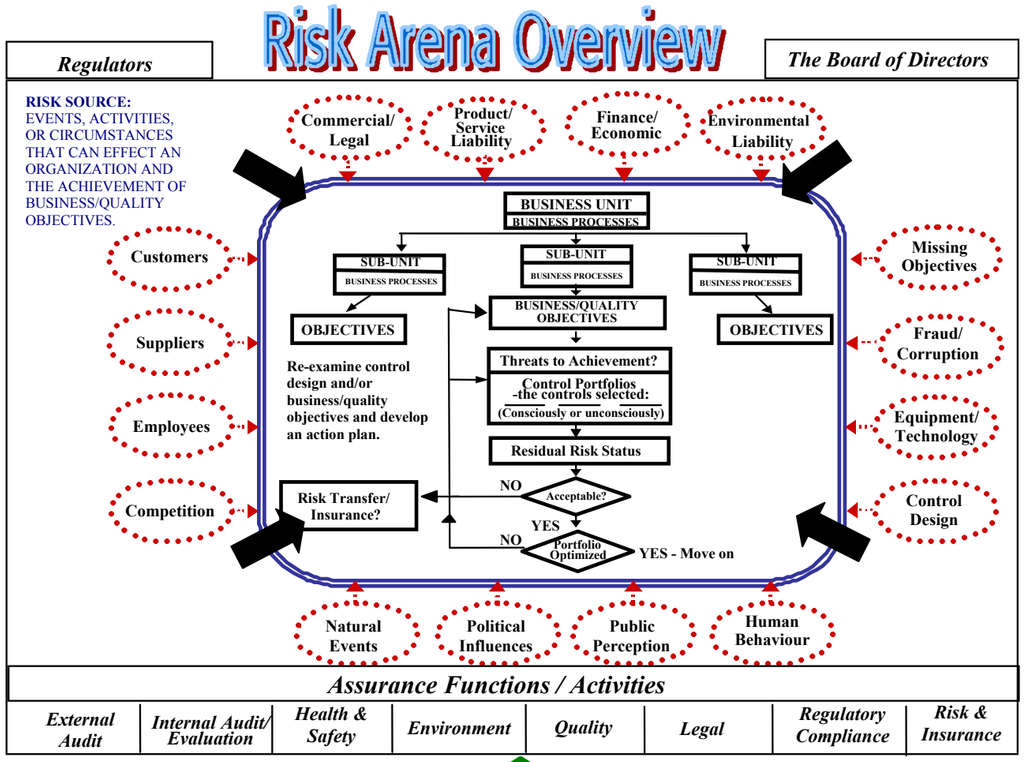
Product: Assurance Specialist's report/opinion on control effectiveness ***(Direct report auditing)***

Assurance Approach

Management/ Work Units

Analysis of risks, processes, controls relating to business objectives

Product: Specialist assurance related to management's report on control/risk status ***(Attestation auditing)***



CARD® *imperatives*

1) **Increase confidence that important current and future business/quality objectives will be achieved with an acceptable level of residual risk.**
2) **Reduce the cost of control to the lowest level possible that results in acceptable levels of residual risk.**
3) **Increase the amount of reliable information on significant risks being accepted across the organization.**
4) **Improve the ability of the Board and senior management to assess how well work units are identifying, measuring, and mitigating key risks.**
5) **Fully integrate the efforts of all assurance functions and reduce the assurance burden imposed on work units.**
6) **Increase the capability and motivation of work units to design, assess, improve, and report on control and risk systems.**
7) **Reduce the overall amount of inspection required. Build quality in, not on, to control and risk management systems.**
8) **Increase clarity and agreement on the areas stakeholders want assurance on and the level of assurance they require.**
9) **Dramatically increase the value added by internal and external audit and other assurance providers.**
10) **Increase the value added as a result of risk transfer/financing activities.**

Deciding on the Right Mix of Assurance Strategies

Direct Report Assessment
Approach Options:

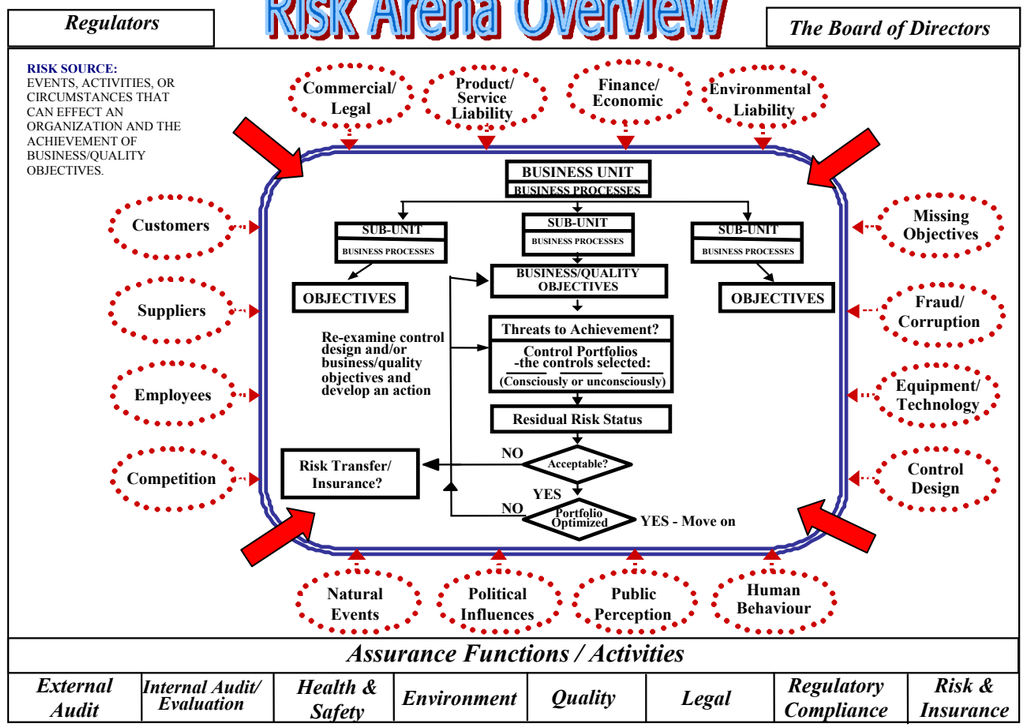
- **DR #1** Compliance/ Inspection Focus
- **DR #2** Business Process Focus
- **DR #3** Business Objective Starting Point
- **DR #4** Risk Starting Point
- **DR #5** Control Criteria Evaluation

Direct Report

Assurance Specialist(s)

Examines, documents and verifies controls and/or risk status

Risk Arena Overview



Self-Assessment

Management/ Work Units

Analysis of risks, processes, controls relating to business objectives

Product: Assurance Specialist's report/ opinion on control effectiveness/status

(Direct report auditing)

Assurance Approach

Product: Specialist assurance related to management's report on control/ risk status
(Attestation auditing)

Self-Assessment
Approach Options:

- **SA #1** Compliance Self-Assessment
- **SA #2** Business Process Focus
- **SA #3** Business Objective Starting Point
- **SA #4** Risk Starting Point
- **SA #5** Control Criteria Evaluation

RISK FITNESS QUIZ

Risk Assessment

How do you identify and measure the threats/risks that could impact on the achievement of your business objectives?

Control Assessment

How healthy are your control frameworks? How long has it been since you evaluated their effectiveness?

Control Cost Optimization

Could you eliminate some controls and still have an acceptable residual risk level at a lower overall cost?

Risk Testing the Future

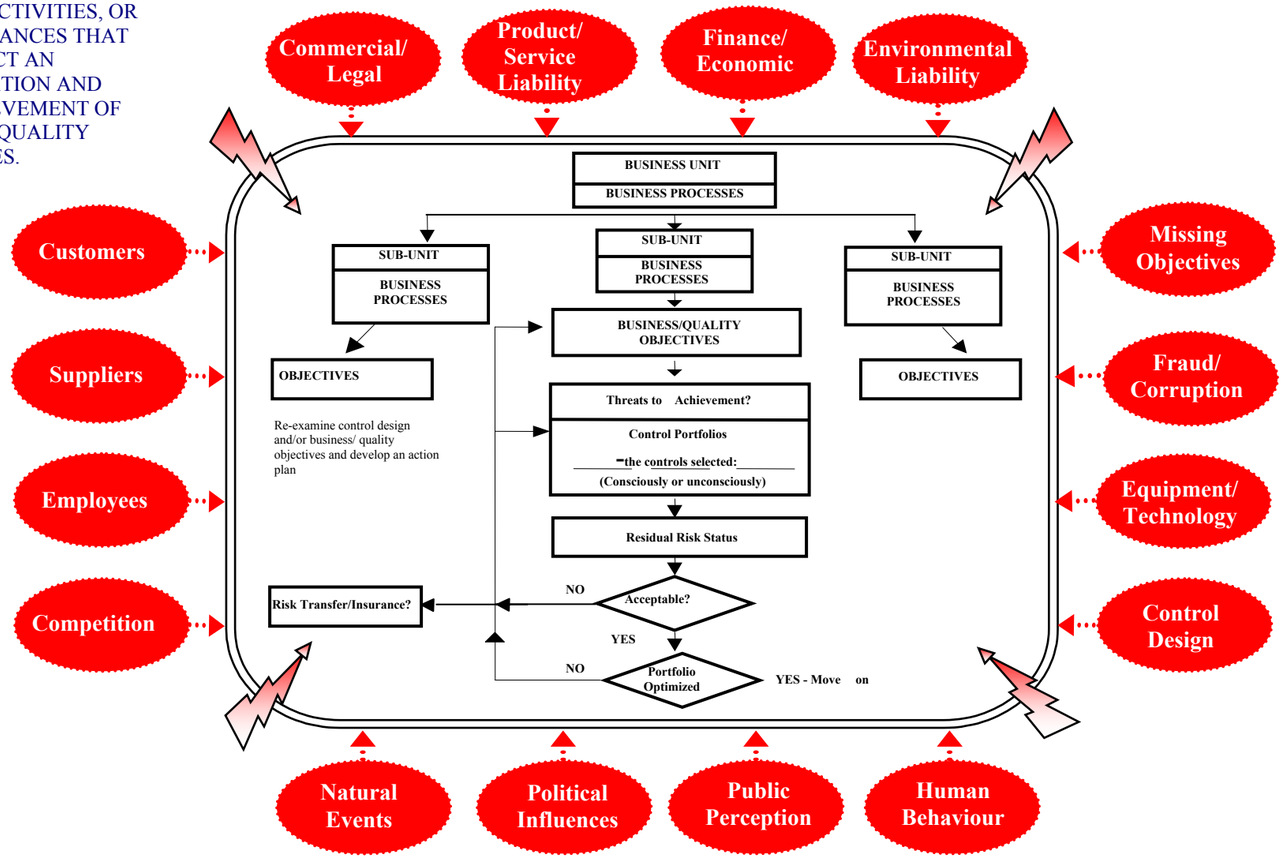
Do you consider and evaluate risks when making important business decisions and preparing strategic plans?

The Business Risk Arena

Regulators

The Board of Directors

RISK SOURCES
EVENTS, ACTIVITIES, OR CIRCUMSTANCES THAT CAN AFFECT AN ORGANIZATION AND THE ACHIEVEMENT OF BUSINESS/QUALITY OBJECTIVES.



Assurance Functions/Activities

External Audit	*Internal Audit/Evaluation*	*Health & Safety*	*Environment*	*Quality*	*Legal*	*Regulatory Compliance*	*Risk & Insurance*

Planning for Serious Risk Situations

Do you have contingency plans in place to deal with low probability, high risk situations that could cripple your unit or the company? Do you periodically revisit these plans to reassess their adequacy?

Worst Case Scenarios

Have you considered the possibility of high risk situations which, if they occurred together, could have a devastating effect on the company?

Oversight Process

Does Senior Management and the Board of Directors understand the major risks the company faces and take steps to ensure work units are identifying, measuring, controlling and monitoring risks?

Regular Reevaluation

Do you periodically reassess the acceptability of your risk acceptance decisions?

Risk Transfer/Financing Options

Have you considered risk transfer and insurance options available to avoid or reduce the consequences of specific threats/risks to your business objectives?

Early Warning Systems

Do you regularly monitor your risk status for early warning signs that changes are needed to your controls and/or objectives?

DEFINING THE RISK & ASSURANCE UNIVERSE

Section Objectives:

(1) Introduce participants to leading approaches to develop comprehensive risk and assurance universes.

(2) Provide an opportunity to debate the strengths and weaknesses of the main options available.

(3) Improve the ability of participants to define end result business/quality objectives.

(4) Provide a foundation that work unit staff and/or auditors can use to construct or refine a risk and assurance universe for their organization.

Simply Worded:
What's Included And What's Not?

BACKGROUND

In order to define a risk and assurance universe some key questions should be answered first:

1. What is a risk and assurance universe?

   A risk and assurance universe establishes the scope of risk and/or assurance work setting boundaries, on what is, and is not, included. This is done using some combination of subjects, topics, processes, objectives, locations or other criteria.

Simply put, a risk and assurance universe defines:
The universe people want information on.

2. What purpose(s) will the risk and assurance universe serve?

   Options include:

   (a) a basis to report to the board of directors, or the equivalent in the public sector, on the topics, locations, issues or objectives that have been or will be covered by review work and those that are in the universe but will not be covered;

   (b) a base for planning assurance activities and making decisions on where to allocate available assurance personnel (i.e. where and what to audit or the location a CRSA workshop will be conducted);

   (c) a tool management can use to monitor achievement levels and significant risks that threaten the achievement of entity and work unit objectives;

   (d) a core element of a Service Level Agreement between one or more assurance groups and their customers that specifies the scope or territory that is covered by the terms of engagement (an analogy would be a checklist of the items an auto garage will include in their service work);

   (e) a monitoring/early warning system to identify and address issues that could threaten the compensation of the senior managers involved;

   (f) all of the above;

   (g) other.

3. Who needs to be able to access the universe, update information, and use the data?

   If the purpose(s) of the universe is very broad, the universe must be very broad. An example of broad mandate the universe must serve would be:

   > *Management and audit are required to report all significant residual risk situations that have the potential to significantly impact on the organization and the achievement of its objectives.*

An example of a much narrower mandate is:

> *Internal audit is required to report significant risk and/or control situations they encounter in the course of their audits that could cause external financial statements to be materially misstated.*

Historically, risk and assurance universes have primarily been created and maintained to serve relatively narrow needs of internal audit, safety, environmental audit and others. They have almost always been fragmented and stored in various places in the organization.

This is changing rapidly!!!!

Information needs are escalating!!!!

REGULATORY TRENDS EXPAND THE UNIVERSE

Regulatory trends are forcing organizations to broaden the scope of the risk and assurance universe. An example is Principle 4 in the Basle Committee report on Internal Control Systems in Banking Organizations:

> **Principle 4:**
> ***Risk Recognition and Assessment***
> **An effective internal control system requires that the material risks that could adversely affect the achievement of the bank's goals are being recognised and continually assessed. This assessment should cover all risks facing the bank and the consolidated banking organisation (that is, credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk). Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks.**

(Framework for Internal Control Systems in Banking Organizations, Basle Committee on Banking Supervision, September 1998.)

CHANGES IN CIVIL DUTY OF CARE EXPANDS THE UNIVERSE

The Canadian Institute of Chartered Accountants in a publication titled "Guidance for Directors - Governance Processes for Control" recommends directors ask broad, sweeping questions of senior management.

Sample questions about risk and control include:

> *Are major risks and opportunities identified and related control objectives set? How are new risks, opportunities and control requirements identified?*
>
> *Are control systems monitored for effectiveness? Against what criteria? By whom?*

Courts and lawmakers in many countries have been expanding civil and regulatory expectations of the duty of care expected of senior management and Boards of Directors.

CHANGES IN THE DEFINITION OF CONTROL EXPANDS THE UNIVERSE

Control in many organizations has been closely linked to accounting, financial control and compliance.

In 1992 COSO, the U.S. control study, proposed a definition of control that formally added regulatory compliance and effectiveness and efficiency of operations to the definition of control.

> *Internal control is a process, effected by an entity's board of directors, management and other personnel, designated to provide reasonable assurance regarding the achievement of objectives in the following categories:*
>
> - *Effectiveness and efficiency of operations.*
> - *Reliability of financial reporting.*
> - *Compliance with applicable laws and regulations.*
>
> *The control environment provides an atmosphere in which people conduct their activities and carry out their control responsibilities. It serves as the foundation for the other components. Within this environment, management assesses risks to the achievement of specified objectives. Control activities are implemented to help ensure that management directives to address the risks are carried out. Meanwhile, relevant information is captured and communicated throughout the organization. The entire process is monitored and modified as conditions warrant.*

The CICA in Canada expanded this definition in 1995 with the release of the CoCo study.

> *Control comprises those elements of an organization (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organization's objectives.*

As the agreed definition of control changes so does the scope of assurance and risk management universes in many organizations.

CHANGES IN THE DEFINITION OF ASSURANCE

In 1999 the Institute of Internal Auditors standards section proposed a radical new definition of assurance that imposes broader responsibilities on assurance providers.

> *Assurance*
>
> *An opinion rendered by a professional internal auditor on a **specific or general component** of the framework of professional practice that the organization's management:*
>
> - *understands risk exposures*
> - *implements appropriate risk management*
> - *balances risk and control adequately - control strategies are relative to risk management strategies*
> - *accommodates changes effectively.*

(Draft Definition of Internal Auditing, IIA, January 11, 1999)

The key question is what is included in the "specific or general component"?

LEADING APPROACHES TO DEFINING RISK & ASSURANCE UNIVERSES

A wide range of approaches to define risk and assurance universes currently exist. Nine approaches that could be used by assurance groups to monitor, assess and report on control and risk are shown below. Some are very traditional and have been used for decades. Others are very new and represent radical departures from traditional thinking. The universe in most of these methods is not explicitly described. Many imply that they cover all parts of an organization and all activities. This is rarely the case!!!

Assurance Resource Allocation Options	
1.	Straight cyclical coverage. All parts of the assurance universe covered over some predefined time period.
2.	Based on requests from senior management.
3.	Using a scoring formula maintained by internal audit which allocates points based on: (1) Annual sales volume (2) Assets at risk (3) Time since last audit (4) Previous audit rating
4.	Based on a scoring formula maintained by internal audit which allocates risk points related to the following categories: (1) Property risk (2) Monetary assets (3) People risk (4) Commercial risk (5) Information (6) Legal Regulatory Risk (7) Political (8) Operational
5.	Based on a scoring formula maintained by internal audit that scores each business unit on their overall "Risk Fitness". 10 questions are scored individually from 1 to 10 possible points. Each score indicates the degree with which the organization manages or completes each activity or process describing the question (i.e. the quality). The maximum possible Risk Fitness score is 100. The questions to be scored are: (1) How do you identify and measure the threats/risks that could impact on the achievement of your business objectives? (2) How healthy are your control frameworks? How do you know? How long has it been since you evaluated their effectiveness? (3) Could you eliminate some controls and still have an acceptable residual risk level at a lower overall cost? How do you monitor this? (4) Do you consider and evaluate risks when making important business decisions and preparing strategic plans? How? (5) Do you have contingency plans in place to deal with low probability, high risk situations that could cripple your unit or the company? Do you periodically revisit these plans to reassess their adequacy? (6) Have you considered the possibility of high risk situations that, if they occurred together, could have a devastating effect on the company? How? How often?

Assurance Resource Allocation Options

(7) Do you regularly monitor your risk status for early warning signs that changes are needed to your controls and/or objectives? How?
(8) Have you considered risk transfer and insurance options available to avoid or reduce the consequences of specific threats/risks to your business objectives?
(9) Do you periodically reassess the acceptability of your risk acceptance decisions? How?
(10) Does Senior Management and the Board of Directors understand the major risks the company faces and take steps to ensure work units are identifying, measuring, controlling and monitoring risks?

6. Based on results derived from anonymous voting workshops. In the workshop people in the business unit vote on the degree to which they believe their unit manifests control criteria in a specified control model such as COSO, CoCo, CARD®*model*, and discuss any concerns identified. This results in a score for each control category in the model and an overall score. Units with low control model conformance scores receive more assurance attention.

7. Based on a risk formula developed by internal audit that uses 19 variables. The variables used are listed below. Ratings are assigned by internal audit judgementally based on available knowledge and information.

(1) Quality of Internal Control
(2) Competence of Management
(3) Integrity of Management
(4) Size of Unit ($)
(5) Recent Change in Accounting System
(6) Complexity of Operations
(7) Liquidity of Assets
(8) Recent Change in Key Personnel
(9) Economic Condition of Unit
(10) Rapid Growth
(11) Extent of Computerized Systems
(12) Time Since Last Audit
(13) Pressure on Management to Meet Objectives
(14) Extent of Government Relations
(15) Level of Employees' Morale
(16) Audit Plans of External Auditors
(17) Political Exposure
(18) Need to Maintain an Appearance of Independence by Internal Auditor
(19) Distance from Main Office

8. Based on performance indicator information on how well objectives are currently being achieved. This information may be input into an integrated risk management system by work units and/or assurance personnel. Performance Indicators input by work units are quality assured by assurance staff independent of the work unit. Objectives with "Very Negative" performance indicator status and high risk to the organization ratings are allocated the most assurance resources.

9. Based on the quality assurance reviews of control and risk self-assessments generated by work units. Units which generate highly reliable, candid self-assessment disclosures are allocated less assurance resources than units that produce incomplete and/or untruthful self-assessments.

DECIDING ON A CORE STARTING POINT TO BUILD A RISK AND ASSURANCE UNIVERSE

Underlying the 9 options shown above are assumptions about the scope of the risk and assurance universe. The scope will be impacted by who will be using the risk and assurance universe and for what purpose(s).

Groups that are potential contributors and/or users of risk and assurance universes include:

1. Internal auditors only.

2. Internal auditors, senior management and the Board of Directors.

3. Internal auditors and other assurance groups such as environmental audit, safety, quality, external auditors, etc.

4. Auditors, work unit personnel and senior management.

5. All assurance players including work units, senior management, boards of directors, internal audit, external audit, safety, environment security, etc.

One approach to seeking clarity on the risk and assurance universe is to use a "Universe Scoping Tool".

A sample of a Risk & Assurance Universe Scoping Tool organized by category of objective is shown on the next page.

GROUP EXERCISE:

Assume the members of your group are the top 10 executives of this company. The company is a 10 billion dollar per year petro-chemical firm with operations at 40 sites around the world. You currently have an internal audit department with 15 professional staff. Complete the table shown below.

RISK & ASSURANCE UNIVERSE SCOPING TOOL - BY OBJECTIVE CATEGORY

Category of Objectives	Include in I.A. Scope Yes / No	Assign to Another Staff Group Yes / No	Require Management/ Work Unit Report on Status Yes / No
Product Quality (PQ)			
Customer Service (CS)			
Minimizing Unnecessary Costs (MUC)			
• Feedstock/Raw Material Costs			
• Manufacturing Costs			
• Admin. Costs			
• Capital Costs			
• Maintain/Grow Market Share			
• Maintain Margins			
Reliable Business Information (RBI)			
• Reliable External Reporting of the Financial Statements			
• Reliable Production Reporting			
• Reliable Operating Statistics			
• Reliable Budget/Actual Reporting			
Asset Safeguarding (AS)			
• Cash			
• Inventory			
• Corporate Information			
• Intellectual Property			
Safety (S)			
• Employee			
• Contractor			

RISK & ASSURANCE UNIVERSE SCOPING TOOL - BY OBJECTIVE CATEGORY

Category of Objectives	Include in I.A. Scope Yes / No	Assign to Another Staff Group Yes / No	Require Management/ Work Unit Report on Status Yes / No
• Community			
• Customer			
Regulatory Compliance (RC)			
• Environment			
• Health & Safety			
• Securities			
• Human Rights			
• Other			
Fraud Prevention (FP)			
• Employee Fraud/Theft			
• Vendor Fraud/Theft			
• Corporate Fraud/Theft			
• Other Fraud/Theft			
Continuity of Operations (COO)			
• Ensure Adequate Feedstock/ Raw Material Supply			
• Ensure Systems are Y2K Compliant			
• Ensure Availability of Critical Business Information Systems			
• Ensure Availability of Critical Plant Operating Computer Systems			
Unintentional Risk Exposure (URE)			
• Compliance (IC)			
• Compliance with Ethical Standards			
• Compliance with Company Policy			
• Compliance with Customer Contracts			
• Compliance with Vendor Agreements			

In addition to categories of objectives shown above, other scope definition criteria can be substituted.

Other scoping criteria options include:

1. Listing each department, function, or geographic location in an organization (e.g. Treasury Accounting, Manufacturing, Human Resources, etc.).

2. Listing all core business processes and sub processes (e.g. Sales Generation, Sales Taking, Sales Fulfillment, Disbursement, Hiring, Manufacturing, etc.).

3. Listing all categories or sources of risk (e.g. technology, political, human error, and fraud).

4. Listing areas, topics or issues that regulators demand evidence of risk management and/or control assessment.

The simple questions to be answered are:

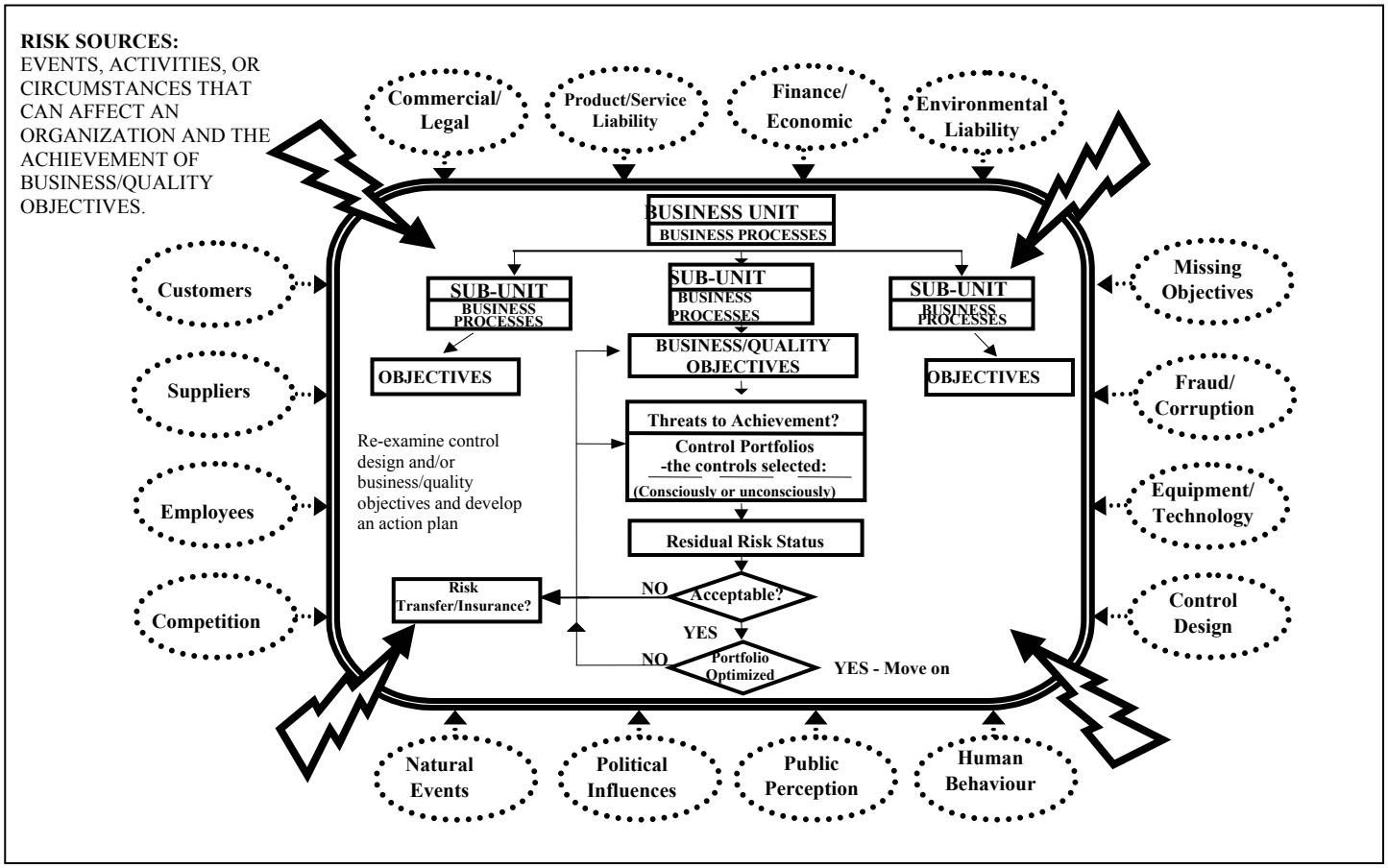
Who wants assurance?

On what?

With what level of assurance?

CONSTRUCTING THE UNIVERSE USING END RESULT BUSINESS OBJECTIVES

R I S K A R E N A O V E R V I E W



GENERAL GUIDELINES

1. Objectives should state what the organization and/or business unit wants to achieve as desired end results, as opposed to specific plans, methods, steps, procedures and/or tools being used to accomplish the objectives. For example, running weekly safety meetings is not an end in itself. Minimizing accidents, preventing loss of life and controlling related costs, are usually the real desired results.

---

2. Ensuring that specific task delegations are being carried out and that corporate policy and laws are complied with are valid business objectives.

   This is true even in cases where the prescribed procedure, task or legal requirement does not relate to any other valid business objective. The prescribed procedure, task, or law may even be counterproductive to achieving the stated goals of the organization.

   When situations like this are identified, steps should be taken to have the defined task or policy changed or eliminated immediately. Laws and regulation can sometimes be influenced as well. Only by analyzing how all tasks and procedures relate to a relevant business/quality objective(s) can these situations be identified and eliminated.

---

3. A common mistake is thinking that a means to an end is an end in itself.

   For example:

   Ensure that all budget to actual variances are reviewed and explained by the manager responsible.

   The real objectives should be: prevent journal entry coding errors, prevent fraudulent transactions, minimize costs, increase the probability of achieving the organization's objectives, etc.

   A budget to actual review is only <u>one</u> way of achieving these objectives.

   Often, when tasks or processes are described as objectives, people lose sight of what the task was originally designed to achieve as an end result.

POINTS TO REMEMBER

1. Objectives frequently conflict with each other. Managing conflicting objectives is one of the most essential and difficult responsibilities of staff at all levels.

For example:

- Ensuring uninterrupted availability of computer systems will be in conflict with minimization of costs in most situations.
- Compliance with the law may conflict with maximization of revenues and/or minimization of costs.
- Providing excellent customer service may, on occasion, mean breaking policy.

2. Objectives may be sub-objectives of core business/quality objectives. All valid objectives should be traceable to an organization's core business and quality objectives.

For example:

- Prevention of errors, irregularities and fraud is usually a sub-objective of other objectives such as minimization of costs, excellent customer service, compliance with statutes, compliance with contracts or maximization of revenues.

3. Objectives may be organization specific/unique as a result of a board or management directive.

For example:

- Some companies have decided to be very proactive on matters related to the environment. They often establish objectives beyond what is required by the law. Other examples exist in the areas of safety, sex discrimination, sexual harassment and many other areas.

OBJECTIVES AND CONTROLS - PITFALLS TO AVOID

1. **Becoming so obsessed with a particular control that one loses sight of what is to be accomplished.**

   For example believing budgets should be perfect, believing that project management is an end in itself, or believing that historical procedures should be continued long after the need/purpose is gone.

2. **Not considering all options available to attain one's objectives due to a lack of training or knowledge**.

   Examples include: believing that more auditors is the only way to improve product quality or reduce the incidence of fraud and waste, believing that disk labelling is the only way to ensure that the correct tape is loaded into computer systems, believing that more rules and policies will correct all problems, etc.

3. **Inadequate consideration of the impact of one's choices in relation to other relevant objectives.**

   For example staffing a department to ensure all requests will be met within 4 hours regardless of the impact on cost.

4. **Focusing on a single control to mitigate specific Threats to Achievement.**

   Example: A Threat to Achievement might be staff do not comply with policy. A simplistic response might be to assign auditors to audit compliance on a frequent basis. In real life most threats are not adequately addressed by just one control. This approach frequently provides a false sense of comfort. The approach used in this training assumes a collection of controls will be necessary in most cases.

Distinguishing Between What Is To Be Achieved And Ways To Achieve Business/Quality Objectives

GROUP EXERCISE

Materials Management Department
A Canadian Hospital (ACH)

		Objective or Sub-Objective (What?)	Way to Achieve an Objective (How?)
1.	All book to physical adjustments must be authorized by a person segregated from the responsibility for physical custody of the goods.	☐	☐
2.	An up to date disaster/contingency plan must be maintained and tested at least twice annually to determine the ability of purchasing stores and distribution to function in the event of major equipment of software failure.	☐	☐
3.	Ensure that staff have no conflicts of interest that are impairing, or could be seen to be impairing, their objectivity and ability to perform their assigned duties.	☐	☐
4.	Establish a Product Standardization Committee and assign responsibility for monitoring and controlling the usage of materials and supplies.	☐	☐
5.	Provide exemplary patient care.	☐	☐
6.	Develop and carry out educational programs in a variety of disciplines.	☐	☐
7.	Provide high quality, cost effective products and services.	☐	☐
8.	Manage resources provided to the ACH effectively.	☐	☐
9.	Minimize the cost of gasoline used in ACH vehicles.	☐	☐
10.	Establish and fund an Internal Audit function.	☐	☐

Distinguishing Between What Is To Be Achieved And Ways To Achieve Business/Quality Objectives

GROUP EXERCISE

Materials Management Department
A Canadian Hospital (ACH)

		Objective or Sub-Objective (What?)	Way to Achieve an Objective (How?)
11.	Install and maintain an annual budgeting and performance reporting system.	☐	☐
12.	Stay current on the latest developments in hospital management techniques through industry associations, journals, and informal network contacts.	☐	☐
13.	Maintain a continuous supply of materials and supplies to support teaching, research and patient care.	☐	☐
14.	Minimize ACH's investment in, and cost of carrying, inventories of materials and supplies.	☐	☐
15.	Maintain a vehicle maintenance system that documents the maintenance history of all ACH vehicles.	☐	☐
16.	Ensure all purchases of goods are accurately accounted for in the records.	☐	☐
17.	Provide all staff that are involved in acquiring and transferring goods with training on the related systems and procedures.	☐	☐
18.	Ensure all materials and supplies transfers are accurately accounted for on a timely basis.	☐	☐
19.	Ensure that staff do not create and maintain unauthorized "off-book" inventories of materials and supplies.	☐	☐
20.	Minimize the overall cost to ACH of meeting ACH's needs for goods and services.	☐	☐

Distinguishing Between What Is To Be Achieved And Ways To Achieve Business/Quality Objectives

GROUP EXERCISE

Materials Management Department
A Canadian Hospital (ACH)

	Objective or Sub-Objective (What?)	Way to Achieve an Objective (How?)
21. Assign direct responsibility for ensuring that staff comply with material acquisition policies to the unit heads of all areas that have been delegated responsibility for purchasing goods and services.	☐	☐
22. Minimize the administrative costs incurred per $1,000 of goods purchased.	☐	☐
23. Periodically compare the administrative cost per $1,000 of goods purchased to that of other hospitals and obtain explanations for any significant variances.	☐	☐
24. Minimize the cost of storing the materials and supplies necessary for the hospital's operations.	☐	☐
25. Establish a separate unit called "Environmental Services" and assign responsibility for ensuring the ACH is in compliance with all applicable environmental laws and regulations.	☐	☐
26. Ensure goods are transported to their assigned destination by the required delivery time.	☐	☐
27. Ensure the specific goods/supplies requested are the goods that are shipped.	☐	☐
28. Segregate the responsibility of staging supply loads from the responsibility of verifying contents prior to shipment.	☐	☐
29. Provide training to materials management staff on the names and intended purpose of goods and supplies they deal with in their daily work.	☐	☐

Distinguishing Between What Is To Be Achieved And Ways To Achieve Business/Quality Objectives

GROUP EXERCISE

Materials Management Department
A Canadian Hospital (ACH)

		Objective or Sub-Objective (What?)	Way to Achieve an Objective (How?)
30.	Install and maintain a minimum reorder point (MRP) inventory management system which tracks and reports inventory levels and locations.	☐	☐
31.	Periodically inventory materials and supplies on hand and compare physical quantities to book inventory quantities.	☐	☐
32.	Minimize internal theft of ACH materials and supplies.	☐	☐
33.	Develop and communicate to all staff and vendors a ACH Code of Conduct.	☐	☐
34.	Minimize damage to ACH vehicles due to traffic accidents and the related repair/replacement costs.	☐	☐
35.	Minimize injury to people transported by ACH vehicles.	☐	☐
36.	Require all ACH personnel responsible for the operation of vehicles to complete an initial 2 day defensive/safe driving course and a half day update program each year.	☐	☐
37.	Comply with all environmental laws relating to the incineration of ACH waste.	☐	☐
38.	Assign specific responsibility for legal compliance with relevant laws to all supervisory employees who are affected, or may be affected, by the relevant legislation.	☐	☐

Sample Draft Objectives For A Federal Park

A BLEND OF PUBLIC AND PRIVATE SECTOR BUSINESS/QUALITY OBJECTIVES

Note: Not all of these objectives comply with the guidelines described in this workbook. They are included for illustration purposes and may not be the actual objectives of public sector employees who operate parks and campgrounds.

CAMPGROUND OBJECTIVES

1. Maintain roads within campground sites at a minimum cost and at quality standard that is not detrimental to visitor satisfaction.

2. Minimize the incidence and magnitude of visitor accidents on the property including:

   A. Beaches
   B. Roads
   C. Sites
   D. Natural Areas
   E. Rec Areas
   F. Facilities

3. Provide a peaceful and secure environment that facilitates/allows for a positive National Park experience.

4. Bring the campground site(s) in line with the department vision for a federal park within 5 years.

5. Minimize damage to the natural environment in the campgrounds and surrounding area.

6. Increase visitor's appreciation of and commitment to preservation of the natural environment and eco system.

7. Maintain facilities at or above Sanitation/Functionality Standards.

8. Maintain or improve the functionality and appearance of the campground sites.

9. Minimize the cost of campground maintenance and security services.

10. Provide an enjoyable and memorable camping experience for visitors.

11. Minimize cost of interpretation services.

CAMPGROUND OBJECTIVES (Cont'd)

12. Minimize cost of core services to visitors.

13. Maximize revenues generated by campgrounds.

14. Prevent and detect employee fraud including theft of funds and conflicts of interest.

15. Safeguard wildlife in campgrounds against illegal acts.

16. Safeguard the possessions of visitors from theft/damage.

17. Ensure visitors are treated equitably, pleasantly, and courteously at all times by team members and vendors working on the site.

18. Increase the net tourist/visitor $ contribution to the local economy.

ASSIGNING & RATING THE RISK & ASSURANCE UNIVERSE

Section Objectives:

(1) Introduce participants to techniques to assign and prioritize risk and assurance universes.

(2) Provide practical techniques work units can use to select the topics or objectives they should spend time analyzing using CRSA or other analysis approaches.

(3) Provide techniques assurance groups can use to decide where to perform direct report audits that will produce maximum payback to the organization and highest customer satisfaction ratings.

Simply Worded:
Who's Accountable, What To Look At,
And When To Look At It?

THE TASK OF DECIDING WHAT TO ANALYZE

Once agreement is reached with customers on the risk and assurance universe, the next critical step is deciding which parts of the universe should be analyzed. Depending on an organization's culture and assurance strategy, assessment work may be undertaken by work units only, auditors and other specialists only, or some combination of both.

GROUP EXERCISE:

Listed below are situations common to a household environment. The family that lives in this 2 storey home is comprised of a father 45 years with a Bachelor of Commerce degree, a mother 43 years of age with a nursing background, a son 17 and daughter 15. Total household income is $125,000 per annum. In your assigned group list considerations and factors that would be most relevant in deciding: (1) the risk each item represents to the household before considering controls; and (2) who, if anyone, should be assigned responsibility for the items shown. The worksheet on the next page has been provided to record ideas generated by your group. The purpose of the exericse is to show the range of factors people consider when rating risk and assurance universes and making decisions on accountability assignment.

Items	Risk of Non-Achievement H M L	Accountability Assignment
1. Prevent injury and/or deaths caused by the gas furnace that heats the home (this is a Canadian home).		
2. Minimization of unnecessary costs related to food purchases.		
3. Security of information stored on the family computer.		
4. Prevention of damage due to roof leaks and plumbing failures.		
5. Minimization of unnecessary costs related to major appliance purchases.		
6. Compliance with speed limit legislation by the three licensed drivers in the household.		
7. Maintenance/acquisition of adequate household income to meet family requirements.		
8. Ensure son and daughter comply with alcohol and drug legislation to avoid jail sentences and/or fines.		
9. Prevention of injuries and death in the home due to fire.		
10. Prevention of financial losses due to vendor fraud.		
11. Appearance of the home and yard.		
12. Ensure that the family unit size does not increase in the foreseeable future (i.e. no new children or grandchildren).		
13. Ensure all family members maintain healthy diets and lifestyles to increase life expectancies and overall "wellness".		
14. Prevent death or injury due to auto safety problems.		
15. Minimize unnecessary dental expenditures due to poor dental hygiene.		

Factors to Consider in Rating the Risk of Non-Achievement of the Objectives Shown (e.g. likelihood of causing personal injury, consequences of non-achievement, etc.)
1.
2.
3.
4.
5.
6.
7.
8.

Factors to Consider When Deciding Accountability Assignments (e.g. technical knowledge required, physical strength required, etc.)
1.
2.
3.
4.
5.
6.
7.
8.

THE CARD® APPROACH

Paisley Consulting has developed software that provides a range of options to rate and prioritize risk and assurance universe.

OPTION 1 - GROSS RISK & CURRENT KNOWLEDGE LEVEL

One approach involves assigning a "gross" risk rating to the business/quality objective selected. This means rating how serious it would be if the objective was not achieved in whole or in part. Next, users are asked on a scale of 1-5 how much is currently known about the control/risk status. Cases where the gross risk is high, and the current knowledge status is low are top candidates for detailed review using a CRSA workshop, direct report audit or other assessment technique.

OPTION 2 - GROSS RISK & PERFORMANCE INDICATOR STATUS

Another approach is to assign a gross risk rating to an objective and form an opinion on how well the objective is currently being achieved. Cases where the gross risk is high and performance indicator status rated as "Negative" or "Very Negative" are top candidates for detailed review.

OPTION 3 - GROSS RISK, CURRENT ASSURANCE LEVEL & PERFORMANCE INDICATOR STATUS

This approach also starts by rating Gross Risk. Assurance personnel accountable for the objective then rate the current "Assurance Level". Assurance level refers to how sure are they that they know the current control/risk status. Cases where the Gross Risk is high, the Current Assurance rating low, and Performance Indicator Status is ranked as "Negative" or "Very Negative" are top candidates for detailed assessment.

OPTION 4 - DATE OF LAST REVIEW AND WHO DID THE REVIEW

Other factors that are relevant to the decision include who did the most recent analysis (i.e. internal audit, the work unit, a specialist, a task force, etc.) and how long has it been since it was completed.

NOTE: IN ALL CASES ABOVE AN ADDITIONAL DIMENSION COULD BE ADDED WHICH ASKS FOR A SUBJECTIVE VIEW ON CURRENT CONTROL EFFECTIVENESS. PAISLEY CONSULTING DOES NOT RECOMMEND THIS ELEMENT BECAUSE IT HAS PROVEN TO BE HIGHLY UNRELIABLE.

ASSIGNING RESPONSIBILITY

CARD®*map* software offers users the opportunity to define a range of accountability assignments. These include:

Who is the "Owner" of the business/quality objective in the universe, if any?

Who is the status reporter for each business/quality objective in the universe, if any?

Who is the primary assurance provider for each business/quality objective in the universe, if any?

GROUP EXERCISE:

In your groups complete the cases assigned by your workshop leader. The purpose of the exercise is to gain a general understanding of "Responsibility Assignment", "Gross Risk", "Knowledge Level", "Assurance Level" and "Performance Indicator Status" as tools to assign responsibility for the universe and select candidates for assessment.

CASE 1 – LARGE BANK LISTED ON LONDON AND NEW YORK STOCK EXCHANGES. 10 BILLION U.S. IN REVENUE/YEAR WITH ASSETS OF 200 BILLION U.S.

OBJECTIVE: ENSURE THE COMPANY COMPLIES WITH ALL SECURITIES LAWS IN ALL JURISDICTIONS IN WHICH SHARES ARE LISTED.

Person or Group with Primary Responsibility for this Objective

CEO	☐	Law Department	☐	Internal Audit	☐	Other _____	☐
CFO	☐	Treasurer	☐	External Audit	☐	Specific Assignment Not Required	☐

Risk to the Organization of Non-Achievement

Low ☐ Medium ☐ High ☐

Level of Knowledge Required re Control/Risk Status

	(1 = Little or None			5 = Extensive)
By Relevant Senior Management	1	2	3	4	5
By Audit Committee/Board of Directors	1	2	3	4	5

Level of Assurance Required From Assurance Providers*

	(1 = Little or None			5 = Extensive)
From Management	1	2	3	4	5
From Internal Audit	1	2	3	4	5
From External Audit	1	2	3	4	5
From Other Assurance Provider – (Please specify _____)	1	2	3	4	5

**(Note: Assurance is defined as a positive declaration intended to give confidence.)*

CASE 2 – MULTINATIONAL OIL COMPANY. ONE OF THE FIVE LARGEST IN THE WORLD.

OBJECTIVE: ENSURE ALL EMPLOYEES COMPLY WITH LAWS RELATED TO SEXUAL HARASSMENT AND DISCRIMINATION.

Person or Group with Primary Responsibility for this Objective

CEO	☐	Law Department	☐	Internal Audit	☐	Other _____	☐
CFO	☐	Treasurer	☐	External Audit	☐	Specific Assignment Not Required	☐

Risk to the Organization of Non-Achievement

Low ☐ Medium ☐ High ☐

Level of Knowledge Required re Control/Risk Status	**(1 = Little or None**			**5 = Extensive)**
By Relevant Senior Management	1	2	3	4	5
By Audit Committee/Board of Directors	1	2	3	4	5

Level of Assurance Required From Assurance Providers*	**(1 = Little or None**			**5 = Extensive)**
From Management	1	2	3	4	5
From Internal Audit	1	2	3	4	5
From External Audit	1	2	3	4	5
From Other Assurance Provider – (Please specify _____)	1	2	3	4	5

**(Note: Assurance is defined as a positive declaration intended to give confidence.)*

CASE 3 – INSURANCE COMPANY WITH OVER 20 BILLION U.S. IN ASSETS WITH REVENUE OF 1.5 BILLION/YEAR

OBJECTIVE: MINIMIZE THE INCIDENCE OF FRAUDULENT CLAIM PAYMENTS.

Person or Group with Primary Responsibility for this Objective

CEO	☐	Law Department	☐	Internal Audit	☐	Other _____	☐
CFO	☐	Treasurer	☐	External Audit	☐	Specific Assignment Not Required	☐

Risk to the Organization of Non-Achievement

Low ☐ Medium ☐ High ☐

Level of Knowledge Required re Control/Risk Status	**(1 = Little or None**			**5 = Extensive)**
By Relevant Senior Management	1	2	3	4	5
By Audit Committee/Board of Directors	1	2	3	4	5

Level of Assurance Required From Assurance Providers*	**(1 = Little or None**			**5 = Extensive)**
From Management	1	2	3	4	5
From Internal Audit	1	2	3	4	5
From External Audit	1	2	3	4	5
From Other Assurance Provider – (Please specify _____)	1	2	3	4	5

**(Note: Assurance is defined as a positive declaration intended to give confidence.)*

CASE 4 – LARGE PUBLIC COMPUTER HARDWARE/SOFTWARE COMPANY.

OBJECTIVE: ENSURE THAT REPRESENTATIONS MADE TO CURRENT AND PROSPECTIVE CUSTOMERS BY SALES AGENTS ARE TRUTHFUL.

Person or Group with Primary Responsibility for this Objective

CEO	☐	Law Department	☐	Internal Audit	☐	Other _____	☐
CFO	☐	Treasurer	☐	External Audit	☐	Specific Assignment Not Required	☐

Risk to the Organization of Non-Achievement

Low ☐ Medium ☐ High ☐

Level of Knowledge Required re Control/Risk Status	**(1 = Little or None**				**5 = Extensive)**
By Relevant Senior Management	1	2	3	4	5
By Audit Committee/Board of Directors	1	2	3	4	5

Level of Assurance Required From Assurance Providers*	**(1 = Little or None**				**5 = Extensive)**
From Management	1	2	3	4	5
From Internal Audit	1	2	3	4	5
From External Audit	1	2	3	4	5
From Other Assurance Provider – (Please specify _____)	1	2	3	4	5

**(Note: Assurance is defined as a positive declaration intended to give confidence.)*

CASE 5 – MID SIZED MANUFACTURING COMPANY 1.5 BILLION U.S. IN SALES.

OBJECTIVE: ENSURE THAT FINISHED GOODS INVENTORIES ARE VALUED AT QUARTER AND YEAR-ENDS IN ACCORDANCE WITH GAAP.

Person or Group with Primary Responsibility for this Objective

CEO	☐	Law Department	☐	Internal Audit	☐	Other _____	☐
CFO	☐	Treasurer	☐	External Audit	☐	Specific Assignment Not Required	☐

Risk to the Organization of Non-Achievement

Low ☐ Medium ☐ High ☐

Level of Knowledge Required re Control/Risk Status (1 = Little or None 5 = Extensive)

By Relevant Senior Management	1	2	3	4	5
By Audit Committee/Board of Directors	1	2	3	4	5

Level of Assurance Required From Assurance Providers* (1 = Little or None 5 = Extensive)

From Management	1	2	3	4	5
From Internal Audit	1	2	3	4	5
From External Audit	1	2	3	4	5
From Other Assurance Provider – (Please specify _____)	1	2	3	4	5

**(Note: Assurance is defined as a positive declaration intended to give confidence.)*

CASE 6 – INTERNATIONAL FOOD AND BEVERAGE COMPANY. 15 BILLION U.S. PER YEAR IN SALES.

OBJECTIVE: ENSURE THE COMPANY MINIMIZES THE COST OF ACQUIRING NECESSARY RAW MATERIALS.

Person or Group with Primary Responsibility for this Objective

CEO	☐	Law Department	☐	Internal Audit	☐	Other _____	☐
CFO	☐	Treasurer	☐	External Audit	☐	Specific Assignment Not Required	☐

Risk to the Organization of Non-Achievement

Low ☐ Medium ☐ High ☐

Level of Knowledge Required re Control/Risk Status	**(1 = Little or None**			**5 = Extensive)**
By Relevant Senior Management	1	2	3	4	5
By Audit Committee/Board of Directors	1	2	3	4	5

Level of Assurance Required From Assurance Providers*	**(1 = Little or None**			**5 = Extensive)**
From Management	1	2	3	4	5
From Internal Audit	1	2	3	4	5
From External Audit	1	2	3	4	5
From Other Assurance Provider – (Please specify _____)	1	2	3	4	5

**(Note: Assurance is defined as a positive declaration intended to give confidence.)*

CASE 7 – LARGE TELEPHONE COMPANY 40,000 EMPLOYEES.

OBJECTIVE: ENSURE CUSTOMERS RECEIVE COMPETENT, PROMPT AND COURTEOUS SERVICE RELATED TO ALL PRODUCTS AND SERVICES SUPPLIED.

Person or Group with Primary Responsibility for this Objective

CEO	☐	Law Department	☐	Internal Audit	☐	Other _____	☐
CFO	☐	Treasurer	☐	External Audit	☐	Specific Assignment Not Required	☐

Risk to the Organization of Non-Achievement

Low ☐ Medium ☐ High ☐

Level of Knowledge Required re Control/Risk Status	**(1 = Little or None**				**5 = Extensive)**
By Relevant Senior Management	1	2	3	4	5
By Audit Committee/Board of Directors	1	2	3	4	5

Level of Assurance Required From Assurance Providers*	**(1 = Little or None**				**5 = Extensive)**
From Management	1	2	3	4	5
From Internal Audit	1	2	3	4	5
From External Audit	1	2	3	4	5
From Other Assurance Provider – (Please specify _____)	1	2	3	4	5

**(Note: Assurance is defined as a positive declaration intended to give confidence.)*

CASE 8 – CHEMICAL COMPANY. 5 BILLION U.S. IN SALES.

OBJECTIVE: ENSURE COMPLIANCE WITH ALL APPLICABLE ENVIRONMENTAL LAWS IN ALL JURISDICTIONS THE COMPANY OPERATES IN.

Person or Group with Primary Responsibility for this Objective

CEO	☐	Law Department	☐	Internal Audit	☐	Other _____	☐
CFO	☐	Treasurer	☐	External Audit	☐	Specific Assignment Not Required	☐

Risk to the Organization of Non-Achievement

Low ☐ Medium ☐ High ☐

Level of Knowledge Required re Control/Risk Status (1 = Little or None 5 = Extensive)					
By Relevant Senior Management	1	2	3	4	5
By Audit Committee/Board of Directors	1	2	3	4	5

Level of Assurance Required From Assurance Providers* (1 = Little or None 5 = Extensive)					
From Management	1	2	3	4	5
From Internal Audit	1	2	3	4	5
From External Audit	1	2	3	4	5
From Other Assurance Provider – (Please specify _____)	1	2	3	4	5

**(Note: Assurance is defined as a positive declaration intended to give confidence.)*

CASE 9 – MINISTRY OF TRANSPORTATION – LARGE GOVERNMENT DEPARTMENT WITH A SERVICE POPULATION OF 10 MILLION TAXPAYERS.

OBJECTIVE: MINIMIZE ROAD INJURIES AND DEATHS.

Person or Group with Primary Responsibility for this Objective

CEO	☐	Law Department	☐	Internal Audit	☐	Other _____	☐
CFO	☐	Treasurer	☐	External Audit	☐	Specific Assignment Not Required	☐

Risk to the Organization of Non-Achievement

Low ☐ Medium ☐ High ☐

Level of Knowledge Required re Control/Risk Status (1 = Little or None 5 = Extensive)

By Relevant Senior Management	1	2	3	4	5
By Audit Committee/Board of Directors	1	2	3	4	5

Level of Assurance Required From Assurance Providers* (1 = Little or None 5 = Extensive)

From Management	1	2	3	4	5
From Internal Audit	1	2	3	4	5
From External Audit	1	2	3	4	5
From Other Assurance Provider – (Please specify _____)	1	2	3	4	5

**(Note: Assurance is defined as a positive declaration intended to give confidence.)*

CASE 10 – ANY PUBLIC/PRIVATE SECTOR ORGANIZATION.

OBJECTIVE: ENSURE THAT THE ORGANIZATION COMPLIES WITH ALL SIGNIFICANT CONTRACTUAL COMMITMENTS WITH SUPPLIERS AND CUSTOMERS.

Person or Group with Primary Responsibility for this Objective

CEO	☐	Law Department	☐	Internal Audit	☐	Other _____	☐
CFO	☐	Treasurer	☐	External Audit	☐	Specific Assignment Not Required	☐

Risk to the Organization of Non-Achievement

Low ☐ Medium ☐ High ☐

Level of Knowledge Required re Control/Risk Status	**(1 = Little or None**				**5 = Extensive)**
By Relevant Senior Management	1	2	3	4	5
By Audit Committee/Board of Directors	1	2	3	4	5

Level of Assurance Required From Assurance Providers*	**(1 = Little or None**				**5 = Extensive)**
From Management	1	2	3	4	5
From Internal Audit	1	2	3	4	5
From External Audit	1	2	3	4	5
From Other Assurance Provider – (Please specify _____)	1	2	3	4	5

**(Note: Assurance is defined as a positive declaration intended to give confidence.)*

IDENTIFYING & RANKING THREATS TO ACHIEVEMENT

Section Objectives:

(1) Provide practical techniques to identify and rank the full range of risks that can jeopardize the achievement of:

(a) an organization's primary mission ("macro level");

(b) a work unit's primary mission ("mid level");

(c) specific business/quality objectives ("micro level");

(d) highly specific sub-sets of business/quality objectives ("sub-micro level"); and

(2) Introduce participants to the risk models available to assist work units and assurance personnel identify significant risks that threaten the achievement of their business objectives at all levels.

Simply put:

Are we aware of things that could hurt or impede us?

BACKGROUND

Over the past four years interest in risk assessment has been growing rapidly. Section 9 of this workbook provides a broad overview of developments that have fueled this trend. Underlying the global shift that is occurring is a general theme.

Management and work units relate well to processes that identify issues and topics that could hurt them and/or impede achievement of objectives they care most about (i.e. risks).

In January of 1999 the Institute of Internal Auditors recognized this trend by releasing a revised definition of assurance focused on effective risk management. The new definition requires an opinion from the assurance provider that management:

- Understands risk exposures
- Implements appropriate risk management
- Balances risk and control adequately
- Accommodates change effectively.

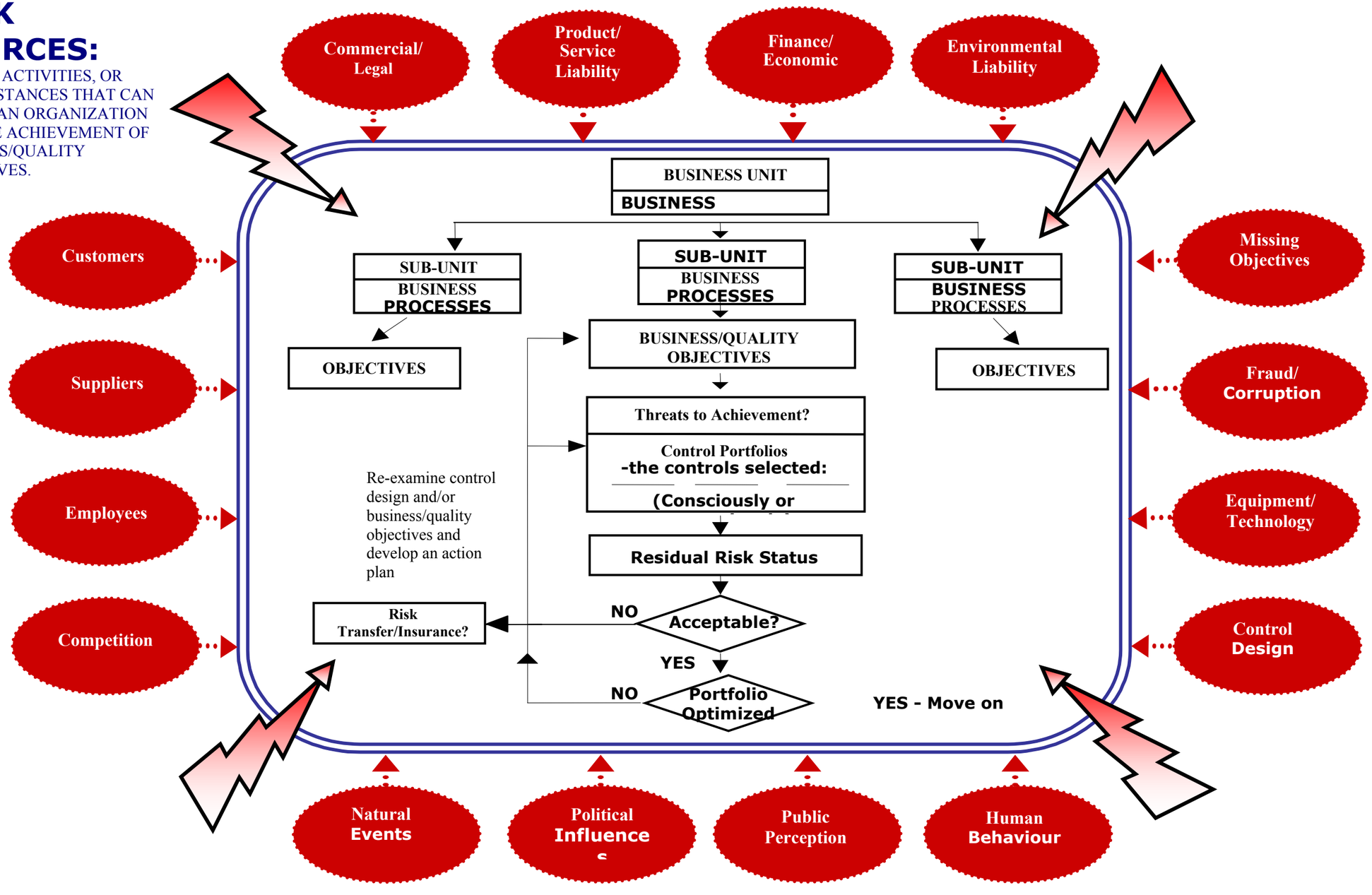
An overview of the "Risk Arena" is shown on the next page.

Risk assessment can be done at a range of levels in the organization including Macro, Mid Level, Micro and Sub-Micro.

RISK ARENA OVERVIEW

RISK SOURCES:

EVENTS, ACTIVITIES, OR CIRCUMSTANCES THAT CAN AFFECT AN ORGANIZATION AND THE ACHIEVEMENT OF BUSINESS/QUALITY OBJECTIVES.



CORE RISK

Risks are relevant to the extent they impact on an enterprise's current and future business

Some risks create and add to the universe of business objectives necessary to succeed – i.e. mitigating certain risks should be included as business objectives (e.g. prevent injury and death of workers, prevent theft of stock from the

Deficiencies in control design (e.g. absence of commitment, objective setting, and risk assessment, poor training, lack of

Considering risks without making explicit linkages to the impacted business objective can lead to sub-optimal resource

Risk status is dynamic as the various risk and control elements interact.

The focus of management should be on defining objectives and analyzing and evaluating the acceptability of residual risk. Assurance agents should focus on whether there is an effective

MACRO LEVEL

This type of risk assessment explicitly or implicitly uses a broad statement as a starting point.

Ensure achievement of all of XYZ's key business objectives.

In the private sector this can be done at the corporate level or for an entire subsidiary. In the public sector this might take a variety of forms depending on the type of public sector entity (e.g. Ensure achievement of all of the Government of Canada's key objectives. Ensure achievement of all of the City of Toronto's key objectives.)

Having identified a macro level objective for assessment, "Threats to Achievement" or "Risks" are identified. These risks can be rated in terms of "Likelihood" and "Consequence". Consequence means how bad would it be if the specific threat occurred. Likelihood refers to the probability of the threat occurring. Likelihood can be further divided into "Gross Likelihood" and "Net Likelihood". Gross Likelihood examines probability of the threat occurring or existing without consideration of the organization's control structure. Net Likelihood begins to factor in the control elements the organization has in place to mitigate the specific threat or risk. In practice people will identify a mixture of items, some of which may be Gross Likelihood, e.g. a train wreck nearby forces evacuation of the building, while others may be influenced heavily by existing controls, e.g. input operator incorrectly enters the amount of cheques received (controls unconsciously considered include highly experienced, good eyesight with strong edit controls built-in, etc).

MID LEVEL

Risk assessments that fit this general category include achieving all of the key objectives of a subsidiary or functional department. Another form of mid level risk assessment focuses on achievement of broad categories or families of objectives. An example of this would be:

Ensure all products delivered meet or exceed customer expectations.

Minimize all unnecessary costs across the organization.

Minimize the incidence of injury and death across the organization.

MICRO LEVEL

Risk assessments at this level start with a specific end result of objective. Threats to Achievement are then identified. These threats can also be ranked in terms of consequence and likelihood. Examples include:

Ensure all truck shipments are recorded in the sales register.

Prevent payment of fraudulent expense claims.

Ensure that all goods shipped to clients meet quality specifications.

SUB-MICRO/HIGHLY SPECIFIC LEVEL

Risk assessments done at this level focus on a very specific end result objective. These are normally conducted when the risk of non-achievement of the specific sub-objective is very high. An example in a retail bank environment is:

Prevent injury and death of employees caused by bank robbers.

Ensure compliance with Section 25 sub(b) of the Financial Institution Regulation statute related to the frequency of statement provision on dormant accounts.

GROUP EXERCISE - HOME ENVIRONMENT

For the objectives listed below list as many threats to achievement of the objective as you can come up with in the time allotted. **Remember, "Threats to Achievement" are possible problems or situations that could result in non-achievement of the objective.**

Business/Quality Objective: **Prevent death and injury in the home due to fire.**

Threats to Achievement:

1. Example: Faulty wiring.
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

GROUP EXERCISE - HOME ENVIRONMENT (Cont'd)

For the objectives listed below list as many threats to achievement of the objective as you can come up with in the time allotted. **Remember, "Threats to Achievement" are possible problems or situations that could result in non-achievement of the objective.**

Business/Quality Objective: **Minimize the cost of acquiring necessary household appliances, groceries and other goods and services.**

Threats to Achievement:

1. Example: Don't want to spend time checking where the good deals are.
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

USING A RISK MODEL AS A COMPLETENESS TOOL

People, when asked to identify Threats to Achievement, will usually draw heavily on their personal knowledge and experience. This approach will work well in identifying some, but rarely all, significant risks. It relies heavily on the experience levels and level of industry knowledge of the assessors. To ensure people have considered the full range of Threats, a Risk Framework can be applied. Paisley Consulting (formerly CARD®*decisions*) has developed a 16-category framework to assist participants. An overview of the framework is shown on 4-3. Definitions of each of the 16 general categories are shown below. Other frameworks currently is use are included in Section 9 of this workbook.

Risk Arena: Risk Source Definitions

Commercial/Legal

Is the entity or objective threatened by contractual issues or relationships or the absence of contracts or by legal or regulatory requirements?

Competition

Is the entity or objective threatened by the actions of competitors including illegal, unethical, collusive and/or strategic actions of competitors?

Control Design

Is the entity or objective threatened by structural deficiencies in the overall approach to control used by the organization? (i.e. the macro control design)

Customers

Is the entity or objective threatened by the actions of customers outside the normal course of business?

Employees

Is the entity or objective threatened the actions of employees involved in organized or unorganized collective actions? (Note: this risk source covers collective actions as opposed to the risk source covered in the Human Behaviour category)

Environmental Liability

Is the entity or objective threatened by liabilities or hazards from environmental events, exposures or situations?

Equipment/Technology

Is the entity or objective threatened by failures or deficiencies in equipment and/or technology including computer hardware and software?

Finance/Economic

Is the entity or objective threatened by general economic or financial conditions, lack of funds trends either positive or negative?

Fraud/Corruption

Is the entity or objective threatened by fraudulent acts of employees, suppliers, customers or outside parties including organized crime schemes?

Human Behaviour

Is the entity or objective threatened by the behaviours of the people necessary to support the objective including employees, suppliers, agents, outsourcer activities etc.? (e.g. forgetfulness, indifference, defiance, etc.)

Missing Objectives

Is the entity or objective threatened by the absence of any key supporting objectives necessary for the long-term success of the entity or to support a specific objective?

Natural Events

Is the entity or objective threatened by natural events such as lightning, floods, fire, ice storms, wildlife, temperature variations, etc?

Political Influences

Is the entity or objective threatened by possible political or regulatory intervention and/or legislation?

Product/Service Liability

Is the entity or objective threatened by liabilities from the products or services provided by the organization or acquired by the organization from others including any outsourcing or sub-contract relationships?

Public Perception

Is the entity or objective threatened the consequences that can flow from public reaction to corporate activities including media reports or other information they obtain about the organization's activities?

Suppliers

Is the entity or objective threatened by the actions of suppliers including the goods and/or services they provide?

It is important to note that this is not an exhaustive trigger list. However, it has proven effective as a tool to assist users in expanding their frame of reference when completing risk assessments.

THE RISK ASSESSMENT DILEMMA - COMPLETENESS AND PERFECTION VS. PRACTICAL AND USEFUL (THE 90/10 RULE)

A serious challenge that people encounter when doing risk assessment is expressed simply as:

How far do I/we go identifying and rating risks?

Some risks by their very nature are highly unlikely but could result in death, jail time, loss of job, or other very serious consequences. Others are so likely and so obvious, there is a tendency to avoid stating the obvious. There is no simple solution to this challenge. As a general rule, the risk assessment done should be "Fit for the Task". This means that the level of rigour will be dictated by the importance of the objective, consequences of non-achievement, time and resources available to do the analysis, skill of the analyst or facilitator, skill of the group members if done in a workshop mode, and other factors. An organization's culture and comfort with rigour has a significant influence on the quantity and quality of risk assessment work completed.

GROUP EXERCISE - MACRO LEVEL

Instructions: Your workshop leader will select a macro level objective that is relevant to as many participants in the class as is possible.

Using the 16 category risk model shown on 4-3 develop a list of 20 to 25 "Threats to Achievement". A worksheet has been provided on the next page to assist you. Rank a sample of the Threats identified in terms of likelihood and consequences.

CARD®*map* software may also be used by the class or individual groups to illustrate how software can be used to perform and report risk assessments.

MACRO LEVEL OBJECTIVE SELECTED:			
Threats/Risk Identified	**Consequence**	**Likelihood**	**Risk Source**
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			

MACRO LEVEL OBJECTIVE SELECTED:			
Threats/Risk Identified	**Consequence**	**Likelihood**	**Risk Source**
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			

DESIGNING & ASSESSING CONTROL PORTFOLIOS

Section Objectives:

(1) Introduce the leading control frameworks available to help users assess macro, mid range and micro level control portfolios (e.g. COSO, CoCo, CARD®*model*, Baldrige, etc.).

(2) Train participants to identify the structural design of control frameworks using a control model.

(3) Increase participants' ability to identify the root cause of control breakdowns.

(4) Increase participant's ability to design high impact, lowest possible cost control portfolios that result in an acceptable level of residual risk

Simply put:
Have we taken the right precautions given our risk tolerance?

SECTION OVERVIEW

This section is organized into four parts.

PART 1 - The Theory of Control

PART 2 - Group Exercise - What is a Control?

PART 3 - Group Exercise - Designing High Impact/Low Cost Control Portfolios

PART 4 - Group Exercise - Identifying Root Causes of Control Breakdowns

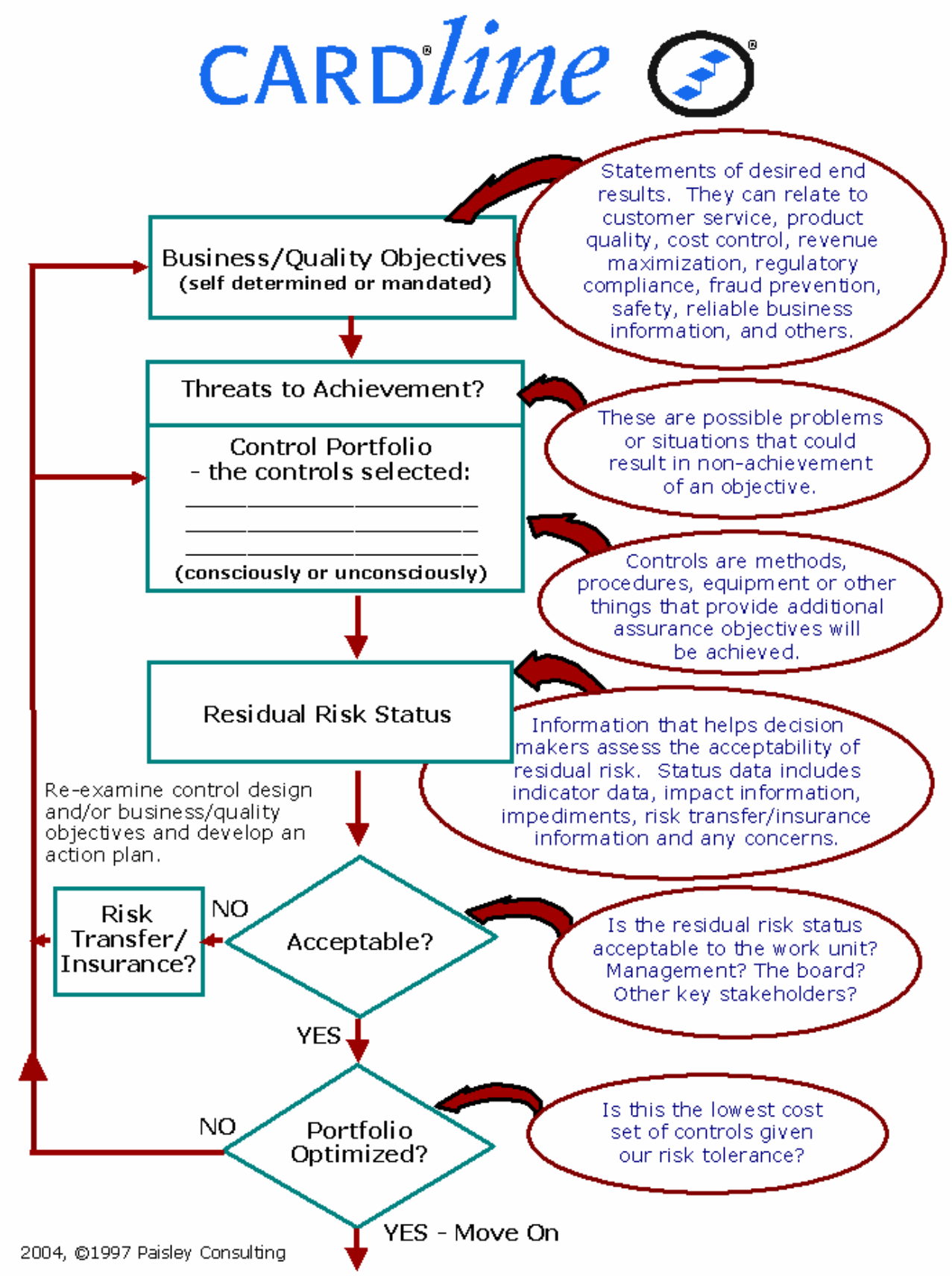
A central theme that will be stressed in this section is value of using a risk framework and control model to design, assess and report on control and risk.

PART 1 - THE THEORY OF CONTROL

Your workshop leader will provide an overview of the evolution of thinking in control management and theory. The reference material for this overview is found in Section 8 of this workbook.

The primary Control Design & Assessment approach Paisley Consulting advocates is the CARD®*line* approach shown on 5-3. We have found this approach produces the best, most consistent control designs and control assessments of all of the approaches currently available.

When you are completing the group exercises in this section - ensure that you keep the Business/Quality Objective to be achieved and the Threats to Achievement clearly in mind.



PART 2: GROUP EXERCISE: WHAT IS A CONTROL?

Instructions: In your assigned group indicate for each item whether you believe it is a potential control that provides incremental assurance that the stated objective will be achieved. You are not being asked to decide if it the best control, or a cost effective control. You are only asked if using or having the item would provide more assurance than not having or using it.

The Fantasy Ranch Case: a Gambling Casino Business

Control Option Checklist

OBJECTIVE: ENSURE THAT SUPPLIES OF GAMBLING CHIPS IN THE CASINO ARE SAFEGUARDED AGAINST THEFT.

Control Options	Potential Control		
	Yes	No	Maybe
1. Monthly budget to actual variance analysis.	☐	☐	☐
2. Detailed inventory records of chip stocks	☐	☐	☐
3. Employment contracts with all staff.	☐	☐	☐
4. Chips are stored in a vault when not in use.	☐	☐	☐
5. Hire very large gambling chip sales attendants.	☐	☐	☐
6. Constant armed patrol of the premises.	☐	☐	☐
7. Annual external audit of the accounts.	☐	☐	☐
8. Custody of the chips is segregated from the cashiers who provide chips to the public.	☐	☐	☐

Control Options		Potential Control		
		Yes	No	Maybe
9.	Regular shift reconciliation of chip sales to shift inventory of chips on hand.	☐	☐	☐
10.	Job description of shift boss requires he/she review and approve shift sales/inventory movement reconciliation.	☐	☐	☐
11.	Fidelity insurance.	☐	☐	☐
12.	Security department staffed by convicted gaming house fraudsman.	☐	☐	☐
13.	Background reference checks on all staff.	☐	☐	☐
14.	Sensors at all entrances and exits that alert security to the removal of chips that have not been disarmed.	☐	☐	☐
15.	Outside consultant review to identify vulnerabilities.	☐	☐	☐

The Fantasy Ranch Case: A Hotel Business

Control Option Checklist

OBJECTIVE: ENSURE THAT HOTEL ROOMS MEET THE RANCH'S QUALITY STANDARDS AT THE TIME OF CHECK-IN.

Control Options	Potential Control		
	Yes	No	Maybe
1. All cleaning staff must attend the Fantasy Ranch's cleaning school prior to commencing their positions.	☐	☐	☐
2. All cleaning supervisors are required to have undergraduate diplomas.	☐	☐	☐
3. The number for the "Complaint Hotline" is written in bold letters on all room phones.	☐	☐	☐
4. Supervisors randomly inspect rooms to check that cleaning standards have been met.	☐	☐	☐
5. Room make-up and cleaning standards and procedures are documented in a Fantasy Standards Manual which is provided to all staff.	☐	☐	☐
6. Annual external audit of the Ranch's financial statements.	☐	☐	☐
7. Formation/existence of a Fantasy Ranch audit committee.	☐	☐	☐
8. All customer complaints are logged in a log titled "Complaints with my Fantasy" and time dated. Steps to resolve the complaint must be described and time dated. The shift supervisor must record an opinion as to whether the customer is: Very Happy. Satisfied. Pacified. Unsatisfied.	☐	☐	☐

Control Options	Potential Control		
	Yes	No	Maybe
9. The Ranch requires all section heads to contribute submissions to the Ranch's Business Planning process.	☐	☐	☐
10. Staff are recognized for outstanding contributions to ensuring the rooms meet the Ranch's standards with an incentive program.	☐	☐	☐
11. The owner of the Ranch often books into the hotel under assumed names in disguise and inspects the rooms personally.	☐	☐	☐
12. Staff are paid large incentives for new ways to reduce costs and cut the time necessary to make up rooms.	☐	☐	☐
13. The Ranch employs a hotel inspection service to randomly audit the condition of rooms.	☐	☐	☐
14. Chambermaids have been equipped with microcomputers which monitor and record the elapsed time to clean each room, the specific cleaning steps employed, problems noted for maintenance, and other details.	☐	☐	☐
15. The Ranch has a Fantasy Ranch Statement of Values and Ethics which is communicated to all employees when they join and annually thereafter.	☐	☐	☐
16. All cleaning staff are required to attend leadership training courses.	☐	☐	☐
17. The Hotel's electronic door lock system records the maids' time in and requires that maids log out when the room has been completed.	☐	☐	☐
18. Up-to-date job descriptions for all chamber maids and floor cleaning supervisors.	☐	☐	☐

PART 3: GROUP EXERCISE – DESIGNING HIGH IMPACT/LOW COST CONTROL PORTFOLIOS

REQUIRED: For the four exercises in this section select the top three impact per dollar of cost control options by indicating notations 1 to 3 in the space provided in order of their impact per dollar of cost. A rating of one indicates that you believe that this control would provide the most or highest incremental assurance impact per dollar of cost for the specific objective listed. The items chosen should represent the three most powerful controls in assuring the achievement of the objective on a result per dollar of cost basis. Only three options are to be selected. Your workshop leader may also request you analyze the individual control options in terms of type or category of control.

EXERCISE 1: *REMEMBER: KEEP THE OBJECTIVE IN FOCUS.*

OBJECTIVE: ENSURE THAT ALL ORDERS DELIVERED TO CUSTOMERS CONTAIN ALL ITEMS AND ONLY THE ITEMS ORDERED BY THE CUSTOMER.

Note: The options relate to a fast food environment but could, with minor adjustments, relate to a shipping area in any business.

Rating	Control Portfolio Option	CARD® I.D.
( ) 1.	Include in the job descriptions of all staff who take and fill customer orders a requirement that they accurately fill customer orders.	_____
( ) 2.	Include a hearing test and an order input accuracy test in the candidate selection criteria and ensure all applicants have achieved at least the minimum acceptable score before being accepted for these positions.	_____
( ) 3.	Investigate each customer complaint received related to order accuracy and completeness. In cases where employee error is the cause, fire the responsible staff person.	_____
( ) 4.	Maintain a customer complaint log and document all complaints including those regarding order accuracy. Assign responsibility for investigation and follow-up of complaints to a specific individual and require resolution steps be documented. Require a supervisor review this log to ensure procedures are followed.	_____

EXERCISE 1: *REMEMBER: KEEP THE OBJECTIVE IN FOCUS.*

OBJECTIVE: ENSURE THAT ALL ORDERS DELIVERED TO CUSTOMERS CONTAIN ALL ITEMS AND ONLY THE ITEMS ORDERED BY THE CUSTOMER.

Note: The options relate to a fast food environment but could, with minor adjustments, relate to a shipping area in any business.

Rating	Control Portfolio Option	CARD® I.D.
( ) 5.	Hire a shopping service to randomly order food at various locations and verify that they are given the correct order.	_____
( ) 6.	Have each order checked by someone other than the preparer prior to being delivered to the customer.	_____
( ) 7.	Require that the order system record the identification of the person who took and prepared the order to aid in identifying employees who are making errors on customer orders.	_____
( ) 8.	Design a computerized order screen which requires each item ordered be marked as shipped by the person filling the order as they assemble the order.	_____
( ) 9.	Provide a video training film to all staff demonstrating the correct procedures to take and fill orders.	_____
( ) 10.	In every case reported where a verified order inaccuracy is found, compensate the customer with a free meal and deduct the cost of the meal from the pay of the responsible employee.	_____
( ) 11.	Include in job descriptions that supervisors oversee order taking and filling operations and randomly check orders prior to delivery to customers.	_____
( ) 12.	Track on a large graph in the food preparation area the incidence of verified inaccurate orders and the cost of free meals provided to customers as compensation for their inconvenience.	_____
( ) 13.	Voice record all incoming orders on tape. Have a supervisor periodically compare the tape orders to the order input by the order taker to check order input for accuracy. All inconsistencies are to be followed up.	_____

EXERCISE 1: *REMEMBER: KEEP THE OBJECTIVE IN FOCUS.*

OBJECTIVE: ENSURE THAT ALL ORDERS DELIVERED TO CUSTOMERS CONTAIN ALL ITEMS AND ONLY THE ITEMS ORDERED BY THE CUSTOMER.

Note: The options relate to a fast food environment but could, with minor adjustments, relate to a shipping area in any business.

Rating	Control Portfolio Option	CARD® I.D.
( ) 14.	Include customer order accuracy as a significant performance evaluation item for all shift managers and link a portion of their performance pay to this item.	_____
( ) 15.	Ensure that the order taking input terminal is designed with large print, and dedicated keys for each food item offered (i.e. large diet coke, cheeseburger, small fries, etc.). Test the design with a representative cross section of employee for order input accuracy prior to placing the hardware in use.	_____
( ) 16.	Require that staff that are responsible for order taking, assembly and delivery self-assess the adequacy of their current controls and related risks, identify unsatisfactory situations, and develop action plans to rectify problems.	_____
( ) 17.	Require that every employee found to be responsible for an error on a customer order wear a button which reads "I disappointed one of our customers today" for the balance of the shift. Additional buttons are issued for each error.	_____
( ) 18.	Require that each shift manager start their shift by requiring the customer service team chant a slogan on the importance of accurate orders.	_____
( ) 19.	Have head office auditors review the order taking and assembly system, perform tests, and report their findings and recommendations to local and head office management on a three year cycle basis.	_____

PART 3 - EXERCISE #2

REQUIRED: For the four exercises in this section select the top three impact per dollar of cost control options by indicating notations 1 to 3 in the space provided in order of their impact per dollar of cost. A rating of one indicates that you believe that this control would provide the most or highest incremental assurance impact per dollar of cost for the specific objective listed. The items chosen should represent the three most powerful controls in assuring the achievement of the objective on a result per dollar of cost basis. Only three options are to be selected. Your workshop leader may also ask you to identify the specific control type from the CARD®*menu* for one or more of the exercises.

EXERCISE 2: *REMEMBER: KEEP THE OBJECTIVE IN FOCUS.*

OBJECTIVE: MINIMIZE THE FREQUENCY AND MAGNITUDE OF HEALTH RELATED PROBLEMS DUE TO ILLNESS. (Oil Company: Middle to Far East Environment)

Rating	Control Portfolio Option	CARD® I.D.
( ) 1.	Develop and maintain a "Total Health Plan" for the staff assigned to Indonesia detailing short term and long term strategies.	_____
( ) 2.	Scientifically inspect all food supplies that staff are likely to consume for the presence of nasty bugs and germs.	_____
( ) 3.	Hire a qualified health specialist with experience in the Middle and Far East and assign responsibility for minimizing health related problems.	_____
( ) 4.	Specify in assignment postings and job descriptions that only healthy, well adjusted, fit people should apply for positions.	_____
( ) 5.	Perform surprise medical checkups on staff assigned to Indonesia and report the results to the individuals.	_____
( ) 6.	Train all supervisory staff to early detect signs of the most common medical ailments that afflict staff and provide guidance on where to get assistance.	_____
( ) 7.	Set minimum health standards and require that all staff undergo a comprehensive medical examination prior to starting their job assignment.	_____
( ) 8.	Show regular video programs to all potential and current staff on good health practices.	_____

EXERCISE 2: *REMEMBER: KEEP THE OBJECTIVE IN FOCUS.*

OBJECTIVE: MINIMIZE THE FREQUENCY AND MAGNITUDE OF HEALTH RELATED PROBLEMS DUE TO ILLNESS. (Oil Company: Middle to Far East Environment)

Rating	Control Portfolio Option	CARD® I.D.
( ) 9.	Display posters of individuals with assorted health related problems. Include an explanation of what the employee could have done to prevent the problem.	_____
( ) 10.	Acquire artificial intelligence health assessment software for staff which helps staff complete comprehensive health self-assessments and provides full analysis and corrective recommendations.	_____
( ) 11.	Fire any staff that have health problems lasting longer than 3 days in duration more than once per year that affect work output.	_____
( ) 12.	Require that the person responsible for on-site health care develop contacts that allow him or her to identify and monitor trends and obtain best practices information.	_____
( ) 13.	Develop and maintain a comprehensive computerized confidential total health information system which contains all health related information on all staff and has the capability of analyzing and reporting health related trends.	_____
( ) 14.	Develop and issue a "Good Health" manual to all staff. This manual will include preventative, detective and corrective information complete with a subject/topic index. Require all staff sign to acknowledge receipt of this manual.	_____
( ) 15.	Include "Days Lost Due to Health" as a key performance measurement in the performance contract of the V.P. operations.	_____
( ) 16.	Post large graphs and charts in prominent sites at the office and main camp which detail the frequency and magnitude of all injuries, illnesses, diseases, etc. contracted/incurred by all staff together with the main causes.	_____

EXERCISE 2: *REMEMBER: KEEP THE OBJECTIVE IN FOCUS.*

OBJECTIVE: MINIMIZE THE FREQUENCY AND MAGNITUDE OF HEALTH RELATED PROBLEMS DUE TO ILLNESS. (Oil Company: Middle to Far East Environment)

Rating	Control Portfolio Option	CARD® I.D.
( ) 17.	Require that all staff, with the aid of health care specialists, complete annual self-assessments of the control framework in place related to this objective.	_____

PART 3 - EXERCISE #3

REQUIRED: For the four exercises in this section select the top three impact per dollar of cost control options by indicating notations 1 to 3 in the space provided in order of their impact per dollar of cost. A rating of one indicates that you believe that this control would provide the most or highest incremental assurance impact per dollar of cost for the specific objective listed. The items chosen should represent the three most powerful controls in assuring the achievement of the objective on a result per dollar of cost basis. Only three options are to be selected. Your workshop leader may also ask you to identify the specific control type from the CARD®*menu* for one or more of the exercises.

EXERCISE 3: *REMEMBER: KEEP THE OBJECTIVE IN FOCUS.*

OBJECTIVE: ENSURE THAT ALL SALES OF FOOD AND LIQUOR ARE ACCOUNTED FOR IN THE BOOKS (RESTAURANT ENVIRONMENT).

Rating	Control Portfolio Option	CARD® I.D.
( ) 1.	Utilize prenumbered sales slips.	_____
( ) 2.	Shift supervisor completes sequence reviews of sales slips to ensure all sales slips are in the batch sent to accounting.	_____
( ) 3.	Complete a monthly variance analysis of actual to budgeted expenses.	_____
( ) 4.	Perform surprise taste tests of food and liquor being served.	_____
( ) 5.	Prepare a detailed one year budget forecast annually detailing revenues and expense estimates and support data.	_____
( ) 6.	Develop and have detailed job descriptions for all shift supervisor positions.	_____
( ) 7.	Require an annual external audit of the accounting records of the Ranch.	_____
( ) 8.	Regularly complete gross margin analysis using the books of account to calculate cost of food and liquor sold as a % of total recorded sales.	_____
( ) 9.	Have the bartender on duty make a mark on a pad for each table served and compare this information to the sales slips turned in by servers.	_____

EXERCISE 3: *REMEMBER: KEEP THE OBJECTIVE IN FOCUS.*

OBJECTIVE: ENSURE THAT ALL SALES OF FOOD AND LIQUOR ARE ACCOUNTED FOR IN THE BOOKS (RESTAURANT ENVIRONMENT).

Rating	Control Portfolio Option	CARD® I.D.
( ) 10.	Utilize a computerized sales system that opens an order in the system at the time food and liquor are issued from the bar or kitchen. This order can only be closed by recording the amount and method of customer payment.	_____
( ) 11.	Set up the chart of general ledger accounts to provide detailed sales and cost information to facilitate gross margin analysis.	_____
( ) 12.	Use a security "shopping service" to pose as customers and document procedures used.	_____
( ) 13.	The design/layout of sales slips that orders are recorded on facilitates recording orders using check marks versus handwritten notes.	_____
( ) 14.	Complete a regular detailed analysis of the direct costs of all drinks and food items served in the bar.	_____
( ) 15.	Obtain fidelity insurance coverage from a reputable insurer that specializes in the restaurant trade.	_____
( ) 16.	Complete an annual performance review for all cashiers and shift supervisors that includes accounting procedures as an evaluation area.	_____
( ) 17.	Develop and maintain a detailed instruction manual for all staff outlining all sales procedures and who is responsible for those procedures.	_____
( ) 18.	Complete weekly food and liquor inventory counts accompanied by a comparison of cost of goods sold to the calculated cost of goods sold from the accounting records.	_____
( ) 19.	Complete an internal audit of the restaurant on a 3-4 year cycle using a qualified internal auditing team and an approved audit program.	_____
( ) 20.	Include responsibility for accurate accounting in the position guides and performance contracts of all restaurant management personnel.	_____

PART 3 - EXERCISE #4

REQUIRED: For the four exercises in this section select the top three impact per dollar of cost control options by indicating notations 1 to 3 in the space provided in order of their impact per dollar of cost. A rating of one indicates that you believe that this control would provide the most or highest incremental assurance impact per dollar of cost for the specific objective listed. The items chosen should represent the three most powerful controls in assuring the achievement of the objective on a result per dollar of cost basis. Only three options are to be selected. Your workshop leader may also ask you to identify the specific control type from the CARD®*menu* for one or more of the exercises.

EXERCISE 4: *REMEMBER: KEEP THE OBJECTIVE IN FOCUS.*

OBJECTIVE: ENSURE THAT INFORMATION RELATED TO POLICYHOLDERS IS SAFEGUARDED AGAINST UNAUTHORIZED ACCESS/ DISCLOSURE (INSURANCE COMPANY)

Rating	Control Portfolio Option	CARD® I.D.
( ) 1.	Include a policy statement in the employee handbook which discusses the obligation of staff to safeguard client information against unauthorized disclosure.	_____
( ) 2.	Issue a policy requiring that all sensitive client related information on company premises be stored after hours in locking file facilities. Issue warnings and formal reports on units/individuals not in compliance.	_____
( ) 3.	Modify the building design to restrict floor access to only those individuals with a valid security ID card and maintain a 5 year history off-site of all employee movements.	_____
( ) 4.	Body search all persons leaving the building for company documents and then record the person's name and position, and the type and extent of documents being removed.	_____
( ) 5.	Develop a hard copy data classification system for client related information and require that documents, which expose clients to harm and/or losses if disclosed to unauthorized individuals, be protected with additional specified security/controls.	_____
( ) 6.	Perform comprehensive background reference checks on all staff being hired and on the company's payroll for less than two years.	_____

EXERCISE 4: *REMEMBER: KEEP THE OBJECTIVE IN FOCUS.*

OBJECTIVE: ENSURE THAT INFORMATION RELATED TO POLICYHOLDERS IS SAFEGUARDED AGAINST UNAUTHORIZED ACCESS/ DISCLOSURE (INSURANCE COMPANY)

Rating	Control Portfolio Option	CARD® I.D.
( ) 7.	Ensure that background checks have been done on all cleaning and maintenance staff prior to them being allowed to work on company premises.	_____
( ) 8.	Install camera monitoring equipment on all floors and have a full time person continuously monitor all floors between the hours of 6:00 p.m. and 7:00 a.m.	_____
( ) 9.	Develop an educational video titled "Protecting Our Clients" which raises the awareness of staff regarding the need to protect client related information and their responsibilities in this area.	_____
( ) 10.	Relocate the guard station to position it between the door and the elevator banks and require all staff accessing the building to have a photo ID visible at all times.	_____
( ) 11.	Train security people to request that photo ID be worn/produced by all persons on company property after hours and to record the names of any staff found in areas other than their normal work areas. Randomly test the alertness of building security staff by having individuals attempt access without correct identification.	_____
( ) 12.	Develop a module on security awareness, including the need to protect client related information. Ensure that all supervisory positions and higher have been exposed to this training.	_____
( ) 13.	Include a section in the performance contracts and job descriptions of all managers who handle client related information on safeguarding of sensitive client related information.	_____
( ) 14.	Ensure that management personnel are made aware of all known methods used by organized crime to steal/access sensitive client related information held by insurance companies by designating an individual to monitor and report on trends in this area.	_____

EXERCISE 4: *REMEMBER: KEEP THE OBJECTIVE IN FOCUS.*

OBJECTIVE: ENSURE THAT INFORMATION RELATED TO POLICYHOLDERS IS SAFEGUARDED AGAINST UNAUTHORIZED ACCESS/ DISCLOSURE (INSURANCE COMPANY)

Rating	Control Portfolio Option	CARD® I.D.
( ) 15.	On a random surprise basis hire individuals to attempt to gain access to sensitive client related information in the custody of the company. Analyze and report on the success rates and methods utilized by these individuals to periodically reassess control design adequacy.	_____
( ) 16.	Assign specific responsibility for safeguarding policyholder information to the head of corporate security.	_____
( ) 17.	Have internal audit include safeguarding of policyholder information on all audit programs and ensure that all areas are audited at least every five years.	_____
( ) 18.	Have all staff in all areas regularly self-assess the adequacy of controls related to this objective.	_____

PART 4 GROUP EXERCISE - IDENTIFYING ROOT CAUSE OF CONTROL BREAKDOWNS

REQUIRED: For each of the situations outlined below develop/define three control element options which your group believes would likely have the highest impact per dollar of cost. The exercises completed earlier in this workshop on control design optimization illustrate the type of description required. The goal should be that the control choices proposed by your group would most often be selected by fully trained risk/control design consultants as top impact/dollar options when asked to select from a wider selection of 15 to 20 risk reduction strategies. It is strongly recommended that you identify the key Threats to Achievement prior to developing your control design recommendations.

1. MINIMIZING UNNECESSARY COSTS

Your organization is large and geographically dispersed. The annual telecommunications budget is in excess of 30 million dollars annually. A portion of this budget relates to fax transmissions. There are in excess of 50 fax machines of various vintages spread across the company.

Business/Quality Objective:

Minimize the cost of meeting the organization's document communication needs.

Top 3 Impact/$ Control Design Choices:

(1)_____

_____

_____

(2)_____

_____

_____

(3)_____

_____

_____

2. ENVIRONMENTAL COMPLIANCE

A new law has been passed which imposes very strict rules on the handling and disposal of laser printer cartridges. The legislation includes large fines and jail sentences for Officers of any company caught violating this new legislation. Laser printer cartridges are used widely all across your organization and have previously been discarded by most units, and recycled only by a few particularly environmentally conscious units. Those who have thrown out cartridges in the past generally claim that the quality of recycled units was not acceptable.

Business/Quality Objective:

Ensure that legislation related to handling and disposal of laser printer cartridges is complied with by all units and all staff.

Top 3 Impact/$ Control Design Choices:

(1)_____

_____

_____

(2)_____

_____

_____

(3)_____

_____

_____

3. CUSTOMER SERVICE

You are an employee in a 5 person multi-disciplinary Control Training and Advisory Unit. Your unit's mandate includes providing training to staff at all levels on control assessment and design and providing control design consulting services on request. Your unit also provides control design architectural services on projects involving new systems and new business activities. One of your unit's business/quality objectives is to provide high quality control design advice that is as good as, or better than, the advice available from external sources. Your Vice President has recently requested that you self-assess yourself on this objective and discuss the results with her.

Business/Quality Objective:

Provide high quality control design advice that is as good as, or better than, the advice available from external sources.

Top 3 Impact/$ Control Design Choices:

(1)_____

_____

_____

(2)_____

_____

_____

(3)_____

_____

_____

4. REGULATORY COMPLIANCE

You have read that a new employment equity law has been passed and organizations must begin complying with this new legislation in 3 months. The changes are extensive and the penalties for non-compliance are severe including jail sentences for Officers and Directors. This legislation requires that detailed records be kept supporting how jobs are classified and pay structures developed. All situations which are considered to be discriminatory by the legislation must be corrected within 2 months of the date the problem is identified. The legislation also requires that regular oversight reviews be conducted to ensure that all the provisions are being complied with. The new legislation is over 200 pages in length. The Human Resource Department has requested that you work with them to construct a control design that provides a virtually certain level of assurance that the law will be complied with and the personal liberty of your Officers maintained.

Business/Quality Objective:

Ensure that employment equity laws are complied with by the company and all personnel.

Top 3 Impact/$ Control Design Choices:

(1)_____

_____

_____

(2)_____

_____

_____

(3)_____

_____

_____

5. SAFEGUARDING OF ASSETS

You have just completed an analysis of computer disc purchases across your entire organization. It appears that over the past 5 years purchases of 3.5 inch computer discs have been skyrocketing at a rate of over 25% per year compound growth. These discs are bought by each business unit from a national office supply company that your company has a blanket contract with. Current controls require that the manager or supervisor of the requisitioning area sign a purchase order which is then sent by fax to the local office supply store. You have determined, based on your analysis of the office supplies records for the last two years, that the number of computer discs charged to your company would equip every employee with over 80 discs each assuming a 10% damage and discard rate. You have done some random surveys of units regarding the number of discs on site and concluded that the actual number of discs per person is about 15. You are convinced that over $150,000 per year of computer discs are being stolen by employees.

Business/Quality Objective:

Reduce the theft of computer discs by company employees to less than $15,000 per year across the country.

Top 3 Impact/$ Control Design Choices:

(1)_____

_____

_____

(2)_____

_____

_____

(3)_____

_____

_____

6. ACCURATE FINANCIAL ACCOUNTING AND FRAUD PREVENTION/DETECTION

A key responsibility of one division of your organization is to pay claims submitted by clients related to insurance coverages you provide. Audits dating back to 1985 have reported that the bank reconciliations for accounts used to make these payments have not been done properly. The net unreconciled difference is currently in excess of $50,000. Staff suspect that the number of items to reconcile this account is in excess of 300 items spread over the last eight years. Management in this area has promised in responses to three separate audits over the eight years to correct this problem area. The 1993 audit has again identified and reported this as a problem area.

Business/Quality Objective:

Reliable financial accounting records and fraud prevention and detection.

Top 3 Impact/$ Control Design Choices:

(1)_____

_____

_____

(2)_____

_____

_____

(3)_____

_____

_____

7. CUSTOMER SERVICE

You are a manager in a large Internal Audit organization with over 40 professional staff. A recent customer survey has revealed that a majority of the managers of the areas you audit are of the opinion that your department:

(1) Reports insignificant issues which require far more of their time and their staff's time to formally respond to than is warranted by the risks.

(2) Often recommends "old style" controls such as hierarchical approval sign-offs, supervisor review, high levels of documentation and other high cost, low return controls.

(3) Rarely examines and provides advice on areas of key importance to the success of their areas such as customer service, and minimizing unintentional exposure to risk.

Your officers have indicated that from their perspective the most important deliverable from Internal Audit is timely, complete and accurate information on the state of control and the significant risks being accepted across the entire organization.

The audit methods you have been using over the past two years include a risk model, recommended by the IIA, a well developed audit and reporting methodology and a state of the art project tracking system. Your frequency of coverage ranges from 2 to 6 years. Not all areas are audited and not all exposure areas are covered in the units that are audited.

Business/Quality Objective:

To provide service to our customers which fully meets or exceeds their needs.

Top 3 Impact/$ Control Design Choices:

(1) _____

_____

_____

(2) _____

_____

_____

(3) _____

_____

_____

IDENTIFYING & EVALUATING RESIDUAL RISK STATUS

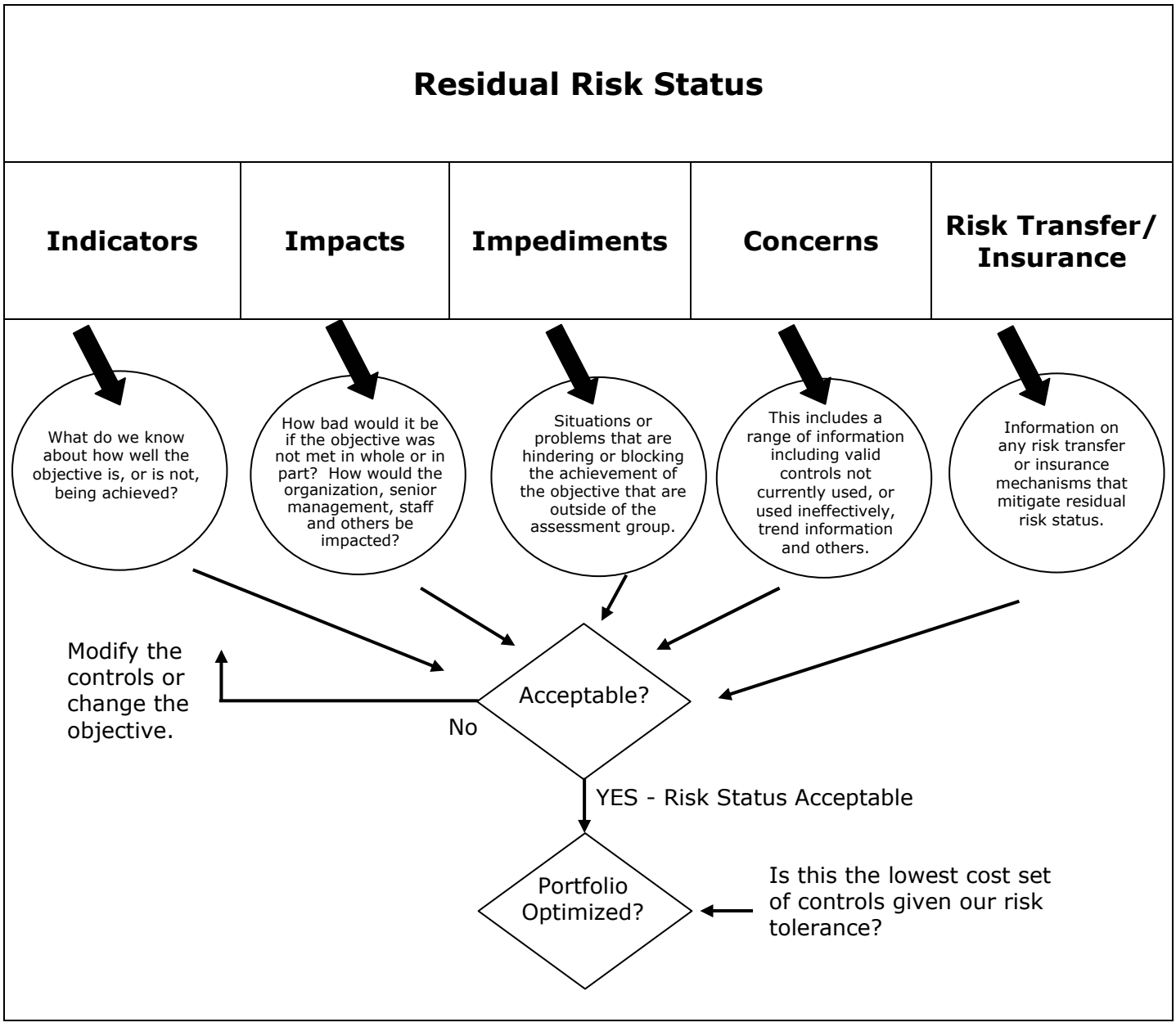
Section Objective:

(1) Train participants to develop a clear picture of residual risk status to assist work units and senior management make better, more defensible risk acceptance decisions.

Simply put:
Can I tolerate the risk?

BACKGROUND

This section provides participants with a general introduction to the elements that comprise Residual Risk Status. Residual Risk Status provides a collection of information decision makers can use to decide whether to maintain the status quo, or make changes. It has been designed to foster accountability for work unit and senior management risk acceptance decisions. A key goal of auditors should be to seek consensus agreement on the acceptability of the residual risk status.



RESIDUAL RISK STATUS: KEY POINTS TO REMEMBER

1. Residual risk status is made up of five types on information: "Indicators, Impacts, Impediments, Concerns, and Risk Transfer/Insurance". This section is designed to capture information that will help you and/or your work team decide whether the current residual risk status is acceptable. The level of precision and detail should be adjusted to a level that results in a well thought out decision, but not so detailed that the group gets bogged down in detail.

2. Often the residual risk status is influenced by constraints such as a lack of funds, inadequately trained staff, senior management's lack of commitment, management skills, ethics in the organization and many other factors. Residual risks status often provides a good indication of your organization's culture and attitude to risk.

3. Care must be taken if your organization or unit is breaking laws or consciously breaching policy and/or contract provisions. Your trainer/facilitator can assist you by providing guidelines in this area. Prudent candidness is recommended. In some cases legal counsel should be consulted.

4. Identification of "Impediments" provides an excellent opportunity to formally articulate situations outside of the control of a unit that are frustrating and resulting in sub-optimal performance and/or non achievement of a stated business/quality objective.

5. "Impacts" means how bad would it be if a business/quality objective was not achieved in whole or part. Non-achievement of some objectives can literally mean the demise of an organization or the firing of the staff responsible or staff that are identified by senior management as responsible. It is important to be realistic in examining impacts. The magnitude and severity of the impacts related to residual risk have a major influence on the motivation of organizations, work teams and individuals to ensure an objective is achieved, and the control portfolio is effective.

6. "Concerns" is a term used to cover any problems that are known or suspected that are directly related to the objective being examined. This category allows broad expression of the group's thoughts and concerns related to the achievement of the business/quality objective. The non use of key generally accepted controls can be noted under this heading.

7. "Indicators" refers to anything the group knows about how effective the current control choices are with respect to the stated business/quality objective. Often evidence already exists relating to the current effectiveness of the control elements. The indicator category will be directly impacted by the quality of indicator/measurement controls currently in use.

8. "Risk Transfer/Insurance" provides a vehicle to describe any insurance coverages or other risk transfer devices that relate to the specific business unit or objective. Significant exceptions or exclusion can also be described.

SAMPLE RESIDUAL RISK STATUS ILLUSTRATIONS

EXAMPLE #1

Business Quality Objective: **Minimize the cost of acquiring necessary household appliances, groceries and other goods and services.**

Residual Risk Status:

SAMPLE "INDICATOR" INFORMATION

Any information known about how effective the current control choices are with respect to the stated business/quality objective.

- Sales advertisements on selected items frequently indicate lower grocery prices than prices paid by the family at Foodco.
- A comparison check last year on six items between Foodco and Saveco showed Saveco lower on 3 items. The maximum difference was 3%. The same price was charged on 3 of the 6 items (the family shops at Foodco).
- Don't currently know if we are getting the best price on car repairs and maintenance as no comparisons have been done in the past 8 years.
- A spot price comparison after the last purchase of a TV indicated a premium of 10% was paid; however the family says they trust the owner to rectify any problems.

SAMPLE "IMPACT" INFORMATION

How bad would it be if the objective was not met in whole or in part? How would the organization, the officers, the staff be impacted?

- Groceries accounts for 10% of the total household budget or about $9,600/year. A 5% improvement would save $480/year.
- The family believes savings on groceries and appliances would likely allow more money for eating out in restaurants reducing the time spent on meal preparation and clean up.
- Don (the dad) was teased by their neighbour (Larry) for careless spending when it was learned he paid $40 more for the same lawn mower Larry bought because he did no comparison shopping.

SAMPLE "IMPEDIMENT" INFORMATION

Any situations or problems that stand in the way of the group or a group member adjusting the control element portfolio. These can relate to lack of funds, cooperation of staff members or other departments, training deficiencies, senior management attitudes, and others.

- The children have refused to use lower priced facial and bathroom tissue as they claim they are too rough.
- Lower prices are available in Bigville at Saveco but the cost in terms of time and gas of the 20 mile trip often offsets any savings.
- Some family members are adamant they will only accept big name products (e.g. Coke, Tropicana orange juice, etc.).

SAMPLE "CONCERNS" INFORMATION

Any known or suspected problems or issues related to the business/quality objective being assessed.

- Since responsibility for shopping is shared between both parents there is currently no clarity on who is directly responsible for developing and proposing cost saving strategies.

- The family has never had a formal household budget or attempted to analyze spending patterns for savings opportunities.

- Both parents know very little about auto maintenance and stated that they take all repair estimates from their garage on faith. They acknowledge they could be paying as much $300-$500/year in unnecessary repairs.

- No analysis or research has been done to analyze the benefit of the family practice of always paying for extended warranties on major appliance purchases (e.g. washer, T.V., VCR, etc.).

- None of the family have ever taken any training on techniques to save money on household purchases.

- Comparison shopping, even on major purchases, is often not done, or if done, usually only involves obtaining one additional price quote.

- The family has never had anyone review the approach they use to manage household spending.

SAMPLE "RISK TRANSFER/INSURANCE" INFORMATION

Information on any risk transfer or insurance mechanisms that mitigate residual risk.

- The family's credit card provides double the manufacturers warranty and 90 days loss or breakage coverage for items purchased using the credit card.

- The family has a blank replacement cost insurance policy that covers up to $100,000 of household appliances and other goods that are stolen, lost in a fire or destroyed by a flood or hurricane. Losses related to sewer back-ups are excluded.

SAMPLE RESIDUAL RISK STATUS ILLUSTRATIONS

EXAMPLE #2

Business Quality Objective: **Prevent death and injuries in the home due to fire.**

Residual Risk Status:

SAMPLE "INDICATOR" INFORMATION

Any information known about how effective the current control choices are with respect to the stated business/quality objective.

- In the past five years there has been one grease fire in the kitchen. There have been no other fires in the family home.
- A renovation project last year showed evidence that an electrical connection was faulty and had created burn marks on the floor beams.
- The current breaker for the outlets in the work room frequently trip and must be reset due to excess load on the circuit.
- There have been two cases of minor burns to family members while barbequing, however alcohol was considered a contributing factor.

SAMPLE "IMPACT" INFORMATION

How bad would it be if the objective was not met in whole or in part? How would the organization, the officers, the staff be impacted?

- The grease fire resulted in the kitchen having to be washed and repainted. Total time required was approximately 20 hours at a cost of $400 including supplies.
- The grease fire caused minor burns on Frank's (the father) hands and burned off one eyebrow and hair on his right arm.

- Minor burns incurred while barbequing, while painful, caused no lasting damage.
- Fires in the home on a national basis result in 200-300 deaths per year and many more injuries requiring hospitalization.
- The house insurance has a $500 deductible. Single incident claims of more than $1,000 result in an immediate premium increase of 15% for five years over claim free status.

SAMPLE "IMPEDIMENT" INFORMATION

Any situations or problems that stand in the way of the group or a group member adjusting the control element portfolio. These can relate to lack of funds, cooperation of staff members or other departments, training deficiencies, senior management attitudes, and others.

- The cost to correct the problem with the overloaded electrical circuit in the work room is thought to be around $1,000 based on work the neighbour had done. Other priorities have diverted funds away from this problem.
- Frank (the father) has shown increased evidence of forgetfulness since he turned 40, increasing the risk of incidents like the grease fire.

SAMPLE CONCERNS INFORMATION

Any known or suspected problems or issues related to the business/quality objective being assessed.

- The two smoke detectors in the house have never been tested using smoke other than when someone burns the toast and they have sounded.
- The family does not have a plan detailing steps to be taken in the event of a fire and have never had a fire drill.
- The electrical outlets in the house have never been tested to check whether they are properly grounded (cost about $6).
- The house has never been inspected to identify fire related risks.

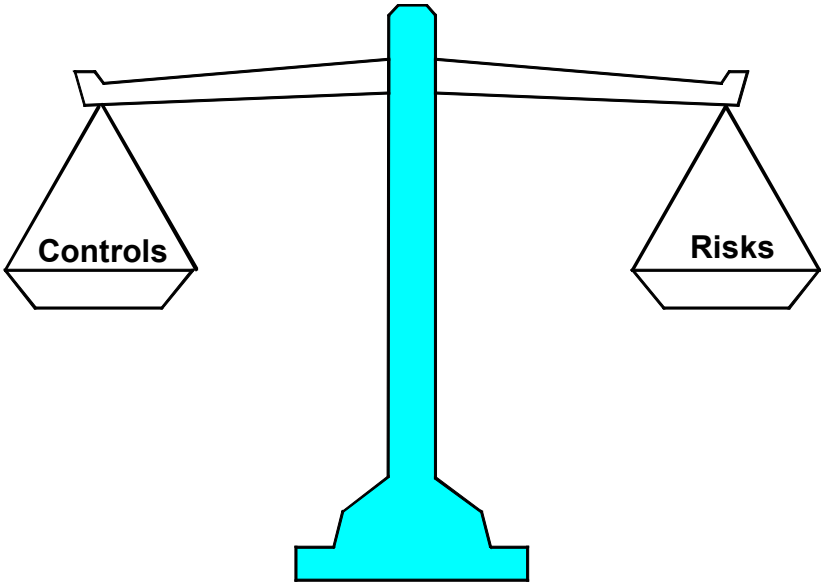
- The children have never been shown how to use the fire extinguisher in the back storage closet.
- Two of the family members indicated they didn't know where the fire extinguisher was located or how to use it.
- Both smoke detectors are battery powered. There is no smoke detector powered by electricity.
- Most of the family have never read the safety operation manual for the gas barbeque.

SAMPLE "RISK TRANSFER/INSURANCE" INFORMATION

Information on any risk transfer or insurance mechanisms that mitigate residual risk status.

- Many of the manufacturers of appliances used in the house carry large insurance policies related to injuries and death caused by product defects.
- In many cases coverage and warranty may be voided if not installed by a certified installer (i.e. pool heater, air conditioner)
- One parent carries a 1 million dollar term life policy and $500,000 accidental death policy.

Residual Risk Index Rating



Residual Risk Index = 0

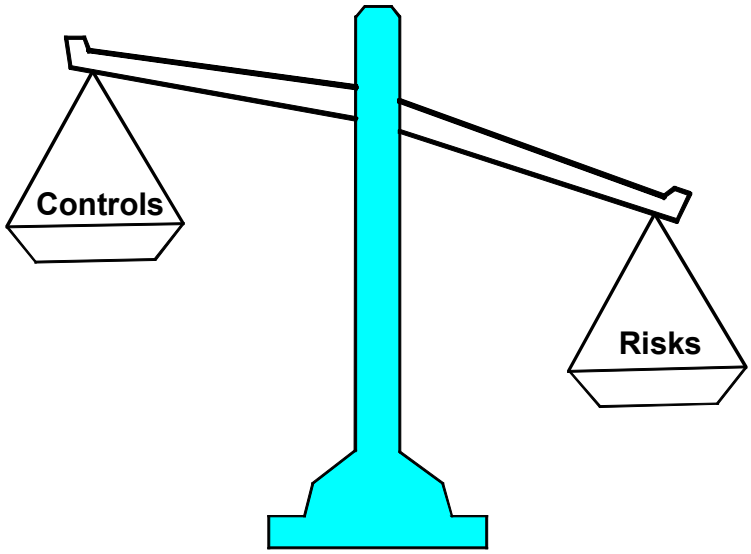
Controls are "adequate". Residual risk status is "acceptable".

CONTROLS AND RISKS ARE IN BALANCE

This rating implies that the group:

- accepts the current residual risk status;
- believes that the current controls elements selection is adequate in relation to the importance attached to achieving the business/quality objective;
- does not believe that any changes need to occur at the present time to the control element portfolio because of unacceptable risk of non-achievement; and
- can now examine whether the control portfolio is "optimized" (i.e. the least costly combination of controls that result in an acceptable residual risk status).

Residual Risk Index Rating



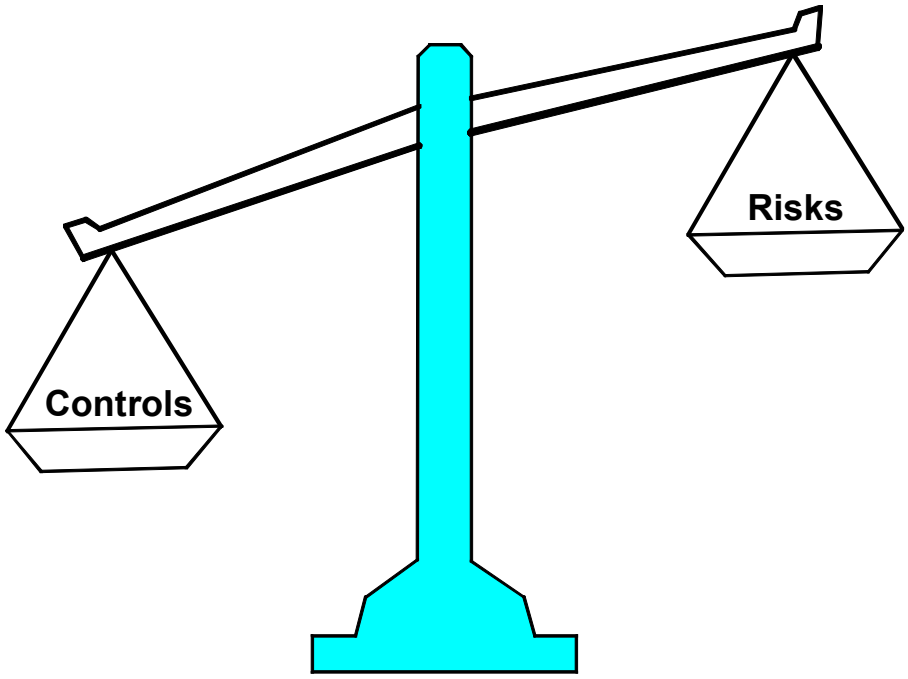
Residual Risk Index = +1

Controls are "inadequate". Residual risk status is "unacceptable".

A risk acceptance index of +1 indicates that the group believes that:

- the residual risk status is unacceptable;
- controls should be strengthened and/or modified; and
- the business/quality objective is not being met, or may not be met to the degree considered necessary.

Residual Risk Index Rating



Residual Risk Index = -1

Controls are "excessive". Residual risk status is below the current tolerance level.

A risk acceptance index of -1 indicates that the group believes that:

- controls are too costly in terms of dollars and/or time; and
- the risk status is below current tolerance levels given the importance attached to the business/quality level and the impacts associated with the risk status.

GROUP EXERCISE:

Your workshop leader will select an objective that is relevant and generally understood by workshop participants. He/she will then illustrate how a description of the current residual risk status can be generated using CARD®*map* software. The concepts applied during this demonstration are also applicable on direct report audits. The key difference between workshops and audits is how the information is obtained.

Two sample CARD®*lines* are included in the section to illustrate a completed CARD®*line* including sample Residual Risk Status elements.

ABC Insurance Co. is a subsidiary of ABC Conglomerate

ABC Conglomerate\ABC Insurance Co.
ABC Conglomerate

Edit History	Created by Michelle Burn/N4S on 05/18/99 02:21:28 PM
Business/Quality Objective	Ensure Underwriting decisions on life insurance applications are based on reliable and truthful information
Family	Unintentional Risk Exposure
Business Process	
Objective Importance	High (Work Unit) High (Corporate)
Risk Sharing	Partial
Analysis Method	
Performance Indicator Status	-

Knowledge Status

Current Level	3 Medium
Target Level	4 High

Threats to Achievement

Unassigned
Threat 1: Applicant lies on application
Threat 2: Test results are inaccurate
Threat 3: Test results are falsified
Threat 4: Agent colludes with client
Threat 5: Client colludes with Lab personnel
Threat 6: Client colludes with person hired to do examination
Threat 7: Inaccurate data capture and/or transmission to head office
Threat 8: Unauthorized changes to computer files
Threat 9: Form design lacks key information necessary for validation
Threat 10:

Control Portfolio

3.4 Selection process for testing labs includes a site visit by an ABC staff person (in most cases)

5.1 The medical form requires that the person who claims to be a doctor state the time that he/she has known applicant (i.e. # of years).

5.1 Third party medical information consent form has a space that requires paramedics to attest that they have requested and seen some type of I.D. such as a photo I.D. card of some type.

5.1 All benefit claims over $1 000 000, and contestable claims flagged as suspicious are reviewed prior to payment for any unusual circumstances.

5.1 For policy applications with coverage in excess of $1 000 000 there must be financial background information on the applicant obtained and reviewed.

5.1 Producers are required on applications >$1,000,000 to include a cover letter outlining their background knowledge of client's situation and need for insurance.

5.1 Branch writes to the person that the applicant represents is their doctor for information on the person's medical history.

6.1 In-house actuaries review mortality trends and claim patterns for irregularities.

Residual Risk Status

Concern - Unrated	Being diligent and highly effective in this area could put ABC at a competitive disadvantage.
Concern - Unrated	Branch is probably not checking that the alleged doctor is currently registered and practicing, but participants were not sure. (i.e. they are a real doctor - a control mechanism is available in computer form to the industry for this).
Concern - Unrated	Currently examiners often do not check photo I.D. in any event per underwriting staff.
Concern - Unrated	Doctors are not required to take steps to verify that the person that they are examining and reporting on is, in fact, the applicant.
Concern - Unrated	IA and/or other specialists have not done any specific fraud vulnerability reviews in this area.
Concern – Unrated	Procedures are not specifically instructed to draw red flags or concerns they have with an application to the attention of Underwriting. The nature of the business transaction and compensation system actually suggests they should not draw red flags to the attention of Underwriting.
Concern – Unrated	The quality of lab inspection work, i.e. qualifications of investigators used, is not known. No quality assurance review has ever been done by ABC or by an expert reviewer as far as staff knows.
Concern – Unrated	Underwriters have not received any formal training on suspicious red flags in Underwriting data.
Concern – Unrated	Underwriting personnel are currently unaware of the specific steps done on death claims or their likely effectiveness.
Concern – Unrated	Underwriting procedures are not appreciably different when doctor has no background knowledge of, or prior dealings with, the applicant.
Concern – Unrated	What constitutes an "acceptable" photo I.D. is not defined by the company.
Impact	Even a small number of fraudulent claims has the potential to impact total corporate earnings (eg. a small organized scheme could hit earning for over 50 million.)
Impediment	Controls that negatively impact on sales and the sales process will be very difficult to sell/implement in the field given the commission pay system.

Risk Acceptance Comp. Index -

Risk Acceptance History

Action Items

Portfolio Optimized

Date of Last Review
Review Frequency Not Specified
Control Status Commentary

Other Imp. Parties Commentary

Note: Check the popup help below for tips on embedding files
Supporting Documentation

Current Assurance Level Not Rated
Target Assurance Level Not Rated
Assurance Provider
Audit Opinion/Rating -
Date of Last Assurance Review
Assurance Review Frequency
Report Generator Flag Corporate Level Report

ABC Insurance Co. is a subsidiary of ABC Conglomerate

ABC Conglomerate\ABC Insurance Co.
ABC Conglomerate

Edit History	Created by Michelle Burn/N4S on 05/18/99 03:02:06 PM
Business/Quality Objective	Ensure reinsurers are financially capable of honouring risks assumed.
Family	
Business Process	
Objective Importance	- (Work Unit) - (Corporate)
Risk Sharing	
Analysis Method	
Performance Indicator Status	-

Knowledge Status

Current Level	-
Target Level	-

Threats to Achievement

Unassigned

Threat 1:
Threat 2:
Threat 3:
Threat 4:
Threat 5:
Threat 6:
Threat 7:
Threat 8:
Threat 9:
Threat 10:

Control Portfolio

3.4 The legal department reviews and approves all reinsurance contracts prior to signing.

3.4 New treaties with reinsurance companies have undergone a rating check, analysis of rates, capacity capability, and a review to assess whether their underwriting philosophy is generally consistent with the company's approach including having one on one discussions with reinsurer personnel and analysis of acceptance patterns.

3.4 Financial statements for the reinsurer are obtained at time of treaty negotiation and reviewed.

4.1 The corporate reinsurance division is more directly involved in the reinsurance industry and more closely tracking trends (not part of Underwriting.) They occasionally provide information on an informal basis to Underwriting re: reinsurers used by the underwriting department.

5.1 The current financial ratings of all reinsurers as determined by rating agencies is checked annually.

6.9 Claim payment patterns of reinsureres are informally tracked and recorded (note: they are not analyzed on a long trend basis.)

Residual Risk Status

Concern - Unrated ABC has little or no knowledge of how older existing reinsurers were originally checked out/selected.

Concern - Unrated ABC not currently subscribing to any reinsurance periodicals/journals.

Concern - Unrated All treaties currently in force do not contain a release clause triggered by financial deterioration of reinsurer.

Concern - Unrated Corporate reinsurance has no direct responsibility to notify Underwriting when they become aware of information detrimental to the reinsurance exposure managed by Underwriting.

Concern - Unrated Feedback on claims payment philosophy and/or history of specific reinsurance companies not checked and monitored.

Concern - Unrated Internal audit has never analyzed the risks and controls related to this objective.

Concern - Unrated	No requirements in treaties related to who must certify/attest to the financial results and position of reinsurers (i.e. who can audit financial statements of reinsurers.)
Concern - Unrated	No Underwriting employee currently belongs to any reinsurance professional networking associations/agencies.
Concern - Unrated	Responsibility for this objective is not formally assigned.
Concern - Unrated	Treaties with reinsurers were reviewed by general legal counsel, not by reinsurance legal specialists.
Impact	Total amount of policy amount reinsured thought to be in excess of 3 billion.
Impact	Worst case single reinsurer insolvency loss scenario thought to be in the 50 to 100 million range by Underwriting staff, but staff are not sure on this. This exposure would increase to very serious proportions if there was a major collapse of numerous reinsurers over a limited time span.
Impediment	ABC staff feel they may not currently have the internal resources to monitor /control this area to the degree considered necessary given the amount of risk.
Impediment	Somebody in senior management of the new business area concluded sometime ago that reinsurance contracts could not contain release clauses linked to the financial stability of reinsurer. This may still be an industry issue.

Risk Acceptance Comp. Index -

Risk Acceptance History

Action Items

Portfolio Optimized

Date of Last Review

Review Frequency Not Specified

Control Status Commentary

Other Imp. Parties Commentary

Note: Check the popup help below for tips on embedding files

Supporting Documentation

Current Assurance Level	Not Rated
Target Assurance Level	Not Rated
Assurance Provider	
Audit Opinion/Rating	-
Date of Last Assurance Review	
Assurance Review Frequency	
Report Generator Flag	

USING TECHNOLOGY TO BETTER MANAGE CONTROL & RISK

Section Objectives:

(1) Provide a forum to debate the ideal specifications for risk and assurance information systems.

(2) Introduce the Paisley Consulting "Wish List For The Ideal Risk Management & Assurance Information System" to assist participants who are considering building, or acquiring risk and assurance management computer software.

BACKGROUND

Most formalized control and risk assessment work has traditionally been done by internal and external assurance groups such as Internal Audit, External Audit, Quality, Safety, Environment, Risk & Insurance, Security and others. The vast majority of this work has been done manually or using standalone PC software.

Over the past few years computerized entity-wide risk management and assurance software has entered the scene.

GROUP EXERCISE

In your assigned group develop as many user requirements for the ideal Risk Management & Assurance information system as you can in the time allocated. Examples include "Ability to rate risks in terms of likelihood and consequences", "Ability to track and report the status of all corrective action underway".

WISH LIST FOR THE IDEAL RISK MANAGEMENT & ASSURANCE INFORMATION SYSTEM
USER REQUIREMENTS
WORK UNITS
1.
2.
3.
4.
5.

WISH LIST FOR THE IDEAL RISK MANAGEMENT & ASSURANCE INFORMATION SYSTEM
USER REQUIREMENTS
SENIOR MANAGEMENT
1.
2.
3.
4.
5.

WISH LIST FOR THE IDEAL RISK MANAGEMENT & ASSURANCE INFORMATION SYSTEM
USER REQUIREMENTS
INTERNAL AUDIT
1.
2.
3.
4.
5.

WISH LIST FOR THE IDEAL RISK MANAGEMENT & ASSURANCE INFORMATION SYSTEM
USER REQUIREMENTS
EXTERNAL AUDIT
1.
2.
3.
4.
5.

WISH LIST FOR THE IDEAL RISK MANAGEMENT & ASSURANCE INFORMATION SYSTEM
USER REQUIREMENTS
ENVIRONMENT
1.
2.
3.
4.
5.

WISH LIST FOR THE IDEAL RISK MANAGEMENT & ASSURANCE INFORMATION SYSTEM
USER REQUIREMENTS
SAFETY
1.
2.
3.
4.
5.

WISH LIST FOR THE IDEAL RISK MANAGEMENT & ASSURANCE INFORMATION SYSTEM
USER REQUIREMENTS
RISK & INSURANCE
1.
2.
3.
4.
5.

NAME OF SOFTWARE:	
RISK & ASSURANCE INFORMATION SYSTEM SOFTWARE EVALUATION CRITERIA	
Software Product(s) Scores (1-10 1 = Poor/Non Existent 10 = Excellent/Full Capability)	
FEATURES:	
1. Ease of use/learning curve a. For Auditors b. For Work Units c. For Senior Management	
2. Ability to record, store, retrieve and report on control/risk information.	
3. Ability of work unit and management personnel to create, access and update control/risk information related to their business unit.	
4. Ability of users to work remotely without being connected to a network.	
5. Ability to automate audit/assurance working papers.	
6. Supports the use of national/international or customized control frameworks (e.g. CARD®*model*, COSO, CoCo etc.)	

NAME OF SOFTWARE:	
RISK & ASSURANCE INFORMATION SYSTEM SOFTWARE EVALUATION CRITERIA	
Software Product(s) Scores (1-10 1 = Poor/Non Existent 10 = Excellent/Full Capability)	
7. Supports the use of a risk model or framework (e.g. Australian Risk Standard, CARD®*model* Risk Arena, etc.)	
8. Allows database updates/access using the World Wide Web.	
9. Existence and quality of software support infrastructure including help desk, trainers and technical support.	
10. System security options/ features.	
11. Assurance resource audit planning capability/ functionality	
12. Ability to store and report status of all work unit action plans.	

NAME OF SOFTWARE:	
RISK & ASSURANCE INFORMATION SYSTEM SOFTWARE EVALUATION CRITERIA	
Software Product(s) Scores (1-10 1 = Poor/Non Existent 10 = Excellent/Full Capability)	
13. Export/graphing capability.	
14. Ability to support custom retrievals/reporting of relevant control/risk information.	
15. Supports control/risk analysis at the macro/entity level, mid level, and micro level.	
16. Ability to store workshop voting results on existence of control criteria and risk profiling.	
17. Supports multiple control/risk assessment approaches (i.e. business objective, risk focus, control criteria, business process, ad compliance etc.)	
18. Capability as a reference/training tool for: a. Auditors b. Work Units	

NAME OF SOFTWARE:	
RISK & ASSURANCE INFORMATION SYSTEM SOFTWARE EVALUATION CRITERIA	
Software Product(s) Scores (1-10 1 = Poor/Non Existent 10 = Excellent/Full Capability)	
19. Incorporates risk transfer/insurance information.	
20. Capability to support cost reduction initiatives.	
21. Ability to export information to other software tools/ applications.	
22. Accessibility/quality of on-line help	
23. Quality of implementation/ training processes and materials.	

FIT WITH EXISTING INFRASTRUCTURE	
1. Compatibility with other standard software tools (e.g. WORD, WordPerfect, Excel, PowerPoint etc.)	
2. Fit/Integration with existing business processes (e.g. planning/budgeting, compensation, Balanced Scorecard, etc.)	
FIT WITH FUTURE INFRASTRUCTURE	
1. Facilitates corporate reorganizations and personnel changes.	
2. Ability to integrate/fit with I.T. strategic mid range/long range plan.	
COST	
1. Cost of purchasing the software.	
2. Cost of implementing the software.	
3. Cost of maintaining the software.	

CORE DATA ELEMENTS IN CARD®*map* SOFTWARE

ABC Insurance Co. is a subsidiary of ABC Conglomerate
ABC Conglomerate\ABC Insurance Co.
ABC Conglomerate

Edit History

The "audit trail" left behind after a user edits and saves a CARD®*line*. Clicking the grey button beside Edit History at the top of the CARD®*line* will display a list of users who have made changes to the CARD®*line* and the date the change was made.

Business/Quality Objective

Business/Quality Objectives are the backbone of CARD®*map*. All information in the database is collected in the context of Business/Quality Objectives or sub-objectives.

Family

Groupings of Business/Quality Objectives under which mid-level and micro-level objectives can be organized. (e.g. Product Quality, Customer Service, Accounting Reliability, etc.)

Business Process

The related business cycle or process. By linking Business/Quality Objectives to processes it is possible to view the universe by process as well as objective. Organizations that have undergone business process reengineering, have done extensive process mapping, or adopted a process focus for audit purposes will find this feature particularly useful.

Objective Importance

An estimate for the work unit and total organization of the consequence and likelihood of not achieving the business/quality objective(s). (i.e. how bad would it be if the objective(s) was/were not achieved?)

Risk Sharing

Users can identify which objectives have some form of risk transfer or insurance in place. Details of the risk transfer/insurance mechanism can be entered as part of the Residual Risk Status information in the Edit Controls & Risks input screen using the Risk Transfer/Insurance information title.

Analysis Method

The method used to analyze controls and risks related to the business objective. CARD®*map* integrates the various types of assessment work done by a wide range of assurance providers.

Date of Last Review

The date when the CARD®*line* information was prepared or last reviewed. CARD®*line* information can be prepared and maintained by work units (ideally) or by assurance groups.

Next Scheduled Review

The date the work unit or assurance provider plans to update CARD®*line* information.

Key Date

This date can be used for a variety of reminder dates including progress checks by teams, project or senior management, or for other purposes.

Performance Indicator Status

A judgemental rating assigned by the CARD®*line* owner or an assurance provider of how well the Business/Quality Objective is currently being achieved.

Knowledge Status
Current Level
Target Level

Current Level: How much is currently known about the control/risk status related to a specified objective. As the rating increases the amount of formal documentation of control/risks status must also increase.

Target Level: How much should be known about the control/risk status related to a specified objective. The Target Level of Knowledge Status would normally be strongly correlated to the risk of non-achievement.

Threats to Achievement

Possible problems or situations which could result in non-achievement of an objective. Threats can be categorized by Risk Source using the Risk Source categories provided, or using a customized Risk Source list. Threats can also be analyzed in terms of consequence and likelihood. The system generates a Residual Risk Level and a Threat Risk Index for each Threat.

Control Portfolio

A description of the controls actually in use or in place in the organization. This description can be developed using the CARD®*model* control framework as a completeness aid or using one of the national control models such as COSO or CoCo, or a customized model.

Residual Risk Status

A composite set of information that helps decision-makers evaluate the acceptability of residual risk status. This includes information on Concerns, Indicator information, Impact information, Impediment information and Risk Transfer/Insurance details.

Residual Risk Index

This is a composite rating by the owner of the CARD®*line* of the severity of the current Residual Risk Status. The "RRI" is a very important piece of summary information that can be used to create "Heat Maps". Heat Maps identify where the organization's highest Residual Risk Status objectives are located.

Risk Acceptance History

Commentary on the history of, and reasons for, previous Risk Acceptance decisions. This field allows a narrative history of prior decisions on controls and risks.

Action Items

When a CARD®*line* has Unacceptable Concerns or Impediments and an unacceptable Residual Risk Index, steps must be taken to address these issues. Action Plans can be accessed by clicking the separate Action Items button on the top of each CARD®*line*.

Portfolio Optimized

Does the group believe that they have the most economical, efficient, and effective combination of controls that provides a level of risk that the group and/or company is willing to accept? Could less be spent on controls and still have an acceptable level of residual risk?

Other Imp. Parties Commentary

Commentary from other impacted parties that have an interest in the assessment or status of a particular business/quality objective.

Supporting Documentation

Information from other sources stored as Microsoft Word files or other formats can be added using the Create/Object command. The File Attach command can also be used. Detailed quantitative risk assessment studies would be an example of the type of document that a user might want to file in this field.

Assurance Information

Information input by the primary assurance provider.

Current Assurance Level
Target Assurance Level

Current Assurance Level: The assurance providers estimate of the current reliability of the CARD®*line* information

Target Assurance Level: The assurance level necessary to meet the expectations of the assurance provider's customers.

Assurance Provider

The individual or group with primary responsibility for assuring that the CARD®*line* data is reliable.

Assurance Provider Commentary

Comments from the assurance provider on the current control/risk strategy and status.

Audit Opinion/Rating

The assurance provider's opinion on the current control effectiveness and/or acceptability of Residual Risk Status. CARD®*lines* where the Assurance agent has disagreed with the risk accepted by management may be reportable items to the Board and/or Senior Management, or require further analysis by the assurance group.

Date of Last Assurance Review

Date the CARD®*line* was last reviewed by the Assurance Provider.

Next Scheduled Assurance Review

The date or timeframe when the assurance provider plans to review and update the assurance information.

Report Generator Flag

The level in the organization that the Assurance provider believes the CARD®*line* status should be reported. Usually, the higher the Residual Risk Index, the higher the level in the organization the issue will be reported.

EVOLUTION OF GENERALLY ACCEPTED CONTROL CRITERIA "GACC"

Section Objectives:

To: (1) acquaint participants with a sample of the events that have resulted in countries developing generally accepted control criteria ("GACC"), (2) trace the evolution of control models, and (3) provide a general understanding of the similarities and differences between the leading control frameworks. This knowledge will assist participants to assess and select the right control model for use in their organization.

The Need for Control Frameworks/Models: Some Background

Illustration #1 - Bank Failures in Canada

Two major banks fail in Canada in 1984.

A Royal Commission was appointed to examine why they failed (The Estey Commission).

Key findings of the Estey Commission included:

- Improvident lending practices.
- High exposure to risk by lending to focused geographic and industry sectors.
- Passive regulatory, inspection system.
- Shortage of senior management with experience in banking.
- Regulatory system was not changed to reflect rapid bank expansion.
- Unconventional lending practices.
- Aggressive accounting practices (capitalization of accrued interest).
- External auditors failure to apply prevailing principles of bank auditing.
- Directors lacked knowledge of the business and did not insist upon simple and straightforward information from management.

The Need for Control Frameworks/Models: Some Background

Illustration #1 - Bank Failures in Canada (cont'd)

Key recommendations of the Estey Commission included:

- The supervisory functions of the Office of the Inspector General of Banks be consolidated with the insurance functions now exercised by the Canada Deposit Insurance Corporation.
- Inspection staff of the regulator be increased by the addition of qualified and experienced bank auditors.
- Where the board of directors of a bank establishes a committee the mandate should be filed with the regulator.
- Employees and officers should not constitute more than 15% of a bank's board.
- The Bank Act should state the term of reference of the audit committee.
- Internal audit and inspection systems be established.
- **The auditors be expressly required to report annually to the federal regulatory body as to the adequacies of internal controls and inspection.**

Illustration #2 - Savings and Loan Crisis in the U.S.

Hundreds of financial institutions fail in the U.S. causing billions of dollars in losses to investors, depositors and the government.

The "Treadway Commission" is setup by the public accountants, internal auditors, financial executives and two other groups to study the situations and report findings.

Key findings and recommendations included:

Conclusions

- Public companies assume an obligation of public trust and accountability.
- Fraudulent financial reporting causes widespread damage.
- Reducing the risk of fraudulent reporting starts with the company.
- The role of the public accountants can be extended.
- Regulatory law enforcement framework can be enhanced.
- Educators have a role in helping to reduce risk.

The Need for Control Frameworks/Models: Some Background

Illustration #2 - Savings and Loan Crisis in the U.S. (cont'd)

Recommendations

- The "tone at the top" influences the control environment. Management should identify risks and the audit committee should oversee management's progress.
- Sponsoring organizations should develop additional, integrated guidance on internal control. (Note: This recommendation resulted in the COSO committee being formed)
- Audit committees should be composed of independent directors.
- **Management should report on it's responsibility for financial statements and on effectiveness of internal control systems.**
- Generally Accepted Auditing Standards should be changed to better recognize the public accountant's responsibility for fraudulent financial reporting.
- Changes in the business and accounting curricula should improve audit knowledge of the factors that cause fraudulent financial reporting and of strategies leading to a reduction in its incidence.

Prominent companies fail in Britain.

Illustration #3 - Business Failures in Britain

The "Cadbury" Commission is established to study the situation and report findings. The model they finalize on is a slightly modified version of the American COSO framework released previously.

Key findings and recommendations included:

Conclusion

- An effective internal control system is an essential part of the efficient management of a company.

Recommendation

- Directors should report on the effectiveness of a company's system of internal control.

The Need for Control Frameworks/Models: Some Background

Illustration #4 - Governance Concerns in Canada

More financial institutions fail in Canada.

The Criteria of Control Committee better known as the "CoCo" Committee is established by the Canadian Institute of Chartered Accountants to study issues related to internal control and report findings and observations. The final report was released in November of 1995.

Key findings and recommendations of the Committee included:

Findings

- Effective control supports the success of an organization.
- Control comprises those elements an organization including its resources, systems, processes, culture, structure and tasks that taken together support people in the achievement of the organization objectives.
- The responsibility for control exists throughout the organization, at all levels.
- 20 criteria of control are proposed grouped under purpose, commitment, capability, monitoring and learning.
- **People with responsibility for internal control should report to the Board on the status of control.**

The Need for Control Frameworks/Models: Some Background

Illustration #5 - Governance Concerns Emerge Worldwide

Major business failures and governance problems occur in many countries.

Commissions similar to the COSO Commission in the U.S. are established — Cadbury in the U.K., CoCo in Canada, and a number of other countries including South Africa and Australia.

Findings and recommendations of these commissions are similar in many respects to those reported by COSO, Cadbury and CoCo.

The Need for Control Frameworks/Models: Some Illustrations

Illustration #6 – Acceptance of the ISO 9000 and 14000 Quality and Environmental Standards

A set of quality and environmental standards developed by the International Organization for Standardization gains widespread international support based on the idea that the amount of inspection in processes should be reduced and quality should be built in through the use of effective quality processes.

The ISO 9000 series of quality standards is supported by an international organization based in Switzerland. These standards are developed and supported by countries around the world and have gained widespread acceptance and use. The standards are adjusted and improved every four years based on experience gained by users.

These "quality standards" constitute a type of control framework and contain many of the same core ideas included in control models such as COSO, Cadbury and CoCo.

Illustration #7 - Concerns with International Competitiveness

Serious concerns develop in the United States in the early 80's related to the quality of American goods and services.

The President of the United States establishes the Malcolm Baldrige Award based on defined criteria. Organizations are scored on conformance to these criteria out of 1000 possible points.

These "quality criteria" constitute a type of control framework.

The Malcolm Baldrige framework is used by many companies as a control framework for managing customer service and product quality. The Baldrige system had a significant influence on the Canadian control framework (CoCo) and the Paisley Consulting international model, CARD®*model*.

The Need for Control Frameworks/Models: Some Illustrations

Illustration #8 - Concerns with Environmental Stewardship

Industry in Canada is concerned that the government and public do not believe that they are acting responsibly.

The Canadian Standards Association develops a voluntary environmental standards.

These environmental standards constitute a type of control framework.

The core environmental management model developed is very similar to the CoCo control model. This voluntary environmental management framework provides a core model to design, maintain and assess controls related to environmental compliance.

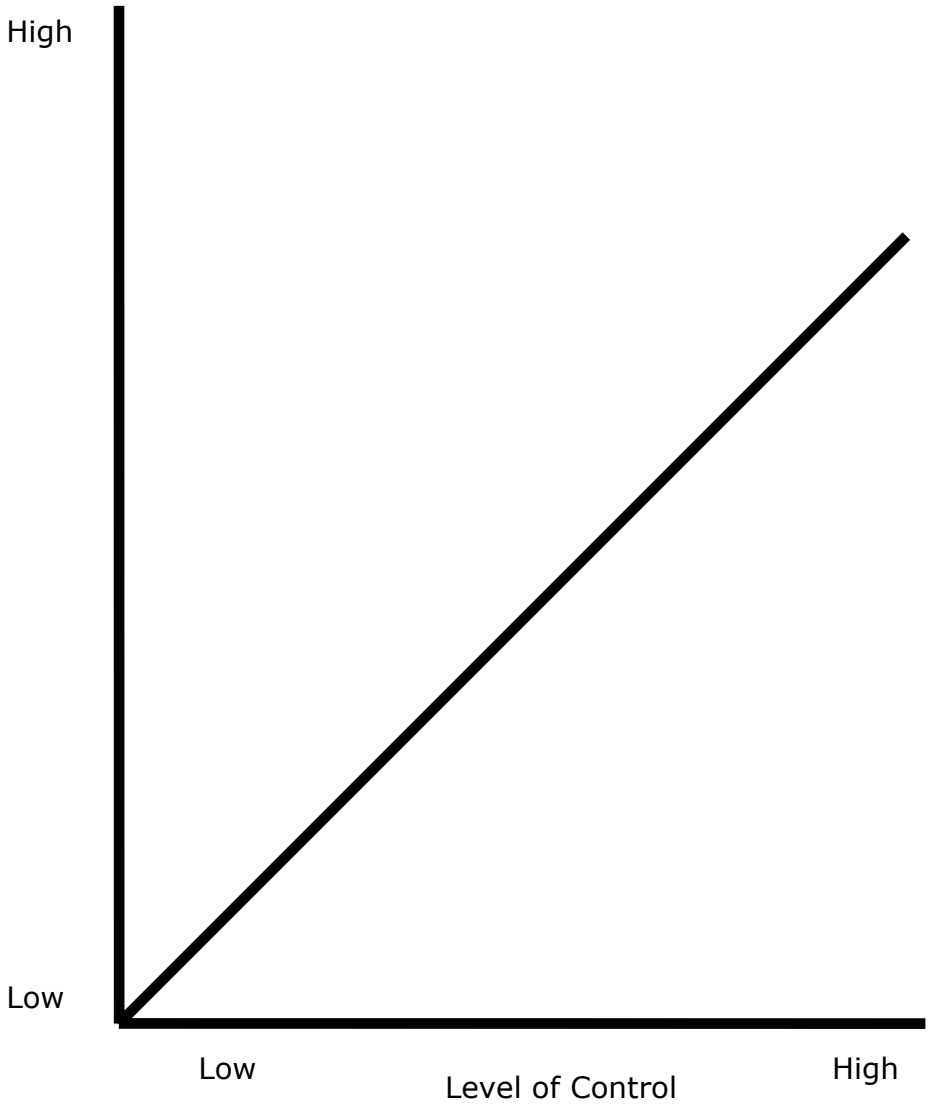
****SUMMARY COMMENT****

Emerging requirements to report on the adequacy or effectiveness of internal control are driving the development of control criteria that can be used to develop representations. Without reasonably specific control criteria, assurance personnel such as internal and external auditors will have great difficulty adding value and forming opinions on the reliability of the representations being made.

CONTROL MODELS - SOME EXAMPLES
THE COMMAND AND CONTROL MODEL

Direct Controls

- System Controls
- Physical Safeguards
- Centralized Decision-Making
- Segregation of Duties
- Supervisory Review

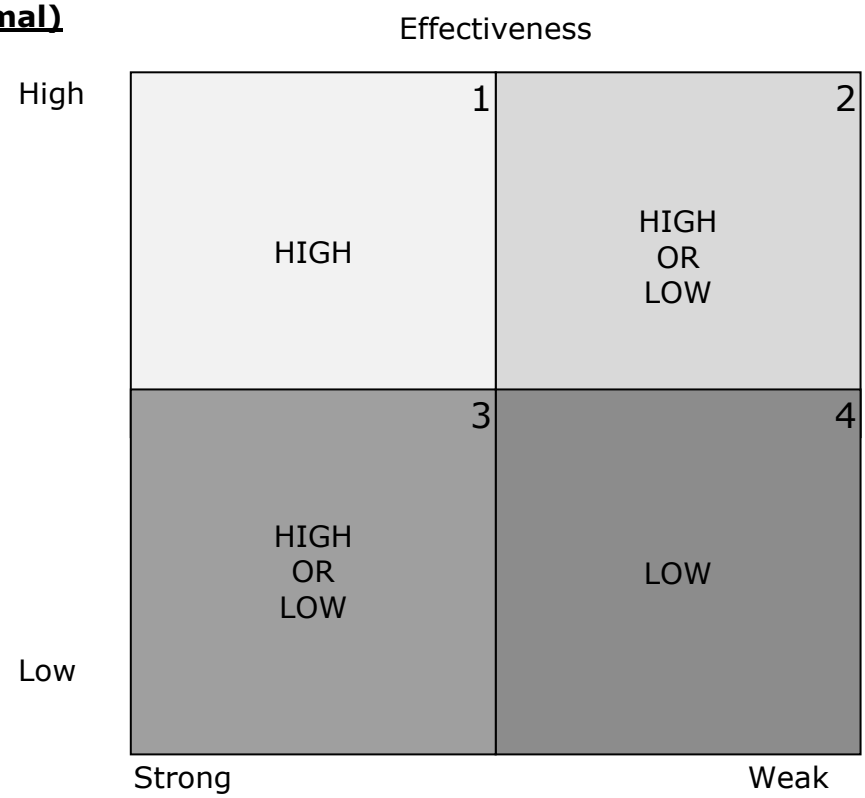


This model shaped the control systems of many large corporations and the audit programs of many internal audit departments. It has come under serious attack over the past ten years as organizations move from Command and Control methods to frameworks based more on empowerment, team work and accountability and its flaws become increasingly apparent .

CONTROL MODELS - SOME EXAMPLES
B.J. WHITE

Control Mechanisms (Formal)

- Policies
- Procedures
- Regulations
- Laws
- Organization Structure
- Bureaucracy
- Restrictive Formal Processes
- Centralized Authority and Decision Making



Control Environment (Informal)

Competence, Trust, Shared Values, Strong Leadership, High Expectations, Clear Accountability, Openness, High Ethical Standards

This model was published in 1980 as part of a study done on U.S. corporations. It was one of the first significant challenges to the core assumptions in the Command and Control framework.

(Source: B.J. White - Internal Control in U.S. Corporation
Financial Executive Research Foundation, New York, 1980)

CONTROL MODEL-SOME EXAMPLES
R.J. ANDERSON DERIVATIVE
USED IN GULF CANADA 1986-87

ORGANIZATIONAL CONTROLS

- Honest and Competent Personnel:
  - Responsibility for Personnel, Training and Employee Relations
  - Hiring Practices
  - Performance Standards
  - Training Programs
  - Supervision
  - Firing practices
  - Systems that Do Not Invite Abuse
  - Evaluation and Promotion Practices
  - Work Environment
- Segregation of Functions
- Overall Plan of Organization
- Accounting/Finance Organization Plan:
  - Specific Control Standards
  - Segregation from Operations
  - Centralization of Reporting Responsibility
  - Segregation of Custodial and Reporting Functions
  - Internal Audit Reporting Lines
  - Interface of A&FC with Management and Operating Departments

SYSTEM DEVELOPMENT AND CHANGE CONTROLS

- Development Controls
- Pre-Installation Controls
- Feasibility and Long-Term Plans

AUTHORIZATION AND REPORTING CONTROLS

- General Authorization, Specific Authorization and Approvals
- Budgets, Responsibility Reporting and Management Information Systems
- Computer Controls Related to Authorization

ACCOUNTING SYSTEMS CONTROLS

- Ensuring Transactions are Recorded Initially
- General Ledger and Chart of Accounts
- Journals, Sub-Ledgers, Balancing Routines
- Document Design
- Cost Accounting

ACCOUNTING SYSTEMS CONTROLS (Cont'd)

- Computer Processing Controls:
  - Master File Controls
  - Data Controls
  - Error Controls
  - Management and Audit Trails

ADDITIONAL SAFEGUARDING CONTROLS

- Restricted Access
- Periodic Count and Comparison
- Protection of Records
- Insurance
- Computer Operations Controls:
  - Prevention or Detection of Accidental Errors
  - Prevention or Detection of Fraudulent Manipulation or Misuse of Data
  - Security Against Destruction of Records and Equipment
  - Disaster and Recovery Contingency Plans

SUPERVISORY CONTROLS

- Management Supervision
- Monitoring of Controls and Detected Errors
- Internal Audit
- External Audit
- Audit Committee

DOCUMENTATION CONTROLS

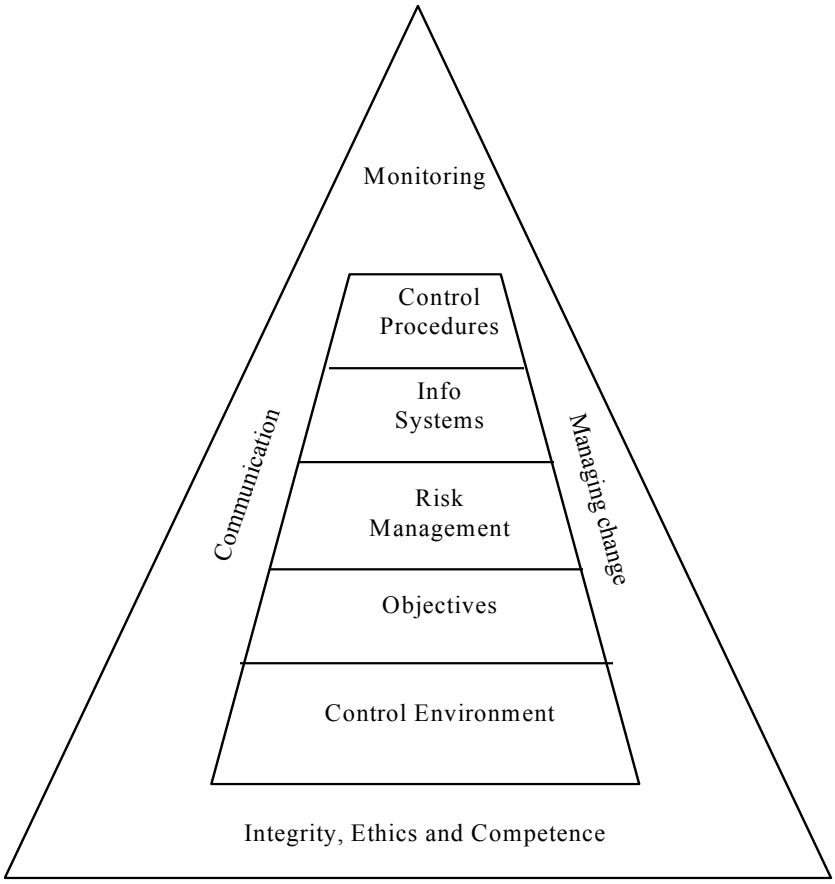
- Manuals of Policies and Procedures
- Systems Documentation
- Program Documentation
- Documentation of Operating Instructions
- Documentation of File Control Procedures
- Documentation of Data Conversion Procedures
- Documentation of Data Base Components
- Documentation of Data Control Procedures
- Documentation of User Procedures

This 1986 framework used in Gulf Canada promoted the role of "Organizational Controls" in an effective control framework. It was derived from a two volume set on external auditing written by R.J. Anderson.

CONTROL MODELS - SOME EXAMPLES

COSO FIRST DRAFT MARCH 1991

The Model



Source: Internal Control - Integrated Framework Exposure Draft March 1991, Committee of Sponsoring Organizations

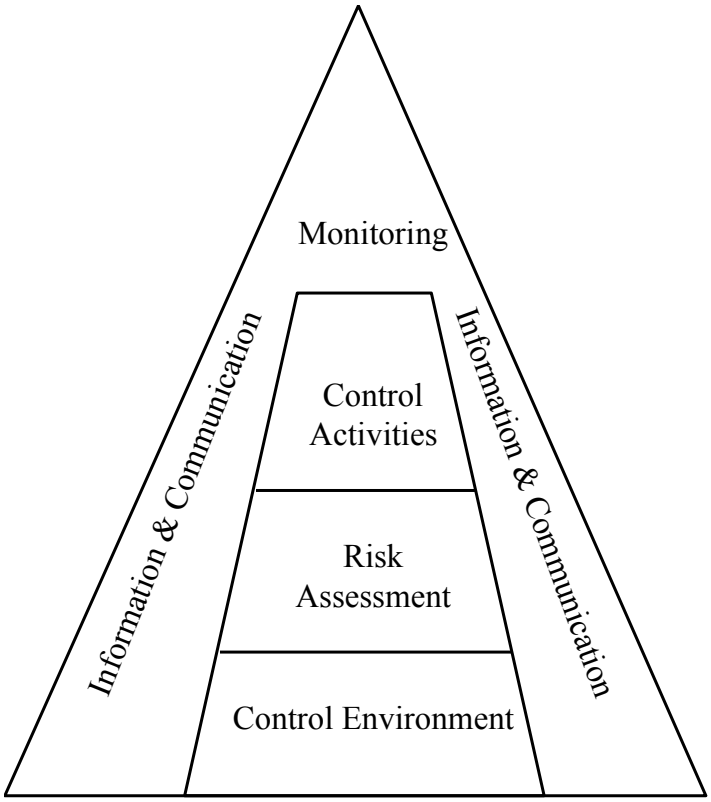
The Definition

Internal Control is the process by which an entity's board of directors, management and/or other personnel obtain reasonable assurance as to achievement of specified objectives; it consists of nine interrelated components, with integrity, ethical values and competence, and the control environment, serving as the foundation for the other components, which are: establishing objectives, risk assessment, information systems, control procedures, communication, managing change, and monitoring.

CONTROL MODELS - SOME EXAMPLES

COSO FINAL SEPTEMBER 1992

The Model



The Definition

Internal control is a process, effected by an entity's board of directors, management and other personnel, designated to provide reasonable assurance regarding the achievement of objectives in the following categories:

- *Effectiveness and efficiency of operations.*
- *Reliability of financial reporting.*
- *Compliance with applicable laws and regulations.*

The control environment provides an atmosphere in which people conduct their activities and carry out their control responsibilities. It services as the foundation for the other components. Within this environment, management assesses risks to the achievement of specified objectives. Control activities are implemented to help ensure that management directives to address the risks are carried out. Meanwhile, relevant information is captured and communicated throughout the organization. The entire process is monitored and modified as conditions warrant.

CONTROL MODELS - SOME EXAMPLES
COSO 1992 (U.S.)

1. CONTROL ENVIRONMENT

- 1.1 Integrity and Ethical Values
- 1.2 Commitment to Competence
- 1.3 Board of Directors/ Audit Committee
- 1.4 Management Philosophy and Operating Style
- 1.5 Organization Structure
- 1.6 Assignment of Authority and Responsibility
- 1.7 Human Resource Policies and Practices

2. RISK ASSESSMENT

- 2.1 Entity-Wide Objectives
- 2.2 Activity-Level Objectives
- 2.3 Risk Identification
- 2.4 Change Management

3. CONTROL ACTIVITIES

- 3.1 Top Level Reviews
- 3.2 Direct Functional or Activity Management
- 3.3 Information Processing
- 3.4 Physical Controls

3. CONTROL ACTIVITIES (CONT'D)

- 3.5 Performance Indicators
- 3.6 Segregation of Duties
- 3.7 Controls Over Information Systems
  - Data Centre
  - Application Development & Maintenance
  - System Software
  - Access Security
  - Application Controls

4. INFORMATION AND COMMUNICATION

- 4.1 Information
- 4.2 Communication

5. MONITORING

- 5.1 Ongoing Monitoring
- 5.2 Separate Evaluations
- 5.3 Reporting Deficiencies

Note: The subpoints noted under each category heading are derived from the narrative in the Framework volume. COSO does not attempt to list specific subelements in the framework but does provide detailed criteria for each category posed as questions.

CONTROL MODELS - SOME EXAMPLES
CADBURY DECEMBER 1994 IN THE U.K.

1. Control environment

- A commitment by directors, management and employees to competence and integrity (e.g. leadership by example, employment criteria).
- Communication of ethical values and control consciousness to managers and employees (e.g. through written codes of conduct, formal standards of discipline, performance appraisal).
- An appropriate organisational structure within which business can be planned, executed, controlled and monitored to achieve the company's/group's objectives.
- Appropriate delegation of authority with accountability which has regard to acceptable levels of risk.
- A professional approach to financial reporting which complies with generally accepted accounting practice.

2. Identification and evaluation of risks and control objectives

- Identification of key business risks in a timely manner.
- Consideration of the likelihood of risks crystallising and the significance of the consequent financial impact on the business.
- Establishment of priorities for the allocation of resources available for control and the setting and communicating of clear control objectives.

3. Information and communication

- Performance indicators which allow management to monitor the key business and financial activities and risks, and the progress towards financial objectives, and to identify developments which require intervention (e.g. forecasts and budgets).
- Information systems which provide ongoing identification and capture of relevant, reliable and up-to-date financial and other information from internal and external sources (e.g. monthly management accounts, including earnings, cashflow and balance sheet reporting).
- Systems which communicate relevant information to the right people at the right frequency and time in a format which exposes significant variances from the budgets and forecasts and allows prompt response.

CONTROL MODELS - SOME EXAMPLES
CADBURY DECEMBER 1994 IN THE U.K.

4. Control procedures

- Procedures to ensure complete and accurate accounting for financial transactions.
- Appropriate authorisation limits for transactions that reasonably limit the company's/group's exposures.
- Procedures to ensure the reliability of data processing and information reports generated.
- Controls that limit exposure to loss of assets/records or to fraud (e.g. physical controls, segregation of duties).
- Routine and surprise checks which provide effective supervision of the control activities.
- Procedures to ensure compliance with laws and regulations that have significant financial implications.

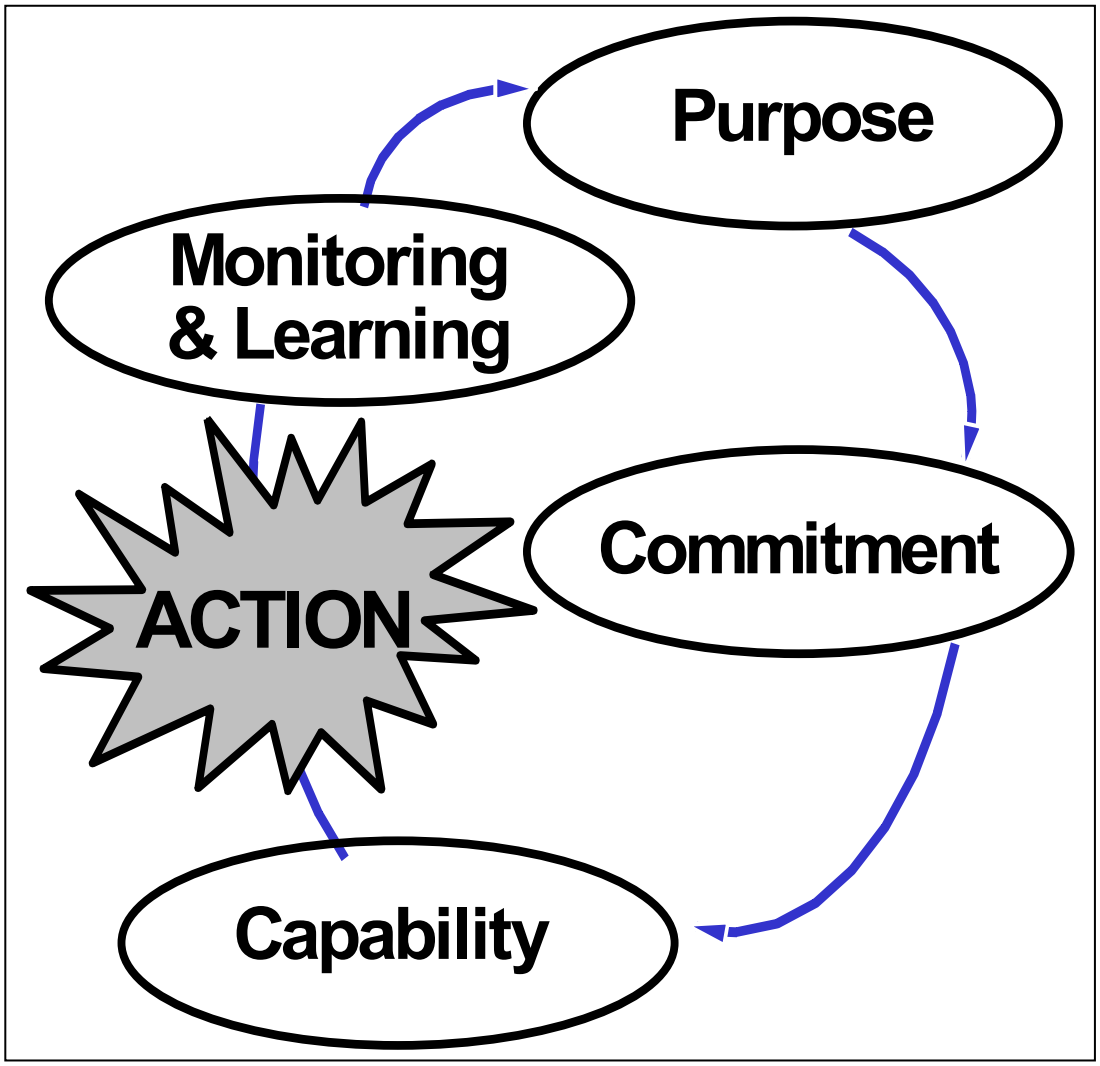
5. Monitoring and corrective action

- A monitoring process which provides reasonable assurance to the board that there are appropriate control procedures in place for all the company's/group's financially significant business activities and that these procedures are being followed (e.g. consideration by the board or board committee of reports from management, from an internal audit function or from independent accountants).
- Identification of change in the business and its environment which may require changes to the system of internal financial control.
- Formal procedures for reporting weaknesses and for ensuring appropriate corrective action.
- The provision of adequate support for public statements by the directors on internal control or internal financial control.

SOURCE: INTERNAL CONTROL AND FINANCIAL REPORTING: GUIDANCE FOR DIRECTORS OF LISTED COMPANIES REGISTERED IN THE U.K. - DECEMBER 1994.

Note: The more detailed framework that supports the structure shown above was included in the October 1993 exposure draft. The more detailed guidance was deleted in the final December 1994 report.

CONTROL MODELS - SOME EXAMPLES
CoCo SEPTEMBER 1995 IN CANADA



CONTROL MODELS- SOME EXAMPLES
CoCo SEPTEMBER 1995 IN CANADA

Exhibit B - The Criteria

PURPOSE

A1 Objectives should be established and communicated.

A2 The significant internal and external risks faced by an organization in the achievement of its objectives should be identified and assessed.

A3 Policies designed to support the achievement of an organization's objectives and the management of its risks should be established, communicated and practised so that people understand what is expected of them and the scope of their freedom to act.

A4 Plans to guide efforts in achieving the organization's objectives should be established and communicated.

A5 Objectives and related plans should include measurable performance targets and indicators.

COMMITMENT

B1 Shared ethical values, including integrity, should be established, communicated and practised throughout the organization.

B2 Human resource policies and practices should be consistent with an organization's ethical values and with the achievement of its objectives.

B3 Authority, responsibility and accountability should be clearly defined and consistent with an organization's objectives so that decisions and actions are taken by the appropriate people.

B4 An atmosphere of mutual trust should be fostered to support the flow of information between people and their effective performance toward achieving the organization's objectives.

CAPABILITY

C1 People should have the necessary knowledge, skills and tools to support the achievement of the organization's objectives.

C2 Communication processes support the organization's values and the achievement of its objectives.

C3 Sufficient and relevant information should be identified and communicated in a timely manner to enable people to perform their assigned responsibilities.

C4 The decisions and actions of different parts of the organization should be coordinated.

C5 Control activities should be designed as an integral part of the organization, taking into consideration its objectives, the risks to their achievement, and the inter-relatedness of control elements.

MONITORING AND LEARNING

D1 External and internal environments should be monitored to obtain information that may signal a need to re-evaluate the organization's objectives or control.

D2 Performance should be monitored against the targets and indicators identified in the organization's objectives and plans.

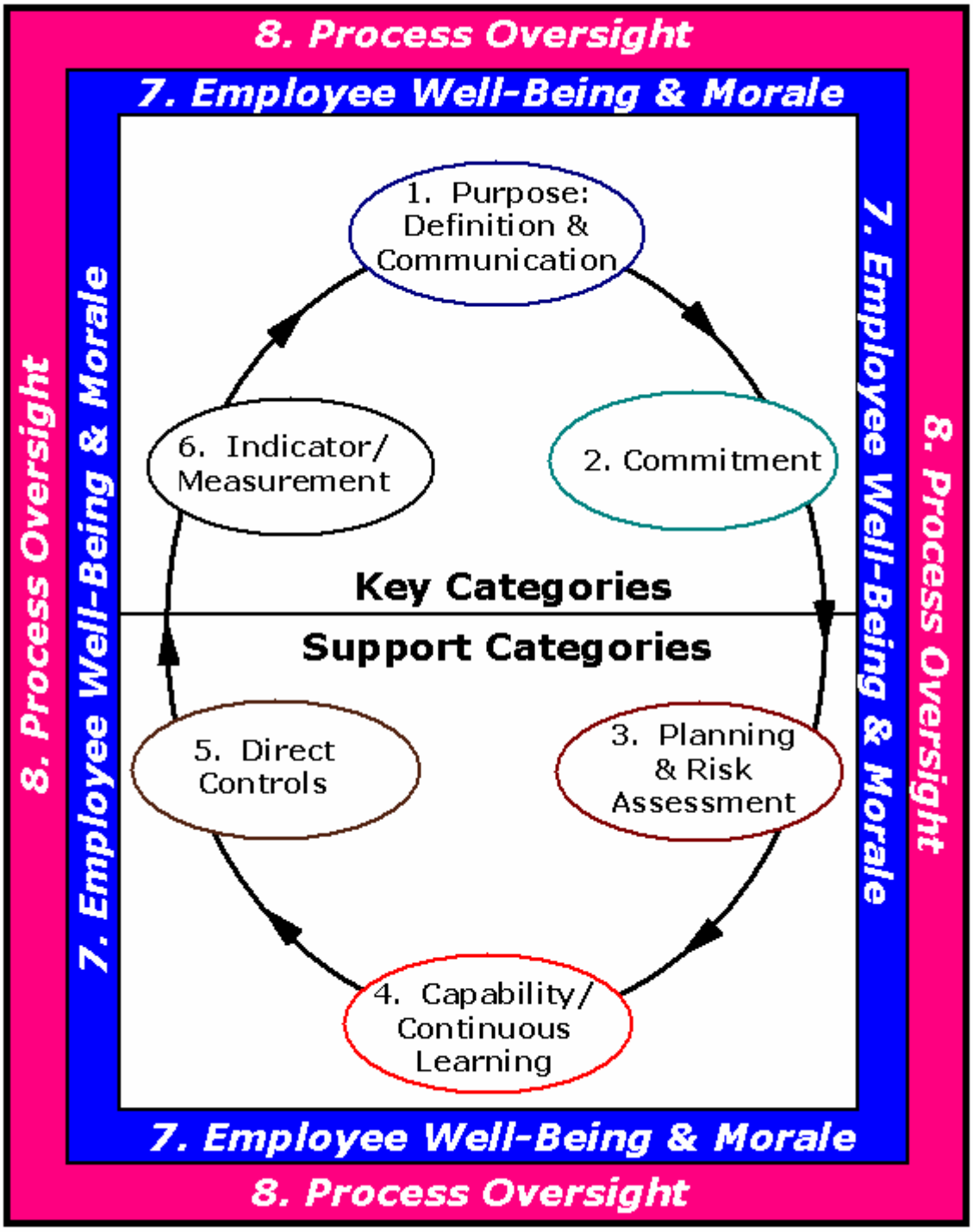
D3 The assumptions behind an organization's objectives and systems should be periodically challenged.

D4 Information needs and related information systems should be reassessed as objectives change or as reporting deficiencies are identified.

D5 Follow-up procedures should be established and performed to ensure appropriate change or action occurs.

D6 Management should periodically assess the effectiveness of control in its organization and communicate the results to those to whom it is accountable.

CONTROL MODELS - SOME EXAMPLES
CARD®*model*



CARD®*model* is a control framework developed by Paisley Consulting (formerly CARD®*decisions* Inc.) over the past decade. CARD®*model* contains all control elements in the major national frameworks (i.e. COSO, CoCo, Cadbury) and is periodically updated based on field experience of users and the findings of relevant research studies.

CONTROL MODELS - SOME EXAMPLES
CARD®*menu*

1. PURPOSE: DEFINITION & COMMUNICATION
1.1 Definition of Corporate Mission & Vision
1.2 Definition of Entity Wide Objectives
1.3 Definition of Unit Level Objectives
1.4 Definition of Activity Level Objectives
1.5 Communication of Business/Quality Objectives
1.6 Definition and Communication of Corporate Conduct Values and Standards

2. COMMITMENT
2.1 Accountability/Responsibility Mechanisms
2.1a Job Descriptions
2.1b Performance Contracts/Evaluation Criteria
2.1c Budgeting/Forecasting Processing
2.1d Written Accountability Acknowledgements
2.1e Other Accountability/Responsibility Mechanisms
2.2 Motivation/Reward/Punishment Mechanisms
2.2a Performance Evaluation System
2.2b Promotion Practices
2.2c Firing and Discipline Practices
2.2d Reward Systems – Monetary
2.2e Reward Systems - Non-Monetary
2.3 Organization Design
2.4 Self-Assessment/Risk Acceptance Processes
2.5 Officer/Board Level Review
2.6 Other Commitment Controls

3. PLANNING & RISK ASSESSMENT
3.1 Strategic Business Analysis
3.2 Short, Medium and Long Range Planning
3.3 Risk Assessment Processes – Macro Level
3.4 Risk Assessment Processes – Micro Level
3.5 Control & Risk Self-Assessment
3.6 Continuous Improvement & Analysis Tools
3.7 Systems Development Methodologies
3.8 Disaster Recovery/Contingency Planning
3.9 Other Planning & Risk Assessment Processes

4. CAPABILITY/CONTINUOUS LEARNING
4.1 Knowledge/Skills Gap Identification and Resolution Tools/Processes
4.2 Self-Assessment Forums & Tools
4.3 Coaching/Training Activities & Processes
4.4 Hiring and Selection Procedures
4.5 Performance Evaluation
4.6 Career Planning Processes
4.7 Firing Practices
4.8 Reference Aids
4.9 Other Training/Education Methods

5. DIRECT CONTROL ACTIVITIES & MECHANISM
5.1 Direct Controls Related to Business Systems
5.2 Physical Safeguarding Mechanisms
5.3 Reconciliations/Comparisons/Edits
5.4 Validity/Existence Tests
5.5 Restricted Access
5.6 Form/Equipment Design
5.7 Segregation of Duties
5.8 Code of Accounts Structure
5.9 Other Direct Control Methods, Procedures, or Things

6. INDICATOR/MEASUREMENT CONTROLS
6.1 Results & Status Reports/Reviews
6.2 Analysis: Statistical/Financial/Competitive
6.3 Self-Assessments/Self-Monitoring
6.4 Benchmarking Tools/Processes
6.5 Customer Survey Tools/Processes
6.6 Automated Monitoring/Reporting Mechanisms & Reports
6.7 Integrity Concerns Reporting Mechanisms
6.8 Employee/Supervisor Observation
6.9 Other Indicator/Measurement Controls

7. EMPLOYEE WELL-BEING & MORALE
7.1 Employee Surveys
7.2 Employee Focus Groups
7.3 Employee Question/Answer Vehicles
7.4 Management Communication Processes
7.5 Personal and Career Planning
7.6 Diversity Training/Recognition
7.7 Equity Analysis Processes
7.8 Measurement Tools/Processes
7.9 Other Well-Being/Morale Processes

8. PROCESS OVERSIGHT
8.1 Manager/Officer Monitoring/Supervision
8.2 Internal Audits
8.3 External Audits
8.4 Specialist Reviews & Audits
8.5 ISO Review/Regulator Inspections
8.6 Audit Committee/Board Oversight
8.7 Self-Assessment Quality Assurance Reviews
8.8 Authority Grids/Structures & Procedures
8.9 Other Process Oversight Activities

CONTROL MODELS - SOME EXAMPLES
ISO 9001

4.1 Management Responsibility
- 4.1.1 Quality Policy
- 4.1.2 Organization
  - 4.1.2.1 Responsibility and Authority
  - 4.1.2.2 Resources
  - 4.1.2.3 Management Representative
- 4.1.3 Management Review

4.2 Quality Systems
- 4.2.1 General
- 4.2.2 Quality System Procedures
- 4.2.3 Quality Planning

4.3 Contract Review
- 4.3.1 General
- 4.3.2 Review
- 4.3.3 Amendment to Contract
- 4.3.4 Records

4.4 Design Control
- 4.4.1 General
- 4.4.2 Design and Development Planning
- 4.4.3 Organizational and Technical Interfaces
- 4.4.4 Design Input
- 4.4.5 Design Review
- 4.4.6 Design Output
- 4.4.7 Design Verification
- 4.4.8 Design Validation
- 4.4.9 Design Changes

CONTROL MODELS - SOME EXAMPLES
ISO 9001 (Cont'd)

4.5 Document and Data Control
- 4.5.1 General
- 4.5.2 Document Approval and Issue
- 4.5.3 Document Changes

4.6 Purchasing
- 4.6.1 General
- 4.6.2 Evaluation of Sub-contractors
- 4.6.3 Purchasing Data
- 4.6.4 Verification of Purchased Product
  - 4.6.4.1 Supplier Verification at Sub-contractors
  - 4.6.4.2 Customer Verification of Sub-contracted Product

4.7 Control of Customer Supplied Product

4.8 Product Identification and Traceability

4.9 Process Control

4.10 Inspection and Testing
- 4.10.1 General
- 4.10.2 Receiving Inspection and Testing
- 4.10.3 In-Process Inspection and Testing
- 4.10.4 Final Inspection and Testing
- 4.10.5 Inspection and Test Records

4.11 Control of Inspection, Measuring and Test Equipment
- 4.11.1 General
- 4.11.2 Control Procedures

4.12 Inspection and Test Status

CONTROL MODELS - SOME EXAMPLES
ISO 9001 (Cont'd)

4.13 Control of Nonconforming Product
- 4.13.1 General
- 4.13.2 Nonconforming Product Review and Disposition

4.14 Corrective and Preventive Action
- 4.14.1 General
- 4.14.2 Corrective Action
- 4.14.3 Preventive Action

4.15 Handling, Storage, Packaging, Preservation and Delivery
- 4.15.1 General
- 4.15.2 Handling
- 4.15.3 Storage
- 4.15.4 Packaging
- 4.15.5 Preservation
- 4.15.6 Delivery

4.16 Control of Quality Records

4.17 Internal Quality Audits

4.18 Training

4.19 Servicing

4.20 Statistical Techniques
- 4.20.1 Identification of Need
- 4.20.2 Procedures

SOURCE: *ISO 9000, International Standards for Quality Management, 4th Edition*

CONTROL MODELS - SOME EXAMPLES
MALCOLM BALDRIGE 2003
CRITERIA FOR PERFORMANCE EXCELLENCE

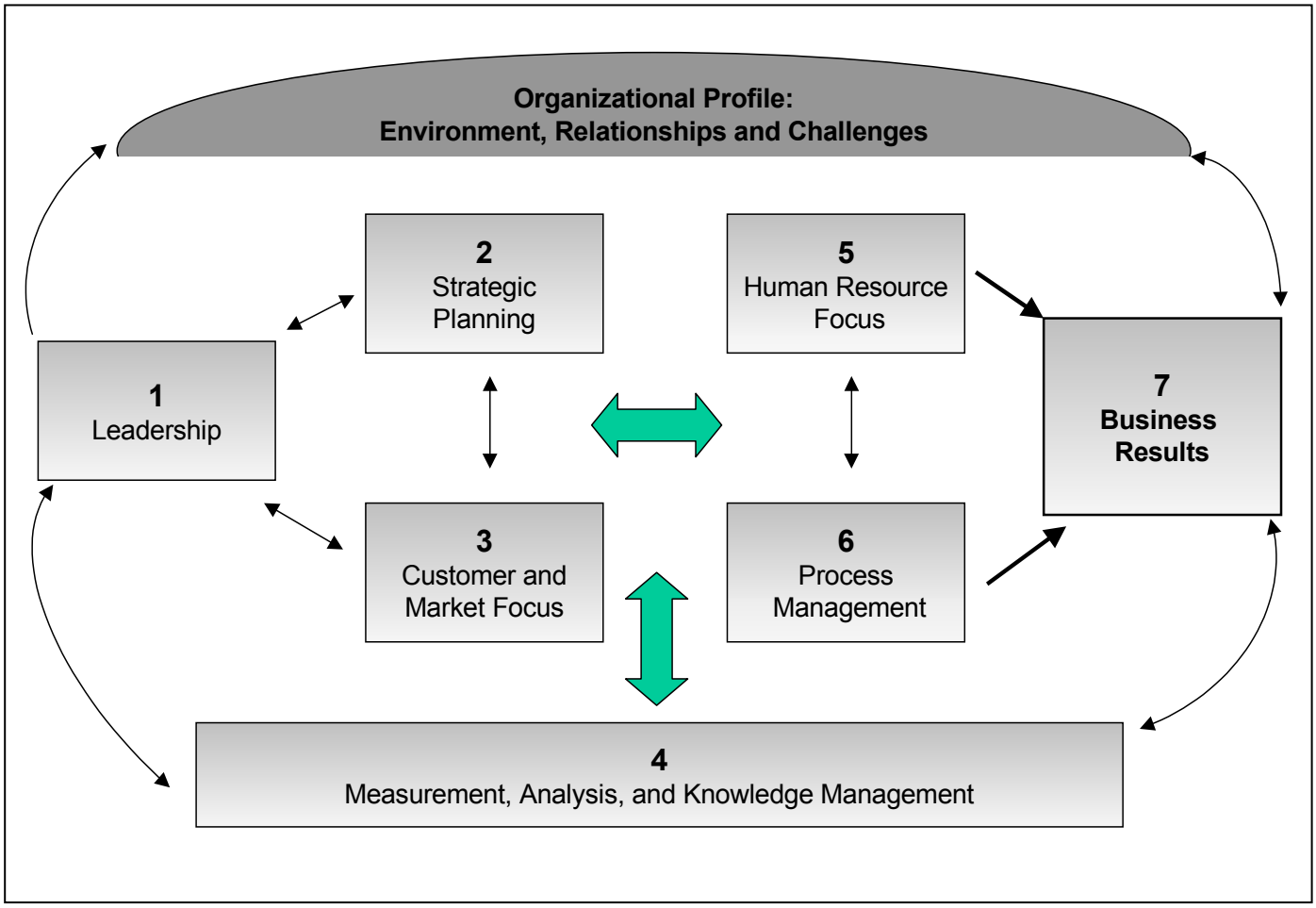
2003 Categories/Items		Point Values
1	**LEADERSHIP**	**120**
1.1	Organizational Leadership	70
1.2	Social Responsibility	50
2	**STRATEGIC PLANNING**	**85**
2.1	Strategy Development	40
2.2	Strategy Deployment	45
3	**CUSTOMER AND MARKET FOCUS**	**85**
3.1	Customer and Market Knowledge	40
3.2	Customer Relationships and Satisfaction	45
4	**MEASUREMENT, ANALYSIS AND KNOWLEDGE MANAGEMENT**	**90**
4.1	Measurement and Analysis of Organizational Performance	45
4.2	Information and Knowledge Management	45
5	**HUMAN RESOURCE FOCUS**	**85**
5.1	Work Systems	35
5.2	Employee Learning and Motivation	25
5.3	Employee Well-Being and Satisfaction	25

MALCOLM BALDRIGE 2003
CRITERIA FOR PERFORMANCE EXCELLENCE

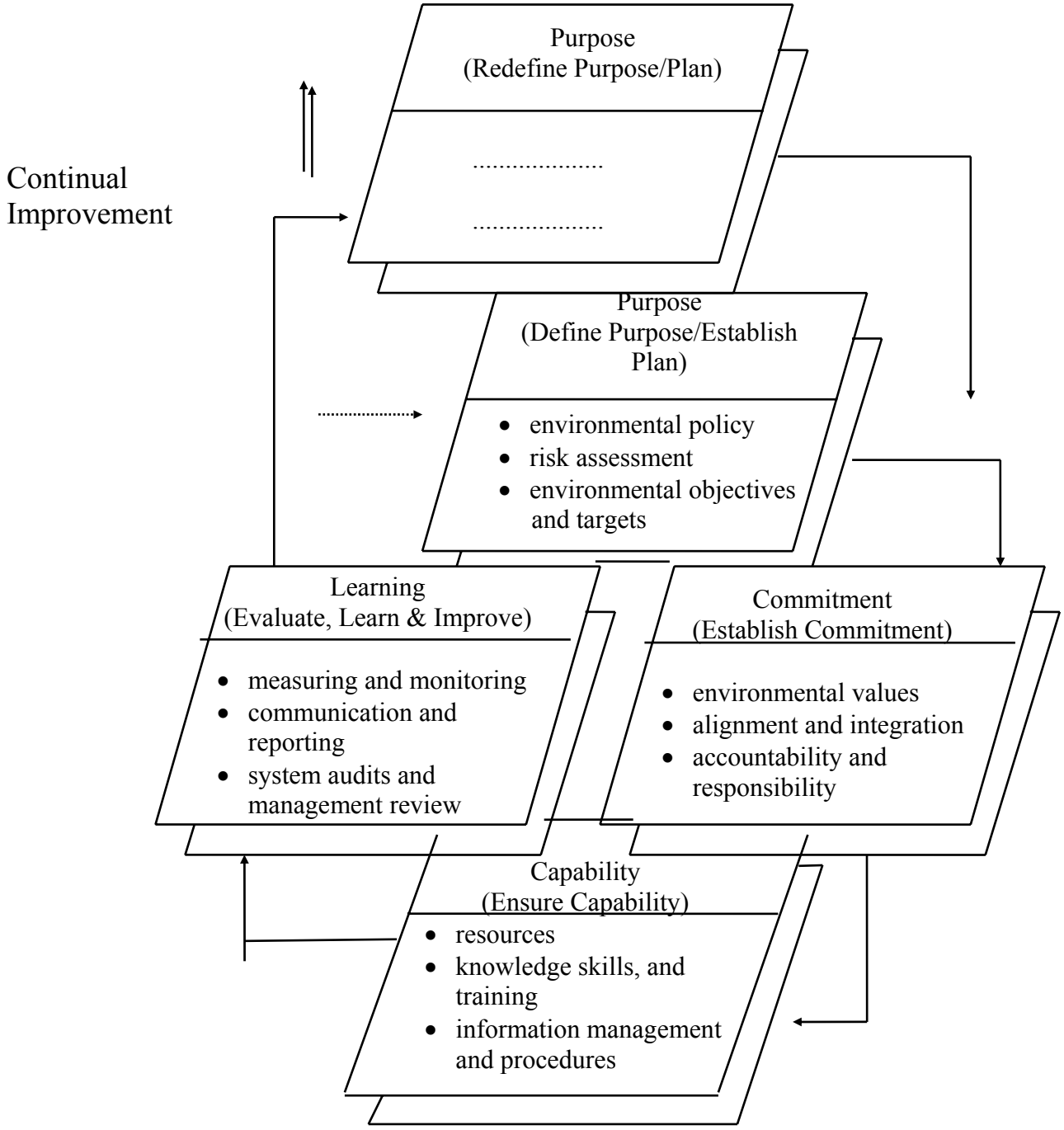
2003	Categories/Items	Point Values
6	**PROCESS MANAGEMENT**	**85**
6.1	Value Creation Processes	50
6.2	Support Processes	35
7	**BUSINESS RESULTS**	**450**
7.1	Customer-Focused Results	75
7.2	Product and Service Results	75
7.3	Financial and Market Results	75
7.4	Human Resource Results	75
7.5	Organizational Effectiveness Results	75
7.6	Governance and Social Responsibility Results	75
	TOTAL POINTS	**1,000**

CONTROL MODELS – SOME EXAMPLES
MALCOLM BALDRIGE 2003

CRITERIA FOR PERFORMANCE EXCELLENCE FRAMEWORK: A SYSTEMS PERSPECTIVE



CONTROL MODELS - SOME EXAMPLES
CANADIAN STANDARDS ASSOCIATION – ENVIRONMENTAL MANAGEMENT FRAMEWORK



CONTROL MODELS - SOME EXAMPLES
A RISK MANAGEMENT VIEW

10 Most Significant Flaws Causing Non Achievement of Objectives

1. Lack of management commitment.
2. Failure to assign responsibility.
3. Failure to establish program objectives.
4. Misunderstanding the role of specialist groups.
5. Lack of supervisory involvement.
6. Failure to involve all employees.
7. Non-existent or inadequate training.
8. Inconsistent enforcement of rules.
9. Poor follow-up.
10. Lack of a total system.

SOURCE: *Loss Control Programs – The 10 Most Significant Flaws, Risk Management magazine, June 1993.*

Which Control Model(s) Is/Are Best For Your Organization?

The key question that must be answered first is:

BEST FOR WHAT?

Best as:

A business process/framework improvement tool?

A training tool?

A communication tool?

An accurate predictor of the future?

A helpful tool to understand the past?

A way of judging whether a particular status or situation is good/bad, adequate/inadequate?

A yardstick that a stakeholder can use to judge the likelihood outputs or outcomes will comply with "fitness for use" "conformance to requirements standards"?

An action determination guide for regulators?

A tool to assist work units to self-assess and report?

A tool to manage risks?

A tool to drive down the cost of control?

A tool to help for Boards and officer groups discharge their responsibilities?

Which Control Model(s) Is/Are Best For Your Organization?

CONCLUSIONS:

CONTROL AND QUALITY MODELS SHOULD BE VIEWED AS TOOLS.

JUDGING WHICH ONE IS BEST SHOULD ONLY BE ATTEMPTED WHEN THE APPLICATION THAT THE TOOL IS TO BE USED FOR IS CLEARLY DEFINED AND UNDERSTOOD.

EVEN WHEN THE PURPOSE OF THE TOOL IS CLEARLY DEFINED, RIGOROUS STEPS SHOULD BE TAKEN TO OBJECTIVELY COMPARE WHICH MODEL(S) OR FRAMEWORK(S) BEST MEETS OR FULFILLS THE DEFINED PURPOSES OR NEEDS.

AUTHORS OF CONTROL MODELS SHOULD STATE VERY CLEARLY WHAT SPECIFIC END RESULTS THEIR MODEL CAN BE USED FOR OR APPLIED TO.

Control Frameworks: Who Needs Them and Why?

REQUIRED: (1) In your groups list below reasons, if any, that justify society spending significant time, money, and energy developing control frameworks.

(2) List applications or uses that your group sees, if any, for integrated control models.

REASONS FOR DEVELOPING CONTROL FRAMEWORKS

1. _____
   _____

2. _____
   _____

3. _____
   _____

4. _____
   _____

5. _____
   _____

Control Frameworks: Who Needs Them and Why?

REQUIRED: (1) In your groups list below reasons, if any, that justify society spending significant time, money, and energy developing control frameworks.

(2) List applications or uses that your group sees, if any, for integrated control models.

APPLICATIONS FOR CONTROL FRAMEWORKS

1. _____
   _____

2. _____
   _____

3. _____
   _____

4. _____
   _____

5. _____
   _____

Which Control Model(s) Is/Are Best For Your Organization?

REQUIRED: This section contains skeleton outlines of 12 control/quality management evaluation guides selected for consideration/study in this course.

The evaluation frameworks covered include:

1. Command & Control 1900s
2. B.J. White 1980
3. R.J. Anderson Derivative 1986
4. U.S. - COSO Framework 1991
5. U.S. - COSO Framework 1992
6. U.K. - Cadbury 1994
7. Canada - CoCo 1995
8. CARD®*model* 1999
9. ISO 9001 1993
10. Malcolm Baldrige 2001
11. CSA Voluntary Environmental Framework 1994

You will be assigned one or more of the models to review and analyze.

In your groups list the strengths and weaknesses you perceive in the model or framework your group has been assigned.

Examples of evaluation criteria that you could include when analyzing the assigned control models include:

1. Tool to report on control and risk status to senior management and Boards.

2. Tool to communicate and discuss control and risk concepts and status with employees at all levels including front line staff.

3. Tool to provide training on control and risk concepts to work units, management, boards of directors and control specialists to increase their skill levels in the areas of control and risk management.

4. Tool to increase the motivation of work units to play a greater role in formalized control/risk analysis.

5. Ability to integrate with quality models such as ISO 9000, Malcolm Baldrige, European Foundation for Quality Management, etc.

6. Ability to help work units optimize the balance between controls and acceptable levels of residual risk.

7. Ability to integrate with risk financing and risk transfer activities including insurance strategies.

8. Ability to support control design and systems development activities.

9. Amount of research done to validate the predictive ability of the model (i.e. research to confirm that conformance to the model does result in greater probability of achieving business objectives vs. non conformance to the model).

10. Ability to integrate the concepts in the control framework to those used to reengineer organizations and/or business units to increase effectiveness and/or reduce costs.

11. Ability to help auditors perform better, more value added direct report audits and minimize non productive conflict.

12. Ability to act as generally accepted criteria for purposes of reporting on control and to assist auditors engaged to form opinions on control/risk status representations.

Which Control Model(s) Is/Are Best For Your Organization?

Control and Quality Framework Reviewed: _____

Strengths	**Weaknesses**

Which Control Model(s) Is/Are Best For Your Organization?

Control and Quality Framework Reviewed: _____

Strengths	**Weaknesses**

Which Control Model(s) Is/Are Best For Your Organization?

Control and Quality Framework Reviewed: _____

Strengths	**Weaknesses**

Which Control Model(s) Is/Are Best For Your Organization?

Control and Quality Framework Reviewed: _____

Strengths	**Weaknesses**

Which Control Model(s) Is/Are Best For Your Organization?

Control and Quality Framework Reviewed: _____

Strengths	**Weaknesses**

Which Control Model(s) Is/Are Best For Your Organization?

Control and Quality Framework Reviewed: _____

Strengths	**Weaknesses**

EVOLUTION OF GENERALLY ACCEPTED RISK CRITERIA "GARC"

Section Objectives:

Introduce participants to developments and trends in the field of risk assessment and risk management. This knowledge will assist participants to assess the approaches available and select the right approach to risk identification, assessment and monitoring for use in their organization.

GENERAL INTRODUCTION

A wide range of approaches have evolved to identify and assess the risks that individuals and organizations face in their daily lives. Some of the risk assessment approaches that have evolved are specific to a topic or industry (e.g. safety, environment, financial derivatives, loss control in retail). Other approaches have attempted to provide generic guidance on how to consider and assess risk in a way that can be applied to a wide range of applications. Work is accelerating around the world to develop new and better ways to assess and manage risks of all types.

RISK MODELS

EXAMPLE 1 – CAUSE OF FAILURE APPROACH

Loss control specialists have devoted significant effort to analyzing and understanding why problems occur. A study completed by Kemper Risk Management Services division identified the following 10 most significant flaws in risk management systems:

1. Lack of management commitment
2. Failure to assign responsibility
3. Failure to establish program objectives
4. Misunderstanding the role of specialist staff groups
5. Lack of supervisory involvement
6. Failure to involve all employees
7. Non existent or inadequate training
8. Inconsistent enforcement of rules
9. Poor follow-up
10. Lack of a total system

SOURCE: *Kemper Risk Management, Risk Management, June 1993*

This approach can be viewed as an attempt to predict the most statistically predictable root cause of control failures.

EXAMPLE 2 – SOURCES OF RISK

In 1995 Australia/New Zealand published a standard on the topic of Risk Management. The standard proposed an 8 category framework to consider sources of risk. The categories proposed include:

1. Commercial and legal relationships
2. Economic
3. Human behaviour
4. Natural events
5. Political circumstances
6. Technology, technical issues
7. Management activities and controls
8. Individual activities

Risk is defined in the Australia/New Zealand Standard as:

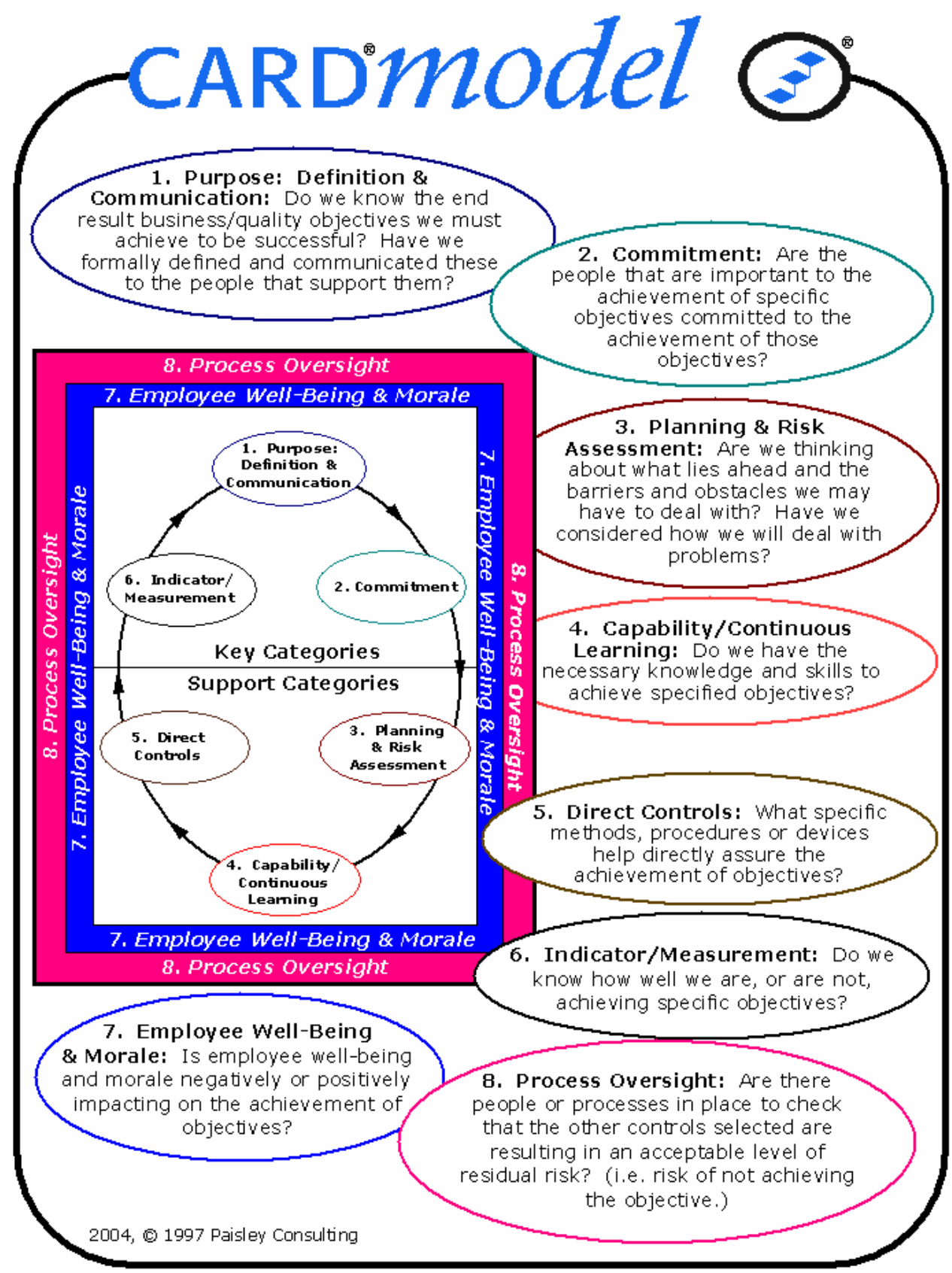
"*the chance of something happening that will have an impact upon objective. It is measured in terms of consequences and likelihood."*

SOURCE: *Australia/New Zealand Standard, Risk Management, November 1995*

EXAMPLE 3 – SOURCE OF RISK - CONTROL DESIGN

Risk can be defined as an event or action that does, or could, threaten the achievement of an organization's objectives. Controls can be defined as methods, procedures, equipment or other things that provide additional assurance that relevant business/quality objectives will be achieved. In other words, controls mitigate risks. If the control design is missing key elements, it becomes a source of risk.

Using this approach, a risk might be "people don't know how to deal with a particular situation or event". In this case if we use the CARD®*model* approach to control categorization the risk is rooted in Control Category 4 – Capability. Another example might be "people don't care". This would be an example of a risk that can be traced to CARD®*model* Control Category 2 – Commitment.



EXAMPLE 4 – CATEGORIES OF RISK

In 1995 the Economist Intelligence Unit published a study co-authored by Arthur Andersen titled "Managing Business Risk – An Integrated Approach". This study proposed a framework to consider various types or categories of risk. The framework included the following elements:

I Environment Risk

II Process Risk

- Operations Risk
- Empowerment Risk
- Information Processing/Technology Risk
- Integrity Risk
- Financial Risk

III Information for Decision Making Risk

- Operational
- Financial
- Strategic

SOURCE: *Managing Business Risk, Economist Intelligence Unit, 1995.*

This approach uses the various risk categories as a tool to identify all of the possible relevant risks an organization faces.

EXAMPLE 5 – SOURCE AND AREAS OF EFFECT

The Australian government in October of 1996 published a document titled "Guidelines for Managing Risk in the Australian Public Service".

This study proposed two approaches to identifying and considering risks:

Possible Sources of Risk

- commercial/legal relationships
- economic
- socio-political/legal
- personnel/human behaviour
- financial/market
- management activities and controls
- technology/technical
- the activity itself/operational
- business interruptions
- occupational health and safety
- property/assets
- security
- natural events
- public/professional/product
- liability

Possible Areas of Risk Effect

- asset and resource base
- cost: both direct and indirect
- people
- community
- performance of activities: how well the activity is performed
- timeliness of activities
- organizational behaviour
- environment
- intangibles

SOURCE: *Guidelines for Managing Risk in the Australian Public Sector, #22 October 1996*

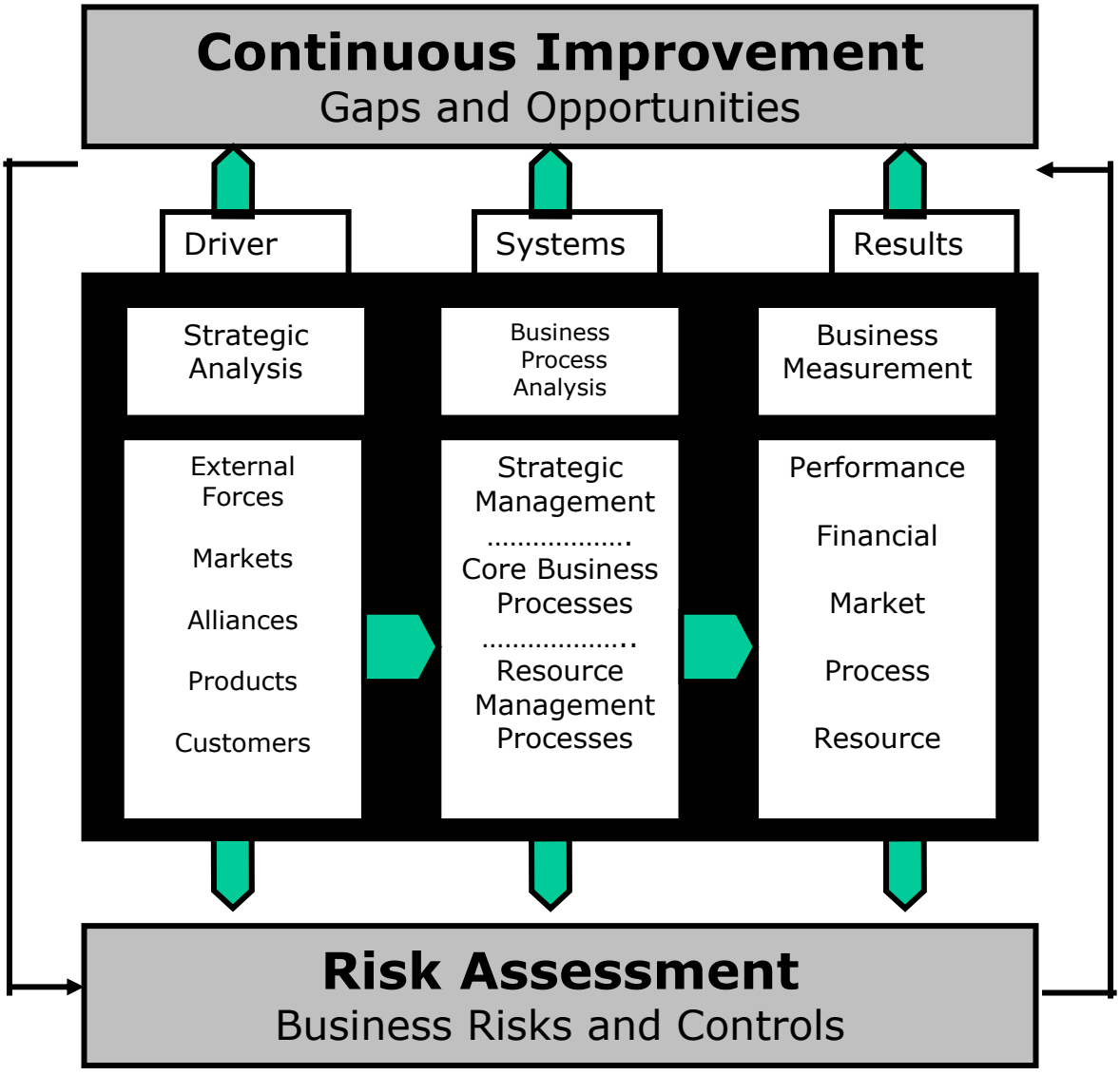
The guidelines propose a matrix to determine risk levels using likelihood and consequences.

Consequences					
Likelihood	extreme	very high	medium	low	negligible
almost certain	severe	severe	high	major	significant
likely	severe	high	major	significant	moderate
moderate	high	major	significant	moderate	low
unlikely	major	significant	moderate	low	trivial
rare	significant	moderate	low	trivial	trivial
SOURCE: *Guidelines for Managing Risk in the Australian Public Sector, #22 October 1996*					

EXAMPLE 6 – ENTITY WIDE RISK MONITORING

KPMG, in a 1997 publication titled "Auditing Organizations Through a Strategic System Lens", proposes a multi-faceted approach to auditing and risk assessment. An overview of the KPMG approach is shown below:

Exhibit 4
The KPMG Business Measurement Process



SOURCE: *Bell, Marrs, Soloman, Thomas. Auditing Organizations Through A Strategic*

EXAMPLE 7 – AREAS OF OBJECTIVE CATEGORIES AT RISK

The Conference Board of Canada in a study titled "A Conceptual Framework for Integrated Risk Management" proposes a broad definition of risk:

> *"events or activities that can effect an organization and the achievement of its goals."*

The Economist Intelligence Unit in Managing Business Risk: An Integrated Approach defines Business Risk as:

> *"the threat that an event or action will adversely affect an organization's ability to achieve its business objectives and execute its strategies successfully."*

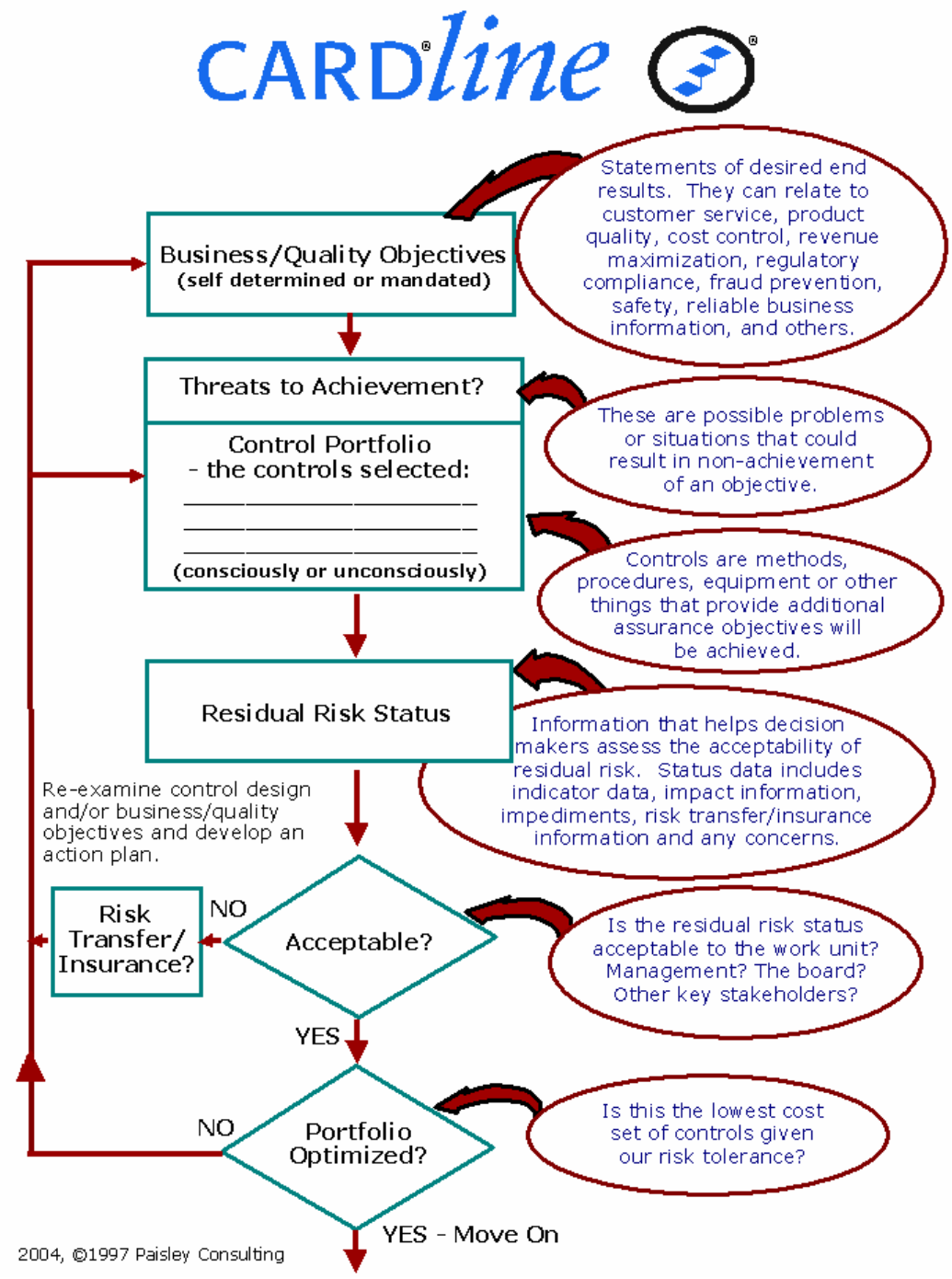
Since risk is generally considered to be threats to the achievement of objectives, one approach to considering risk is to classify the categories or types of objectives that risks relate to, or impact on. Paisley Consulting has categorized the different families of business objectives as follows:

1. Product Quality
2. Customer Service
3. Minimizing Unnecessary Costs
4. Revenue/Profit Maximization
5. Reliable Business Information
6. Asset Safeguarding
7. Safety
8. Regulatory Compliance
9. Fraud Prevention/Detection
10. Continuity of Operations
11. Unintentional Risk Exposure
12. Internal Compliance

Risks threaten the achievement of objectives that can fall into any of these categories. The categories can be adjusted to accommodate a range of organizations including non-for-profit and public sector.

EXAMPLE 8 – FOCUS ON THREATS TO ACHIEVEMENT AND RESIDUAL RISK STATUS

Paisley Consulting (formerly CARD®*decisions*) has pioneered an approach to considering risk by focusing on possible threats to all business/quality objectives collectively and/or information assists decision makers assess the acceptability of the current residual risk status. The core elements of this approach are shown in the diagram below:



Using the CARD®*line* approach risk is analyzed by focusing the attention of decision makers on threats to achievement of objectives and the current residual risk status including the following information:

Indicator Data - Any information know about how effective the current control choices are with respect to the stated business/quality objective.

Impact Data - How bad would it be if the objective was not met in whole or in part? How would the organization, the officers, the staff, be impacted?

Impediment Data - Any situations or problems that stand in the way of the group or a group member adjusting the control element portfolio. These can relate to lack of funds, cooperation of staff members or other departments, training deficiencies, senior management attitudes, and others.

Concern Data - Any known or suspected problems or issues related to the business/quality objective being assessed. This data is useful in assessing the likelihood of non-achievement given the controls in use or in place. This is referred to as Residual Likelihood or the likelihood of non-achievement after considering the current control portfolio.

Risk Transfer/Insurance - Any information on risk financing or transfer mechanisms in place that relate to the objective being analyzed. Significant exceptions, deductible ceilings and other pertinent information are included under this heading.

Residual risk status information assists decision makers decide whether to increase or decrease efforts and spending to mitigate the various threats to the achievement of a specific business/quality objective or leave things as they are until new information emerges or additional analysis is completed and re-evaluated.

GROUP EXERCISE:

Analyze the strengths and weaknesses of the risk approach your workshop leader assigns to your group.

APPROACH
STRENGTHS **1.** **2.** **3.** **4.** **5.** **6.** **7.** **8.**
WEAKNESSES **1.** **2.** **3.** **4.** **5.** **6.** **7.** **8.**

APPROACH
STRENGTHS **1.** **2.** **3.** **4.** **5.** **6.** **7.** **8.**
WEAKNESSES **1.** **2.** **3.** **4.** **5.** **6.** **7.** **8.**

APPROACH
STRENGTHS **1.** **2.** **3.** **4.** **5.** **6.** **7.** **8.**
WEAKNESSES **1.** **2.** **3.** **4.** **5.** **6.** **7.** **8.**

APPROACH
STRENGTHS **1.** **2.** **3.** **4.** **5.** **6.** **7.** **8.**
WEAKNESSES **1.** **2.** **3.** **4.** **5.** **6.** **7.** **8.**

APPROACH
STRENGTHS **1.** **2.** **3.** **4.** **5.** **6.** **7.** **8.**
WEAKNESSES **1.** **2.** **3.** **4.** **5.** **6.** **7.** **8.**

CARD®MODEL/CARD®MENU ELEMENT DEFINITIONS

CONTROL ASSURANCE & RISK DESIGN MENU TRIGGER QUESTIONS

1.0 PURPOSE: DEFINITION & COMMUNICATION

Primary Category Definition: Do we know the end result business/quality objectives we must achieve to be successful? Have we formally defined and communicated these to the people that support them?

1.1 Definition of Corporate Mission & Vision

Has the organization defined its primary reason for existence? Does the organization have a documented mission and/or vision statement?

1.2 Definition of Entity Wide Objectives

Has the organization defined the business/quality objectives that it needs to accomplish? Do they include objectives related to customer service, product quality, cost control, revenue generation, fraud prevention, reliable business information, legal compliance, and others?

1.3 Definition of Unit Level Objectives

Are end result business/quality objectives defined for each business unit or team? Are these linked to the objectives defined in elements 1.1 and 1.2? Is there a process to check that unit and activity level objectives support corporate level objectives?

1.4 Definition of Activity Level Objectives

Are end result business/quality objectives clearly defined for, or linked to, all activities being carried out in the business units? Do people know what they are expected to do, and more importantly, why they are doing these activities?

1.5 Communication of Business/Quality Objectives

Have end result business/quality objectives been communicated to all the people that must support the achievement of those objectives? Do they understand what the objectives mean?

1.6 Definition and Communication of Corporate Conduct Values and Standards

Specifically in the area of objectives related to corporate conduct and ethics, has the organization communicated its values and standards to employees, suppliers, customers and other relevant stakeholders? Is there a process to update and communicate these standards regularly?

2.0 COMMITMENT

Primary Category Definition: Are the people that are important to the achievement of specific objectives committed to the achievement of those objectives?

2.1 Accountability/Responsibility Mechanisms

Has the organization or unit defined and assigned accountability for achieving business/quality objectives? (Note: it is important to distinguish between assigning accountability for completion of activities or processes versus defining accountability for end result business/quality objectives).

2.1a Job Descriptions

Do employees know through job descriptions or other documentation the specific business/quality objectives their daily work supports?

2.1b Performance Contracts/Evaluation Criteria

Are performance contracts or other forms of employee evaluation criteria linked to specific business/quality objectives? (i.e. is performance evaluation linked to specific end result business/quality objectives?)

2.1c Budgeting/Forecasting Processing

Does the budget and forecasting process link the achievement of objectives to specific business units and/or individuals?

2.1d Written Accountability Acknowledgements

Have employees been asked to formally acknowledge in some way that they accept responsibility for one or more business/quality objectives?

2.1e Other Accountability/Responsibility Mechanisms

Are there any other mechanisms, which establish accountability for specific business/quality objectives?

2.2 Motivation/Reward/Punishment Mechanisms

Are there personal consequences related to the accomplishment or non-accomplishment of specific business/quality objectives?

2.2a Performance Evaluation System

Are there clear linkages between publicized business/quality objectives and the employee performance evaluation system(s) in use?

2.2b Promotion Practices
Is there linkage between the organization's stated objectives and the performance of those that are being promoted or demoted?

2.2c Firing and Discipline Practices
Are there negative consequences attached to lack of commitment to business/quality objectives up to and including firing of those responsible for supporting the achievement of those objectives?

2.2d Reward Systems - Monetary
Is there visible linkage between the accomplishment of specific objectives and the monetary rewards provided by the organization?

2.2e Reward Systems - Non-Monetary
Are there any non-monetary techniques or methods that provide positive consequences for achievement of business/quality objectives, or negative consequences for the non-achievement of the objectives? (eg. employee or team awards, special recognition, plaques, posters showing units that are not meeting targets, etc.)

2.3 Organization Design
Does the design of the organization and sub units assist in clarifying who is responsible and/or accountable for specific business/quality objectives?

2.4 Self-Assessment/Risk Acceptance Processes
Do work units engage in self-assessment processes which assist in clarifying and/or reinforcing ownership of business/quality objectives?

2.5 Officer/Board Level Review
Does senior management and/or the board of directors ask for information and reports on specific business/quality objectives and/or the adequacy of the systems and processes that support the achievement of those objectives?

2.6 Other Commitment Controls
Are there any other mechanisms in use or place which increase the commitment of employees to achieve business/quality objectives?

3.0 PLANNING & RISK ASSESSMENT

Primary Category Definition: Are we thinking about what lies ahead and the barriers and obstacles we may have to deal with? Have we considered how we will deal with problems?

3.1 Strategic Business Analysis

Does the organization periodically analyze the current level of achievement relative to what the organization believes should or must be accomplished?

3.2 Short, Medium and Long Range Planning

Does the organization plan for the immediate future, usually covering the next year, the medium term often viewed as a two to five year time horizon, and the longer term which may stretch out many decades?

3.3 Risk Assessment Processes - Macro Level

Are there mechanisms or forums to identify, consider and analyze the significant risks which may threaten the achievement of the organization's business/quality objectives including risks related to inadequate human and/or monetary resources?

3.4 Risk Assessment Processes - Micro Level

Are there any mechanisms or processes in place to analyze specific risks or threats which may result in the non-achievement of business/quality objectives of specific departments, business units or other part of the entity including risks caused by inadequate or inappropriate human, monetary or other resources?

3.5 Control & Risk Self-Assessment

Do work units or groups of employees with responsibility for specific objectives periodically take time to develop or clarify objectives, formally analyze the risks or threats to their objectives, and assess the ability of the controls in use or place to mitigate these threats?

3.6 Continuous Improvement & Analysis Tools

Does the organization and/or sub units use any formalized techniques to continuously review and improve work methods and processes? (eg total quality management tools, recognized quality systems such as Malcolm Baldrige, European Quality Model, ISO 9000 series of standards, etc).

3.7 Systems Development Methodologies

Does the organization use some form of structured development method when designing or reengineering business systems products or processes that considers possible threats and obstacles to the achievement of objectives?

3.8 Disaster Recovery/Contingency Planning

Does the organization have mechanisms or processes in place to anticipate and consider the possibility of significant negative and/or positive events and develop plans to deal with these situations? Examples include disasters which impact on computer systems, executive kidnapping, terrorist attacks, major natural disasters, a hugely successful sales launch, demise of a competitor, new technology, negative or positive legislative developments, and others.

3.9 Other Planning & Risk Assessment Processes

Are there any other processes or activities that relate to the analysis of the past, consideration of threats and opportunities that may occur in the future, and establishment of plans to achieve business/quality objectives?

4.0 CAPABILITY/CONTINUOUS LEARNING

Primary Category Definition: Do we have the necessary knowledge and skills to achieve specified objectives?

4.1 Knowledge/Skills Gap Identification and Resolution Tools/Processes

Are there processes in place to define the knowledge levels and skills necessary to successfully meet job responsibilities; inventory the knowledge and skills of the people doing the work or being considered for job assignments, and frameworks or processes to close any knowledge/skill gaps identified?

4.2 Self-Assessment Forums & Tools

Does a process exist for people individually or collectively to take time to consider whether their current knowledge levels, skill sets, and resource levels are adequate to achieve the organization's business/quality objectives?

4.3 Coaching/Training Activities & Processes

Are there processes in place to close knowledge or skill gaps through coaching and/or other forms of training activities? These can be informal methods such as on the job coaching and feedback, or involve more formalized training in classroom or workshop environments.

4.4 Hiring and Selection Procedures

Does the hiring and selection process formally consider the knowledge and skill attributes of candidates and attempt to hire or select personnel that have knowledge and skill profiles as close to the desired knowledge and skill profile as is possible? Or alternatively, if knowledge and skill mismatches are accepted consciously, are steps taken to mitigate the risks that may result?

4.5 Performance Evaluation
Does the performance evaluation process in use attempt to identify and correct performance related problems which are being caused by knowledge and/or skills gaps?

4.6 Career Planning Processes
Does the organization have formalized processes to identify the developmental steps necessary to ensure employees are acquiring knowledge, skill and experience necessary to fill positions that may open up or emerge in the organization in the future?

4.7 Firing Practices
When serious efforts have been made to correct knowledge and skill gaps but the efforts have been unsuccessful, does the organization take steps to address capability and/or commitment problems through termination or job reassignment?

4.8 Reference Aids
Are there reference aids or resources available which employees can refer to assist them in fulfilling their job responsibilities?

4.9 Other Training/Education Methods
Are there any other processes or activities which increase the assurance that people have the necessary knowledge and skill?

5.0 DIRECT CONTROLS
Primary Category Definition: What specific methods, procedures or devices help directly assure the achievement of objectives?

5.1 Direct Controls Related to Business Systems
Are there specific direct controls built in to business systems to ensure the desired results are achieved? (Note: these tend to be the type of controls auditors have historically concentrated on when evaluating control systems).

5.2 Physical Safeguarding Mechanisms
Are there controls which protect the organization's assets through direct measures such as locks on doors, bars on windows, use of safes to secure valuables, fences around the perimeter of a plant, armed guards protecting a work site, and other similar techniques?

5.3 Reconciliations/Comparisons/Edits
Are there traditional control techniques such as reconciling bank accounts, comparisons of subledger totals to control accounts, system edits, etc. that are relevant to the achievement of the objective?

5.4 Validity/Existence Tests
Are there mechanisms to validate the existence of assets? Fairly common examples include physical inventory counts to determine that quantities and descriptions of goods and/or supplies on hand are accurate, fixed asset inventories to validate the existence of items represented in the accounts, and other similar processes.

5.5 Restricted Access
Is data in manual files or computer stored records protected from unauthorized access through systems based or manual techniques?

5.6 Form/Equipment Design
Does the design of manual business forms, computer input screens, or equipment such as cash registers or computer input terminals assist to reduce the probability of errors?

5.7 Segregation of Duties
Are tasks or processes segregated to reduce the risk of accidental errors and/or fraud?

5.8 Code of Accounts Structure
Does the design of the general ledger or subledger account codes assist in minimizing errors and allow for effective data capture and reporting?

5.9 Other Direct Control Methods, Procedures, or Things
Are there any other methods, procedures or things that have a direct impact on ensuring the achievement of business/quality objectives?

6.0 INDICATOR/MEASUREMENT

Primary Category Definition: Do we know how well we are, or are not, achieving specific objectives?

6.1 Results & Status Reports/Reviews

Are there processes or other mechanisms in use or place which report on or examine the achievement status of a particular objective or objectives? A common example is the review of the monthly or quarterly financial results by senior management or the board against targets. Other examples include a safety review meeting, environmental status review, customer service level reports, and many others.

6.2 Analysis: Statistical/Financial/Competitive

Are there analysis processes in place or use that analyze current achievement levels against relevant benchmarks or planned achievement levels?

6.3 Self-Assessments/Direct Report Audits

Are there any self-assessment activities which include specific consideration of how well an objective is, or is not being achieved? Are there audits performed by people not responsible for the activity or objective which examine and consider the current achievement status relative to some desired or required status?

6.4 Benchmarking Tools/Processes

Does the organization benchmark current achievement levels against the levels or outputs achieved by others? Common examples include benchmarking the cost to produce a defined product or service relative to that of others, comparing service levels provided relative to competitors, performance of a fund manager compared to that of other fund managers, and many other applications.

6.5 Customer Survey Tools/Processes

Are there activities and processes that seek information and feedback from customers in relation to a business/quality objective or objectives? These processes may be very sophisticated and intensive, or as simple as a customer complaint hotline.

6.6 Automated Monitoring/Reporting Mechanisms & Reports

Are there any measurement activities undertaken by computers or machines which result in action occurring if the mechanism indicates situations outside of acceptable tolerance?

6.7 Integrity Concerns Reporting Mechanisms

Are there reporting options in place that allow people to report situations which are, or may be, violations of corporate ethical standards or societal objectives without fear of reprisal? Integrity concerns relate to areas such as employee or corporate honesty, individual or corporate compliance with the law, treatment of people, and other similar situations. These are also referred to as hotlines, or whistleblowing options.

6.8 Employee/Supervisor Observation

Do employees and/or supervisors observe directly the current status of achievement related to one or more business/quality objectives? This can include a service supervisor observing the length of a line-up for bank services, a construction worker assessing if a pipeline is being built to the required specifications, an employee spotting a flawed product being loaded for shipment, etc.

6.9 Other Indicator/Measurement Controls

Are there any other methods, procedures or other things that assist in determining how well or how badly a specified business/quality objective is, or is not being achieved?

7.0 EMPLOYEE WELL-BEING & MORALE

Primary Category Definition: Is employee well-being and morale negatively or positively impacting on the achievement of objectives?

7.1 Employee Surveys

Are employees periodically surveyed to determine their views and attitudes to the organization? Do employees view the organization as a good or a bad place to work? Do they believe that the organization treats employees fairly and with respect?

7.2 Employee Focus Groups

Does the organization periodically assemble groups of employees to discuss and obtain feedback on issues important to the success of the organization? Does the organization work to create shared visions of what is important or does it impose one or more senior manager's vision of what the organization stands for, and the direction it is taking to succeed?

7.3 Employee Question/Answer Vehicles

Does management at all levels provide opportunities for employees to ask questions regarding the organization's direction, treatment of employees, ethical values, and other areas of employee concern or interest?

7.4 Management Communication Processes

Are management personnel at all levels encouraged and trained to effectively communicate with employees in their business units? Are there mechanisms in place to identify managers that are weak in this skill area? Does the organization have vehicles such as e-mail, newsletters, communication hotlines, etc. that provide mechanisms which encourage frank and candid communication with staff?

7.5 Personal and Career Planning

Are there mechanisms and processes in place which assist employees to think about their careers and consider ways to develop themselves and achieve their personal work related goals? Does the organization provide any management training or specialist assistance to help employees identify sources of help and guidance when they are having severe difficulties in their personal lives such as alcohol or drug dependencies, death of close family members, divorce, severe depression, etc?

7.6 Diversity Training/Recognition

Are managers and employees at all levels provided with awareness training, and if necessary, behaviour modification coaching, to ensure that they understand the value of diversity in the composition of work teams and organizations?

7.7 Equity Analysis Processes

Does the organization or work units periodically take time to self-assess or have other mechanisms to assess whether employees are being treated fairly in terms of pay, opportunities and other relevant areas?

7.8 Measurement Tools/Processes

Does the organization attempt to measure and track the state of morale in the organization and in the various business units that make it up to identify problems which may seriously impact on the organization's ability to achieve its objectives?

7.9 Other Well-Being/Morale Processes

Are there any other methods, procedures or other things which assist in measuring and improving employee morale?

8.0 PROCESS OVERSIGHT

Primary Category Definition: Are there people or processes in place to check that the other controls selected are resulting in an acceptable level of residual risk? (i.e. Risk of not achieving objectives).

8.1 Manager/Officer Monitoring/Supervision

Do managers at all levels periodically assess the areas they are responsible for to determine if the current control and risk management designs in place are resulting in an acceptable level of residual risk? Can managers and officers demonstrate that the controls in use or place are conscious selections, or are the controls in use a collection of activities that have evolved over the years without formal analysis occurring to evaluate the ongoing appropriateness of the controls and related risk levels?

8.2 Internal Audits

Do internal audit personnel periodically review specified topics or business areas to analyze whether the controls selected are cost effective and resulting in a level of assurance and residual risk that is acceptable to the work unit, senior management and the board of directors? (eg. internal auditors, safety auditors, environmental auditors, quality auditors, etc.)

8.3 External Audits

Are personnel external to the organization used to assess and report on the organization's public disclosures particularly those related to the organization's financial status?

8.4 Specialist Reviews & Audits

Does the organization engage specialists from time to time to examine and report on the way the organization is managing specific issues or areas of business activity? These reviews can relate to any facet of an organization's activities including such things as customer service, product quality, cost minimization, safety, fraud prevention, regulatory compliance, computer security, derivatives trading operations, and others.

8.5 ISO Review/Regulator Inspections

Does the organization periodically measure its business methods and frameworks against known control or quality criteria such as: the ISO 9000 and 14000 series of standards; quality frameworks including the Malcolm Baldrige system, European Quality Foundation model, derivatives of the Baldrige systems; a disclosed control model such as COSO, CoCo, the Paisley Consulting Control Assurance & Risk Design™ Model, or regulatory criteria related to specific industries or areas of business activity?

8.6 Audit Committee/Board Oversight

Does the audit committee and the board of directors as a whole understand and fulfill their responsibility to oversee the adequacy of the control and risk management frameworks established by management? Has the board subjected the quality of their control governance oversight to a self-assessment process or an external review to check if they are measuring up to national and/or international governance best practices such as the Canadian standards for directors related to control governance? Is there evidence that the board of directors is asking for, and receiving, the quantity and quality of information on the status of control and risk necessary to fulfill their control governance responsibilities?

8.7 Self-Assessment Quality Assurance Reviews

If the organization utilizes self-assessment processes to examine and report on all or part of the operation, are the self-assessment reports subjected to some form of quality assurance review to ensure that they are producing reliable information?

8.8 Authority Grids/Structures & Procedures

Does the organization have formalized criteria that specifies the level of management, up to and including the board of directors that must review and approve decisions taken or being considered by employees and management in the business units? Authority grids may exist which relate to capital spending, hiring of senior executives, risk exposure positions related to derivatives or foreign currency movement, decisions to undertake new lines of business, geographic expansion plans, access to computer systems and files, and many others.

8.9 Other Process Oversight Activities

Are there any other methods, procedures or other activities which are designed to assess the appropriateness of the control and risk management frameworks in place or in use in the organization?

Building the Next Generation RMIS

by Scott Lange

Organizational managers, eager to reduce costs wherever possible, are outsourcing entire departments. Like other internal functions risk management is being challenged to defend the value it contributes to the organization. But while many functions can validate their contributions with cost, revenue or other measurements, risk management has few compelling value metrics to highlight. In an age when information is more accessible than at any time in our past, risk managers face perhaps their greatest need ever for it.

One of the key problems is that risk, by its very nature, defies certainty, predictability and any attempt to define it precisely. Unless backed up by unassailable statistical profiles, risk-related numbers are suspect at best. Even a strong case for the risk management function may not win executive management support if the risk manager can't provide meaningful proof that the function contributes positively to the business. It's a bad situation to be in — risk managers today can't convincingly measure the risk they face, let alone how well they are combating it.

In this environment, risk managers must move quickly to improve their ability to identify, analyze and communicate risk-related information. Technology must be a large part of the solution, yet the suite of risk management products and online information services currently available to risk managers is less than disappointing. And if history and tradition prevail, risk managers will sit in their offices and wait for the insurance industry to come up with solutions. After all, risk managers have historically relied on the insurance industry to record, retain and manage the information flow associated with claims and losses.

After decades of loss tracking, however, risk managers are still hard-pressed to get useful information from their insurance partners. Not only is industry risk information relatively inaccessible, the available data are becoming less and less valuable. The universe of risk for these organizations has changed, broadening the need for data well beyond the scope of the limited and filtered information the industry might provide. Insurance information loses much of its relevance in an environment where the more significant exposures faced by organizations are noninsurance risks.

As we search for information solutions to support risk management, it is important to learn from the past. There are several key reasons why we haven't achieved an effective information infrastructure thus far. When risk managers accepted insurance-based data as their basic sources of risk information, they overlooked the importance of having a more complete view of their organizations' risks. And when industry participants elected to create proprietary data systems lacking common standards, they severely hindered their ability to compile and share quantitatively derived information about risk and losses. The lack of common standards effectively precludes credible combination of data across industries and seriously thwarts attempts to provide meaningful benchmark data on risks facing modern organizations. Looking to the future, it is evident that risk managers and the Insurance industry must change their approach to information management. The ability to measure, analyze and communicate risk effectively is becoming one of the core competencies management expects of risk managers. At the same time, large-organization consumers of insurance recognize that industry providers must upgrade their technology systems and provide useful and efficient risk information to support this emerging expectation. As a result, there is growing pressure to "reinvent" the technology base of this entire industry. This time, however, instead of leaving it up to the insurance industry to define what the new information architecture will look like, risk managers must become actively involved in defining the new solutions.

The Information Hierarchy

While every organization will have different risk-related information system needs, the next generation of risk management information tools must include several primary categories. At the very foundation of this infrastructure is the risk Management information system (RMIS). Not the type of RMIS with which you are familiar, which is basically an insurance information and administration system. The RMIS needed for the future is an essential database of risk information that underlies an organization's quantitative and analytical assessments of risk. It is this repository of data from which the risk manager must derive valuable in-

formation, and the contents must not be limited to only those transactions in which insurance is involved. The system must contain as complete a picture as possible of all risk transactions involving the organization along with ongoing measurements of the associated "exposures".

The second layer of information capability is the analysis tools that will enable the data contained in the RMIS to be converted to useful insights about risk. Without effective analysis, the information contained within the RMIS is largely worthless.

The third and fourth layers of risk information capability are decision and process-management tools. *Decision tools* are technology-based applications that incorporate risk profiles derived from the analysis of data in the RMIS or risk-based knowledge derived from other sources. Decision tools are designed to empower employees by leading them to optimal business decisions and designs. These tools can increase risk management efficiency by embedding key risk expertise and knowledge into decision processes that would otherwise require direct involvement and input from the risk management knowledge worker. *Process management* tools are similar to decision tools in that they empower employees to manage internal processes effectively. The key difference is that these tools are also designed to simultaneously capture information that may get picked up in the RMIS or in separate systems designed to monitor process risks and optimize process management.

The RMIS needed for the future is an essential database of risk information that underlies an organization's analytical assessments of risk.

The final layer of risk information capability consists of communication and distribution tools that bring risk management-related information and services efficiently to the people that need, or can benefit from it. In the modern world, that means networking capability, which will probably need to be global in scope.

In addition to these internal systems, the risk manager will also require external information and transaction links that will enable communication with people and companies outside the organization. Included in this capability are basic e-mail, connectivity, the ability to transfer documents and information, the ability to access and review external data and information and, eventually, the ability to transact business in a cyber-setting.

While not an exhaustive list, these general categories represent a broad spectrum of risk management information capabilities that must be addressed for risk management to deliver and expand its value proposition. Without at least some elements of the above information architecture being available, the risk management franchise will remain threatened.

Enabling the Future

Given risk management's own failure to develop information tools, and the lack of an industry-generated infrastructure to respond to our information needs, how can we establish the information infrastructure we need so desperately today? Must we each build our own tools to achieve the necessary information functionality? Or should we rely on service providers to develop this critical infrastructure? How can we each leverage the work being done by others in our profession and our industry to obtain the new information tools necessary to assure future success?

In fact, these are all questions that the new RIMS Technology Advisory Council will address in the coming year. The council will highlight critical risk management information issues, develop a consensus for common approaches in each identified area, facilitate the development and distribution of effective solutions and provide general leadership to both the industry and the profession in regard to the creation of new technology. To assure a balanced view, the council includes members of the insurance industry and the risk management profession.

To enable the council to focus on and develop solutions for key risk areas, task groups will be formed to specialize in specific areas. Thus far, the council has identified five such groups. One will focus on common industry data standards and how we can evolve from the present landscape to more uniform data structures through which information can be exchanged broadly and efficiently. A second group will focus on electronic commerce standards to assure that the industry will opt for a common approach rather than a patchwork of incompatible transaction systems.

A third task group will monitor how RIMS uses technology for creating value and delivering services to Society members. This group will explore and recommend the implementation of new technologies that will enhance the value of RIMS services to members. A fourth group will seek to leverage the individual solutions being created by member organizations to solve their risk problems. By facilitating sharing among risk managers, and the commercial development by industry of promising solutions, this group will attempt to expand the technology tool box available to risk professionals. Finally, a fifth group is necessary to align these diverse interests into a common set of standards we can all live with.

RIMS' involvement in guiding technology development acknowledges the fact that an industry wide effort is required to help create an effective risk management information infrastructure. Without

the participation of RIMS and its member companies, the industry is not likely to break away from its past tradition of using proprietary solutions to capture and retain customers. Nor is it likely to put the interests of industry customers at the forefront when developing new information technology products.

The Next Generation RIMS

The most significant new technology opportunity for both the risk manager and the industry is the "next generation RMIS" (NGRMIS). An expanded repository of risk attributes and related transactions, the NGRMIS will become the foundation information infrastructure for all of us in the risk management profession.

Before describing the NGRMIS and its related benefits, it is important to highlight the critical shortcomings of the current RMIS products on the market. There are many. Current RMIS products are basically insurance administration databases that focus primarily on claims data. While useful for tracking claims and transaction activity associated with insurance policies, they aren't designed to capture and track risk activity beyond these narrow boundaries. This limitation is not helpful at a time when organizations are trying to expand the scope of risks they are tracking.

Today's systems also rely heavily on insurance sources for data input, which is one of their most significant shortcomings. Unless you are using an insurance company's RMIS system, it is necessary to pay a third party to "convert" data from the insurer's data formats to those of your system. The ludicrous result is that the primary activity (and highest cost) associated with maintaining an RMIS is the "back office cost" of regularly converting insurance data to the system's data format. Very little of the customer's dollar actually goes to improving the user interface or the functionality of the system.

Even if the organization can find value in a database confined to insurance risks, and is willing to pay the high cost of converting data, the credibility of the data captured by the RMIS is questionable. Totals in the system represent only what the insurer reserved and paid on claims. These values are truncated, however, by retentions, policy limits, costs and expenses not paid by the insurer (such as legal fees beyond a set hourly rate) and internal costs incurred in defending a claim. So, if you try to provide meaningful risk analysis, the numbers you come up with will understate the actual cost of the risk event to the organization. For all of the above reasons we simply can't look to current generation RMIS systems as the answer to the risk manager's information dilemma.

How will the next generation RMIS differ from current products? In many ways.

Most important, the NGRMIS will be designed to capture the impact of risk across a much wider spectrum than current systems limited to the insurance subset of organizational risks. To visualize this, consider a blank piece of graph paper. Imagine the hundreds of small cells on the paper each represent a different unit or type of risk. Now assume that approximately 25 percent of the cells are shaded clusters — most of them in gray but perhaps a few in solid black. The shaded cells would represent the risks covered by insurance — gray cells meaning partial-coverage risks and the black ones representing risks completely covered by insurance.

What stands out in this image is that all of the unshaded and gray cells represent areas in which the effects of risk are not captured completely — essentially the condition with today's RMIS systems. The NGRMIS seeks to capture risk transactions for each cell, providing a complete picture of how risk affects the organization. By applying a standard table of risk classifications and attributes, each cell can represent a specific unit of risk. If well-designed, the same table of risk classifications can be used by all organizations.

RIMS' involvement in guiding technology development acknowledges that an industry wide effort is needed to create an effective data infrastructure.

In reality, the table of risk attributes and classifications is more complex than a two-dimensional matrix. The complex data structure necessary to provide flexibility and still produce unique codings for risk situations will probably look more like the structure of DNA than a three-dimensional spreadsheet. That is, each specific risk condition tracked will have a unique string of attribute codes that, when unraveled, will provide a total summary of each loss. Defining the comprehensive table of risk attributes is the critical starting point for development of the NGRMIS and an area where the RIMS Technology Advisory Council will provide leadership.

Defining a standard risk attribute table is just one part of the standards aspect of the NGRMIS. The second layer that must be applied to systems are the technical standards. As noted above, each risk attribute will need to have an exclusive identity code or "mailbox". In addition, it may be necessary to link certain attributes to "auxiliary tables" that provide additional details. If the primary and auxiliary tables are standardized, the identity codes for each risk feature will be unique. This means that any application developed for the NGRMIS will need to incorporate the code structure to facilitate application data linking. It also means that developers will

be able to write new risk applications that automatically map data elements to the NGRMIS identity code structure. In other words, no longer would risk data need to be physically remapped when it is routed from one standards-compliant application to another. As a result, all of the next-generation applications developed for risk analysis, process management and other functions can interface with the NGRMIS as long as the proper data-coding structure is incorporated.

A second important aspect of the NGRMIS will be its linkage to internal accounting systems. The only way to assure that all risk costs will be captured would be to map the risk attribute table to the organization's general ledger system. That is, as the organization incurs risk cost, it will be assigned to the appropriate "cell" on the risk table as a matter of course. Unlike current RMIS systems, such a system will be capable of capturing all expenditures connected with a loss, including retentions as well as uninsured and internal costs. Recoveries — whether from insurance, litigation, salvage or some other source — can be recorded and assigned to the proper cell through the same accounting system. What is interesting here is that the critical definitions of risk for the organization become how the accounting system defines and classifies a transaction rather than how the insurance industry defines it.

By incorporating a standard risk attribute table, a common data standard and an accounting-defined risk-tracking structure, the enhanced value of the NGRMIS becomes very significant. With all organizations applying the same standards in capturing the impact of organizational risk, the available data is now comparable. And combinable. This is critically important, as individual organization databases can be uploaded and consolidated into much larger data sets covering selected organizations, specific industry groups or even whole economic sectors. Benchmarking of risk costs — now virtually impossible — can become a precise science.

It goes almost without saying that the NGRMIS will have other attributes that current RMIS systems lack. As long as the accounting system is running, the risk manager will have a live view of risk unfolding within the organization. Selected attributes can be extracted from the system to provide monitored key performance indicators or metrics on the fly. Using an accounting foundation also means the NGRMIS can be understood and managed by internal finance departments rather than expensive external specialists. And for reporting to executive management, it will be easy to pinpoint how the costs of risk affected the organization's overall performance because each risk transaction can be traced to its balance sheet or income statement effect. Of course, NGRMIS data will be accessible via the Internet, the company Intranet or extranets set up to exchange data with selected business partners.

If the NGRMIS can be designed and applied in a consistent manner, we will begin to generate detailed and homogeneous data on how risk affects our organizations. Over time, as the data matures on longer-term risks, the accumulated data will be of tremendous value to both the risk manager and the broader industry. It will also provide a vastly improved risk management tool for identifying and reducing risks. It will be possible, for instance, to set the system to track leading risk indicators that can provide early warnings on emerging exposures. By participating in data exchanges, risk managers will also be able to obtain broader benchmark information against which to compare their organizational risk profiles. The NGRMIS will enable better internal allocation of risk mitigation resources and allow risk professionals and company management to more clearly define the interrelationship of risk and reward in organizational decisions.

The effects on risk financing activities will be enormous. Currently, most insurance purchases are based on subjective assessments of organizational risk. Having concise data for each risk cell, on both an internal and industry basis, will enable risk managers to better assess their exposure to risk and the corresponding need for risk financing products. With the aid of credible data, the risk manager can being to customize financing programs around the top 10 or 20 risk exposure cells for their organization.

The Industry Wins Too

Equally exciting is the potential value the NGRMIS can provide to the insurance industry. With a standardized and complete customer profile, carriers can be much more selective and accurate in accepting and pricing risk. Having complete insight into the organizational risk profile means the insurer can begin to customize coverage to fit the customer precisely. If the customer wants to buy coverage for 20 risk cells, the insurer will have cost information on those cells and will be able to accurately price the resulting combination. The NGRMIS infrastructure will enable the industry to extend coverage to any or all of the cells because they will be able to accurately predict the likely costs associated with each one. At the claims end, improved pricing, combined with a full understanding of internal and external loss costs, means the insurer will not be as confrontational when responding to claims.

The ability to build risk financing programs cell by cell also opens the door to much more efficient risk management by insurance companies, whose risk accumulation can be tracked by monitoring the

aggregate value of underwritten cells. To diversify their exposures, insurers can build exposure portfolios around the absence of correlation between risks. It will be much easier for the insurer to sell off or swap assumed cells with either the financial markets or reinsurers. In this way the NGRMIS supports the securitization of risks by the financial markets. Different companies can specialize in different cells or combinations. Some companies may elect to specialize in risk consolidation or packaging for ultimate transfer to secondary markets, much in the way mortgages are bundled for resale.

Finally, because the NGRMIS takes an accounting approach to risk, it will be possible to clearly define each risk cell in the same manner in which a general ledger account is described. These account descriptions could actually become the underlying insuring agreement for each risk cell. Such an approach would move us away from the current confusion and conflicts that exist with insurance industry policy language. Instead of having claims resolved by insurance personnel and lawyers, accountants could verify charges and the applicability of cost to the recipient cells. This is another opportunity for industry process revision and redesign that may bring with it significant efficiencies.

Indeed, the NGRMIS will open up new opportunities for the insurance and insurance services industry. On the one hand, risk managers and client organizations will be much more informed about which risks to finance and how much they should pay to transfer risk. Gone will be the days of inefficient financing programs based on a lack of objective risk profiles. While this means "excess profits" generated by unsophisticated buyers will be reduced for insurers, at the same time it opens the door for insurers to recapture much of the market that has left the industry in favor of alternative or self-financing techniques. It also means that organizations with high risk profiles or poor loss experience will have a much more difficult time getting the insurance marketplace (and its customers) to subsidize their risks. Unquestionably, this new information infrastructure will allow carriers to be much more selective about who they insure and what areas of risk they underwrite, leading to greater profitability and reduced earnings volatility.

Looking Ahead

It is easy to see the benefits of the next generation RMIS, but it is not as easy to see how risk managers and industry will work together to improve and enact the basic concepts described here. Nevertheless, it is an effort that must be undertaken. No information technology application can provide as much increased value to the risk management community as the next generation RMIS. As a result, this project will be the first priority of the RIMS Technology Advisory Council. In the coming year, the council will work to define common risk attribute tables, data structures for capturing and storing risk attribute information and technology standards for the NGRMIS and associated applications. RIMS, other risk management organizations and individual consumers of insurance industry products should begin to push the industry to replace its narrow and inefficient data infrastructure, which seems to be serving nobody particularly well.

Needless to say, this article does not begin to provide a complete picture of all of the pieces of technology that must come together to constitute the risk management workstation for the new millennium. Each layer of the risk manager's information tool hierarchy must be presented and discussed as a prerequisite to finding effective technology solutions for the future. To accomplish this, expect subsequent articles directed at the remaining tool categories in future editions of *Risk Management0*

Scott Lange was at the time this article was written, director of risk management at Microsoft Corporation in Redmond WA, and chairman of the RIMS Technology Advisory Counsel.

Excerpt from April 1998 Issue of Risk Management – Reproduced with permission of publisher.

Knowledge Management
An essential ingredient of success

It would be easy to dismiss "knowledge management" as yet another abstract marketing tag that the information technology industry coins regularly to sell more computers, more software and more services.

But while the IT industry is certainly driving the campaign to highlight the benefits of knowledge management, technology is only one of several elements needed to make it work.

In practice, knowledge management requires a combination of many disciplines, from human resources and personnel development to corporate re-engineering and IT.

Technology is, of course, important. Without it, knowledge management would be impossible. IT provides the mechanisms for capturing, storing and retrieving the raw data that form the basis of "knowledge".

The emergence of the web browser and the internet communications infrastructure as standards makes it simple and inexpensive to access data. But while the technology infrastructure has evolved to make knowledge management possible, the real benefits can only come from applying knowledge.

Undoubtedly, it is the potential benefit of applying knowledge management that has attracted the attention of senior executives. A recent survey by PricewaterhouseCoopers in conjunction with the World Economic Forum found that 95 percent of chief executive officers saw knowledge management as an essential ingredient for the success of their company. Many also admitted that their knowledge management programs could be improved.

There is good reason. Businesses can only survive and thrive by exploiting every possible advantage in an increasingly competitive market. It follows that any special knowledge that an organization might have – from ownership of intellectual property in the form of patents and copyrights to special skills and innovative business processes – is an asset work protecting and nurturing.

Knowledge management is a combination of disciplines and technologies which aims to do exactly this. The disciplines have evolved from several areas, including business process re-engineering and human resource management.

The technologies spring from two main sources: the universal communications medium of the internet and established software technologies such as information retrieval, document management and workflow processing.

This complex pedigree does make knowledge management hard to define – with each area of academia, industry or consultancy offering its own variation. IT people see it as an extension of technologies such as data warehousing and information retrieval. Human resources experts see it as part of re-casting the corporation as the "learning organisation".

And different flavours of consultancy see it as exploitation of "intellectual capital" or the foundation for "knowledge-centric" organisations.

John Keane Junior, chief executive of US software company Keane, offers a practical definition:

"Knowledge management means different things to different people. We see it as combining people, process and technology to share information to gain competitive advantage. The only sustainable competitive advantage comes from learning faster than your competitors."

Peter Dorrington, a consultant specialising in knowledge management at international IT services consultancy Ecsoft says: "It's about getting knowledge from those who have it to those who need it."

Philip Crawford, European vice-president of US software group Oracle, offers an even more simple definition: "Knowledge is the information needed to make business decisions."

The truth is that knowledge management covers a wide range of activities with a common theme of sharing information.

At its most primitive, knowledge management can be as simple as writing down contact telephone numbers in Filofax format, photocopying the list and sending it to everyone who needs it.

At its most advanced, knowledge management attempts to encode the unencodable. It sets out to capture the unwritten tricks of the trade which make an organisation function, store them "formally" in a computer database and use them as a corporate resource.

The theory is that once formalised, the knowledge may be tapped by employees to help them do their jobs better and, ultimately, improve the performance of the organisation.

Most organisations are, of course looking for something between these two extremes. The pressures of the market and the changing business environment mean that every organisation must exploit its knowledge assets to the full. But most would stop short of trying to capture something as intangible as personal judgement.

"It is important to start with business objectives and then see how knowledge can fit in – how it can help meet those objectives," says Elizabeth Lank, knowledge programme director at computer services company ICL.

ICL, part of Japan's Fujitsu, is a keen advocate of knowledge management. In 1997, it helped establish the Strategic Management of Knowledge and Organizational Learning Consortium.

Chaired by Keith Todd, ICL's chief executive, the consortium is composed of senior directors and executives form top companies including Imperial Chemical Industries of the UK, Unilever, the Anglo-Dutch consumer goods group, Switzerland's Ciba Specialty Chemicals, Monsanto, the US life sciences group, and Statoil, Norway's state-owned oil company.

Ms. Lank says knowledge management is a challenge that organisations cannot ignore. "Companies cannot afford to ignore the value they have invested in their knowledge assts. We can demystify it and find ways to look after it – but this does not have to be expensive."

"The first step is to recognise that knowledge is not a "thing" – it is a constant flow. At ICL, for example, we have been working on creating a culture of collaboration which encourages people to share their knowledge."

Over the past decade, ICL has changed from a hardware manufacturing company to a service-based systems integrator and application developer. Ms. Lank says that the change has led to a much greater emphasis on knowledge as an asset.

The company's "Café Vik" initiative is an example of the practical initiatives that ICL has taken to promote knowledge. "Vik stands for Valuing ICL Knowledge and the idea is to encourage employees to make knowledge visible. Knowledge sits in people's heads and that is where it will stay unless you find ways to bring it out," explains Ms. Lank.

Chris Matthias, chairman of consultant Conduit Communications, agrees that cultural change is an essential first step for any company aiming to get the best from knowledge management. But he also acknowledges the important role of technology.

"It is absolutely about culture – and it is also about technology. Technology has a huge role to play in brining the information together that forms the knowledge base. Obviously, we couldn't get there without it. But it is essential to start with a strategy that brings people, process and technology together – and it must include a program for cultural change."

Mr. Matthias believes that this is often the hardest barrier to overcome: "People do not share their knowledge naturally – in fact we are

taught from an early age that sharing is bad. At school, sharing knowledge is called cheating."

"When we start working, we are rewarded for what we know – so we don't want to share knowledge or we lose value. We have to change that culture to get knowledge management to work."

Mr. Dorrington of ECsoft also sees the importance or cultural change combined with effective IT. "Knowledge management demands expertise in a lot of different disciplines – job deconstruction from training experts, business process re-engineering – and technology tools have a role to play."

There is certainly no shortage of technology to support knowledge management programmes. The broad base of technology needed to create the infrastructure and application-support tools has attracted a diverse set of operators.

These include big names in the IT world such as Microsoft and IBM; specialists such as Verity, Fulcrum and Excalibur who start from traditional information retrieval; document management specialists such as Documentum, Filenet and Novasoft; and workflow product suppliers such as Staffwware and Action Technologies.

Open text's Livelink is an example of a comprehensive approach – bringing information retrieval, workflow and document management together under a single environment.

Derek Buchanan, UK managing director for Canadian-based Open Text, says: "We think the important issue is how you harness technology to make knowledge management more effective. Our approach is to bring the components together behind a web interface to make it easy to access and use."

"If it is difficult to use, then people will struggle to get it to work and become disillusioned."

Mr. Crawford of Oracle agrees that accessibility is one of the keys to successful knowledge management and technology is the way to deliver it. "In the past, there was a whole heap of information locked up in the mainframe. Only very few people had access to it and they were not necessarily the decision-makers. It was like the days when writing was in the hands of scribes and priests. But the internet is like the dawning of a new era – comparable to the arrival of the printing press. The Internet gives access to anyone."

He adds that the key is to apply the knowledge once it has been captured by the technology. "We have spent the last 30 years building up information bases and we could not have got to where we are today without that. But I think we have moved on past the processes that generate what you do with the information. Is it going to bring a business closer to its customers? Is it going to make the business perform better?"

Used properly, knowledge management can provide positive answers to these questions. The trick comes in balancing the technology with all of the other factors – human resources, corporate structure, and organizational processes.

This is not an easy task by any means – but one that no 21st century enterprise can afford to ignore.

Article by Philip Manchester – appeared in Financial Times April 26, 1999