R.I.S.C.
International

An Executive Guide to

Corporate Defence Management (CDM)

A Whitepaper By Sean Lyons
November 2006

Risk-Intelligence-Security-Control

R.I.S.C. International (Ireland)

www.riscinternational.ie

TABLE OF CONTENTS

Executive Summary

In these changing times the constantly evolving challenges facing corporations are giving rise to ongoing turbulence in the corporate world, and there are indications of ominous times ahead. Defending a corporation requires far more than simply concentrating on security or legal defence, to help ensure survival contemporary corporate defence requires a far more comprehensive brief.

Corporate Defence

The challenge of enterprise-wide defence is to defend an organisation from a multitude of threats and vulnerabilities. Defending an organisation includes defending the interests of all the stakeholders, and consequently it is an extremely responsible station. While the term corporate defence is perhaps intuitively understood, what remains to be understood is, why to date it has not occupied a more eminent role in corporate strategy. Organisations already implement a variety of corporate defence related disciplines in order to address potential threats, and this multiplicity can result in some uncertainty concerning ultimate responsibility and accountability for corporate defence. Corporate defence requires a strategic outlook, and the convergence and alignment of a number of existing disciplines, which need to be co-ordinated in a strategic manner (e.g. under the one umbrella). Using advanced technologies it is now possible to create this fusion and eliminate any “chinese walls” which exist. Common sense alone dictates that the requirement for an active corporate defence function is not just a nicety, it is a necessity, a necessity that must be demanded by all the stakeholders in the organisation. Going forward the most robust organisations will seek to have the highest pre-emptive capabilities in place, as it is the reaction times to potential threats which determine the magnitude of the initial impact and the subsequent collateral damage.

Corporate Defence Management (CDM)

Corporate Defence Management (CDM) represents a holistic solution to the challenges facing corporate defence. CDM requires a proactive approach to co-ordinating and integrating a range of interrelated disciplines which taken together can help protect the organisation from potential hazards. In order to adequately defend the organisation one must first know what you are defending, and what you are defending against. To do this effectively all defensive disciplines need to be operating in unison towards a common set of objectives. By focusing on anticipating future threats, preventative measures can be taken to shield the organisation. The operation of a comprehensive detection system can help ensure rapid and effective reaction to issues which do occur, and enable timely mitigation of threats and possible collateral damage. The task of CDM is an unending one, it is a constantly evolving discipline which requires ongoing vigilance in order to ensure continuous improvement. While the accurate prediction of future threats can never be guaranteed, many of these can be identified in advance, which presents the opportunity to take appropriate steps to avoid the dangers and avert a crisis.

By taking a proactive stance and putting a CDM framework in place, many dangers and potential hazards can be avoided or at least mitigated. The benefits of implementing an integrated CDM program are abundant, as an organisation puts itself in the best possible position to, not only defend itself and help minimise both uncertainty and the resulting threats, but to take full advantage of the opportunities which present themselves. By focusing on preserving the assets of the organisation, and protecting and safeguarding the safety, welfare and wellbeing of all its stakeholders, corporations will demonstrate a desire to realise a more meaningful sense of corporate integrity. By securing the assets of the organisation, the business value of the organisation is also being protected in the process. If corporations are to continue to successfully evolve financially, economically and ethically, then defending their stakeholders must be prioritised, and CDM is currently the best available option to achieve this objective.

An Executive Guide To Corporate Defence Management (CDM)

PREFACE

This whitepaper on the emerging discipline of Corporate Defence Management (CDM) is the first whitepaper of its kind dealing with this subject. The whitepaper represents the 3rd installment in a series of papers designed to raise awareness of the requirement for corporate defence to play a more eminent role in corporate strategy.

This paper was prepared as a further development of, and natural progression to, the previous two papers recently published by the author on the topics of "Corporate Defence" and "Corporate Defence Management". It is designed to act as a helpful guide to executives interested in the area of contemporary corporate defence and in particular in the discipline of Corporate Defence Management (CDM).

Previously published papers include:

"Corporate Defence: Are Stakeholders Interests Adequately Defended?"

- *The Journal of Operational Risk, Vol. 1, No. 2*

"Corporate Defence Management: A Strategic Imperative"

- *BankDirector.com / Resource Center / Strategy*

The content of this whitepaper represents the author's professional opinions and is intended to act as a commentary to promote further debate and discussion on the issues raised.[1]

THE AUTHOR

The author, Sean Lyons, has gained a wealth of experience, and has engaged in extensive research, in the area of contemporary corporate defence. In addition to being the architect and pioneer of the discipline of Corporate Defence Management (CDM), the author has already had a number of original papers published internationally on corporate defence.

A graduate of the University of Limerick, Sean is a former Internal Auditor and Operational Troubleshooter. With close to two decades of professional experience in the banking and financial services industry, he has worked with a number of leading financial institutions in Ireland, the U.K. and Australia.

Sean Lyons is the founder and principal of R.I.S.C. International (Ireland) where he operates as a corporate defence advisor and consultant.

[1]This publication contains general information only and should not be relied upon for accounting, business, financial, investment, legal, tax or other professional advice services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect you or your business. Before making any decision or taking any action that may affect you or your business, you should consult a qualified professional advisor. The information contained in this publication likely will change in material respects; we are under no obligation to update such information. R.I.S.C. International (Ireland) shall not have any liability to any person or entity who relies on this publication.

INTRODUCTION

The 21st century has already seen profound changes in the corporate landscape, and this is continuing at an increasingly alarming rate. While in former times the challenges facing the corporate world were continually changing, it is the accelerated rate at which this change is currently occurring which may yet prove to be the greatest challenge to corporate survival.

In an "information age" full of uncertainty, intelligence is considered to be paramount, yet our knowledge is at best provisional, imperfect or obsolete, as it so often relates to yesterday's emergency and is subject to change at any point in time.

The spate of recent scandals from Enron to Hewlett-Packard, has only served to highlight the challenges facing self regulation in the corporate world. Many of these "scandals" involved so-called pillars of society within the business community. Subsequent investigations only highlighted the inherent weaknesses in the checks and balances in operation, and how an unethical culture can be fostered in seemingly respected organisations.

As a result public attention has firmly focused on corporate operations, while the issue of corporate ethics has also been subject to increased scrutiny. The sheer magnitude of the financial impact of these scandals, and the resulting impact on stakeholders, served to prompt regulator reaction. In an attempt to plug the obvious gaps uncovered, and to help restore public confidence, the regulators have been stung into action like never before. This has resulted in the introduction of a litany of compliance related issues, including a multitude of legislation, regulations and best practice guidelines.

Potential Global Concerns

- Effects of a potential energy crisis
- Unprecedented level of natural disasters
- Problems facing continuing globalisation
- Race to develop nuclear technology
- Worsening crisis in the Middle East
- Competition from Asia's economic giants
- Conflict with leftist regimes in Latin America
- Increased social unrest in old Europe

Corporate Threats

- Bankruptcies as a result of senior executive mismanagement and incompetence
- Persistent increase in internal fraud and white collar crime
- The continuous evolution and mutation of cyber-threats
- Increasingly complex and sophisticated financial crime
- Laundering of the proceeds from organised crime and terrorism
- Financial misrepresentations and accounting fraud

Every corporate institution has to some degree already been significantly affected by these challenges, be it directly or indirectly. In addition to the direct losses incurred by institutions there has also been the requirement to increase overheads and the opportunity cost of the deflection of management time. Added to this has been the additional stress of senior management facing criminal prosecutions and the very real threat of incarceration.

Under such circumstances this is certainly no time for complacency, as organisations continue their fight for corporate survival in an increasingly unpredictable world. As the defence of our stakeholders is becoming a progressively difficult task, traditional strategies are no longer adequate and a more progressive approach is now required. A passive attitude is simply no longer sustainable against ever-changing threats, if we are to adequately defend the diverse interests of our stakeholders into the future.

CORPORATE DEFENCE EXPLAINED

While corporate defence is a term quite often used and perhaps intuitively understood, it remains somewhat of a mystery as to why to date it has not occupied a more eminent strategic role in modern corporations. The term "Corporate Defence" is sometimes used in a headline, or quite often referred to in a bullet-point however there appears to be a distinct lack of detail as to what is meant by the term. As a result its role and purpose also appears not to be fully understood or indeed its worth fully appreciated.

All too often it is considered in a very narrow focus, as discussions about the topic of corporate defence with executives of successful organisations, will very often be restricted to corporate legal or security issues. Contemporary corporate defence has of course a far more comprehensive brief.

Corporate Defence Defined

"Corporate Defence can be defined as an alchemy of both science and art, aimed at defending an organisation from a multitude of possible threats and vulnerabilities."[2]

Defending an organisation includes defending the company name and all its stakeholders. This includes defending the shareholders, the business partners, and of course its clients. Defending the company name also means defending its people, management and staff. Corporate defence focuses on stakeholders as people, as human beings, and not just numbers or bottom line financials.

Consequently the defence of the organisation is an extremely responsible station, and there are a large number of stakeholders who rely on this function to operate in an effective manner in order to defend their diverse interests.

Stakeholder Checklist

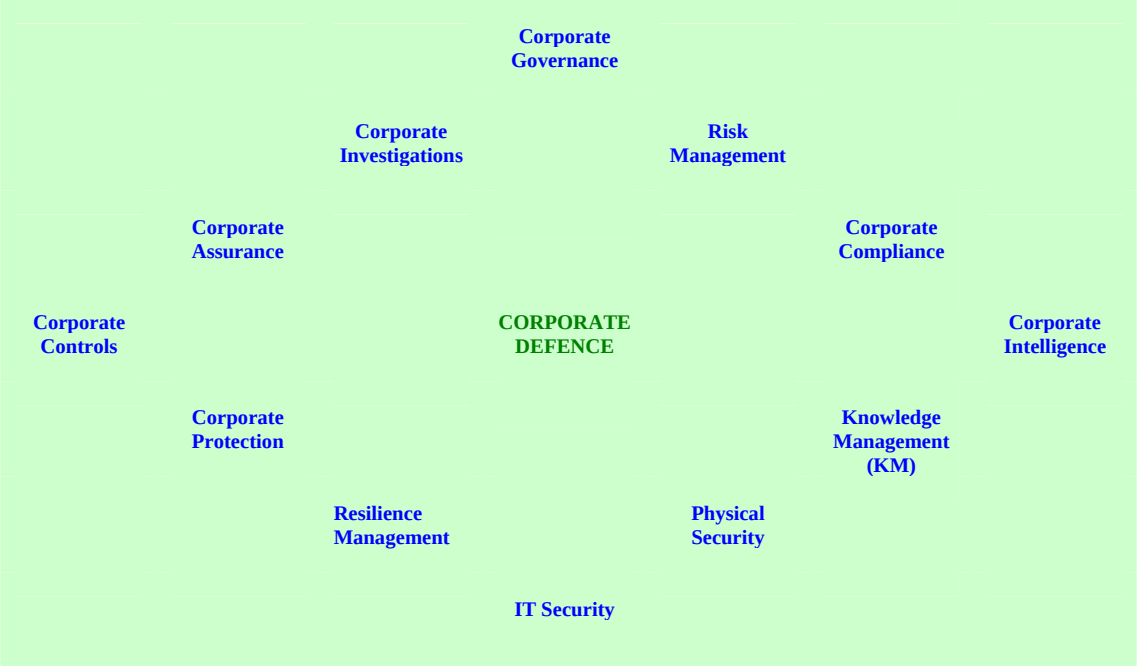
Should stakeholders be concerned about their organisation's position in relation to corporate defence? In order to determine if there are grounds for them to have concerns, they should consider their organisation's position in response to the following five questions.

1. Does it have a formal corporate defence program or strategy in place?
2. Does it have a formal corporate defence committee, director or function in place?
3. Where exactly does the responsibility for corporate defence actually rest within the organisation and who is accountable?
4. How does it defend the interests of the stakeholders?
5. How are stakeholders interests communicated and prioritised?

With this in mind it is rather remarkable that stakeholders should even have to contemplate whether top organisations actually have a formal "Corporate Defence" strategy in place. In many cases stakeholders need only enquire as to whether or not their organisations have a formal corporate defence program, strategy, committee, or director in place, for concerns to be aroused. The critical questions which must be raised are obvious ones, where exactly does the responsibility for corporate defence actually rest within the organisation and who is accountable? Defending the organisation is not a once off, point in time, assignment. The challenge of defending against threats and vulnerabilities is without end, it is a constantly evolving process which requires ongoing vigilance and an iterative approach, in order to ensure constant revision and continuous improvement. It requires a strategic outlook and the alignment of a number of existing disciplines which need to be co-ordinated in a strategic manner.

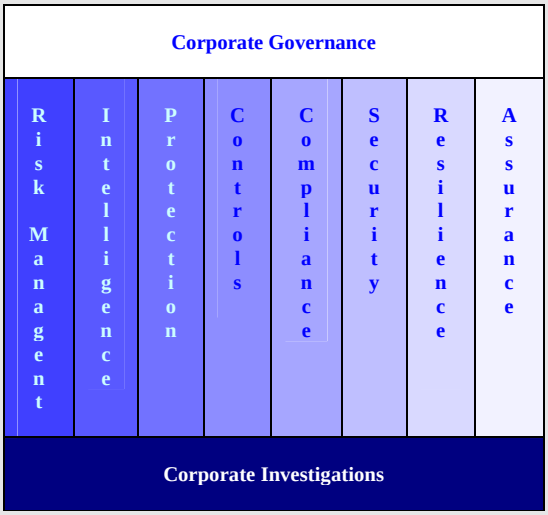
[2] "Corporate Defence: Are Stakeholders Interests Adequately Defended?" – Sean Lyons – The Journal of Operational Risk, Vol. 1, No. 2, (www.thejournalofoperationalrisk.com)

The Corporate Defence Domain



Currently organisations already implement a variety of what could be best described as corporate defence related disciplines, in order to address potential threats. Each of these represents an important link in the chain to help corporations defend against internal and external threats, and to collectively work together towards a common set of objectives. Unfortunately very often these disciplines are not in alignment with one another and tend to operate in isolation (e.g. in silos) thereby creating vulnerability, and reducing their potential for overall effectiveness.

A Traditional Paradigm



The traditional paradigm (opposite) illustrates the silo effect. In this diagram certain disciplines are displayed vertically to illustrate the silo type organisation, the horizontally displayed disciplines reflect their cause and effect nature. In order to achieve a holistic solution to corporate defence the symbiotic relationship which exists between these disciplines must be understood and fully appreciated.

For "Corporate Defence" strategies to be effective they must incorporate all of these disciplines in a co-ordinated and systematic manner. What needs to be created is a cybernetic loop whereby communication includes multi-dimensional feedback, both top-down and bottom-up, as well as operating horizontally.

CORPORATE DEFENCE MANAGEMENT AS A STRATEGIC DISCIPLINE

The necessary holistic approach needed will require a strategic re-alignment within the organisation, and must not only include Front, Middle and Back office participation, but also requires an independent critical role with high level responsibility for strategy and planning, co-ordination, and crucially, communication. If organisations genuinely wish to progress to the next level of corporate integrity, this must include proactively protecting and defending the interests of all of its stakeholders.

It is time to introduce a mechanism to proactively manage these challenges, and Corporate Defence Management (CDM) represents a strategic management discipline and a holistic solution to the challenges facing corporate defence.

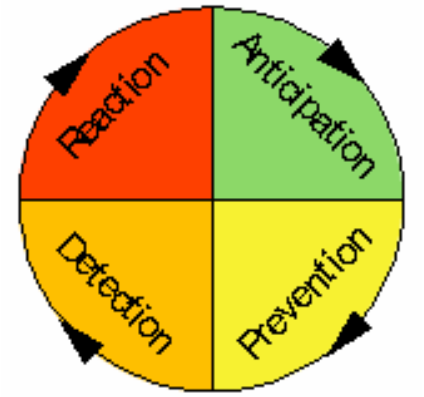
CDM can be defined as "***the discipline of managing corporate defence in order to adequately defend the interests of the stakeholders. It requires a proactive approach to co-ordinating and integrating a range of interrelated disciplines, which taken together can help to anticipate, prevent, detect and react to potential threats and vulnerabilities, thereby protecting the organisation from potential hazards.***"[3]

Potential Hazards

- Professional Negligence Prosecutions
- Fraud, Corruption and Embezzlement
- Accounting Irregularities
- Insolvency, Liquidation & Bankruptcy
- Regulatory Compliance breaches
- Rogue Traders & Insider trading
- Public and Civil Litigation
- Product Liability Class Actions
- Employee Theft and sabotage
- Terrorism & Armed Robbery
- Cyber Attacks, Viruses & Trojans
- Organised Crime & Money Laundering
- Espionage, Bugging & Spyware
- Confidentiality and Data Protection
- Intellectual Property
- Natural Disasters

The function of CDM should be responsible for directing and co-ordinating the range of related defensive disciplines in order to achieve a coherent strategic approach. For corporate defence related disciplines, their defensive mission is generally to anticipate, prevent, detect and react to potential threats and vulnerabilities in a timely manner. Therefore it could be said that anticipation, prevention, detection and reaction are the four cornerstones of a corporate defence (see the corporate defence cycle below).

Corporate Defence Cycle

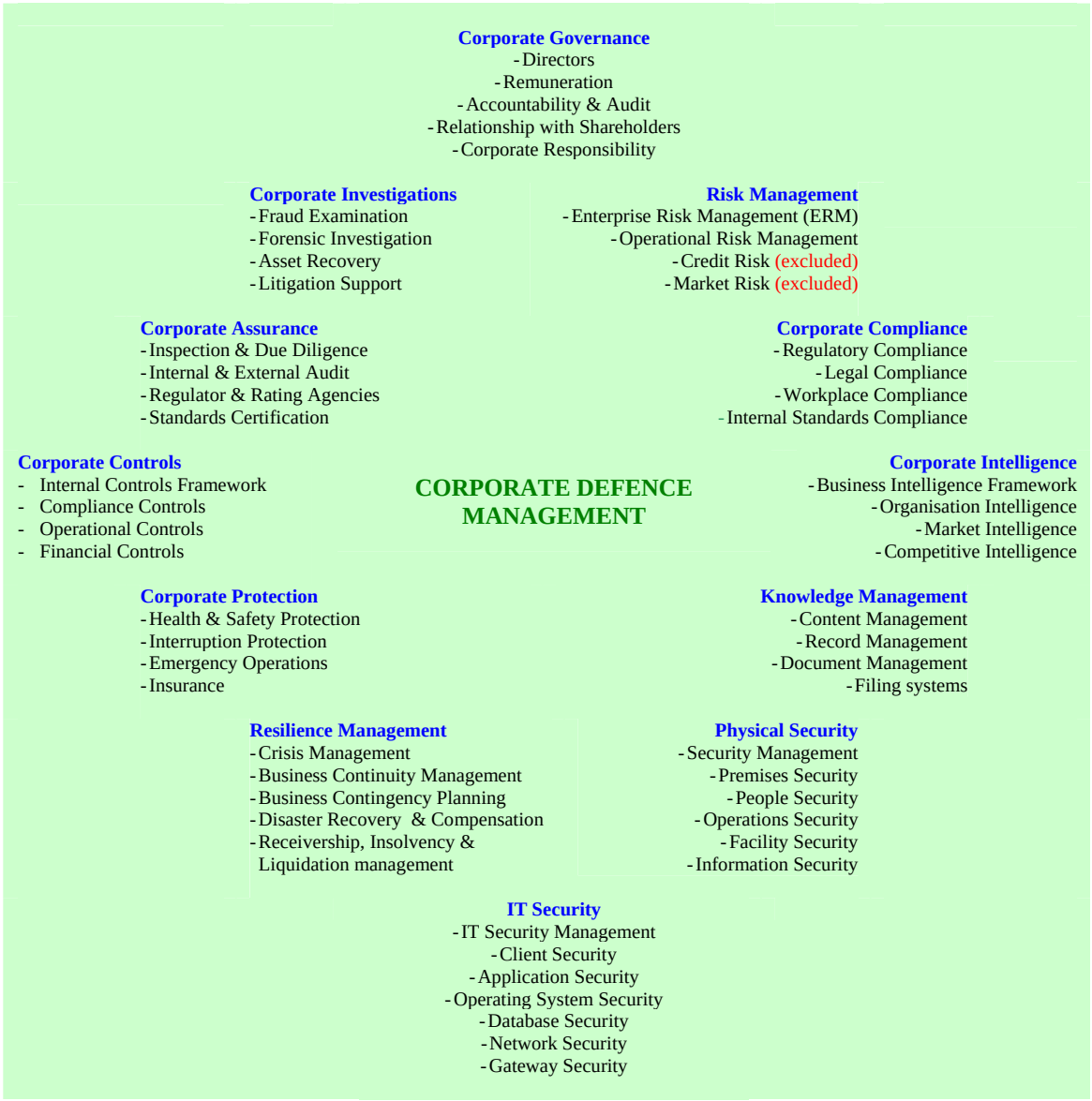


Note: *This is a continuous improvement process.*

Anticipation: The timely identification and assessment of existing threats and vulnerabilities, and the prediction of future threats and vulnerabilities.
Prevention: Taking sufficient measures to shield the organisation against anticipated threats and vulnerabilities.
Detection: Identification of activity types (exceptions, deviations & anomalies etc) which indicate a breach of corporate defence protocol.
Reaction: The timely response to a particular event or series of events, in order to both mitigate the current situation, and to take further corrective action in relation to deficiencies identified, and to prevent these events re-occurring in the future.

[3] Corporate Defence Management: A Strategic Imperative – Sean Lyons – BankDirector.com / Resource Center / Strategy - Oct 2006

The CDM Continuum



The task of CDM involves the consolidation of the above defensive activities, which involves the alignment of a multitude of diverse yet interrelated domains. CDM must be all inclusive in order to be effective. All defensive disciplines need to be functioning in unison, with the same performance expectations. This holistic approach must include input (constructive criticism and healthy challenging) and co-operation from Front, Middle and Back Office activities. Using advanced technologies it is now possible to create a fusion of these disciplines and to eliminate any chinese walls.

This task of integrating and co-ordinating all of these activities demands astute political insights and subtle communication skills from those entrusted in this role, and a spirit of co-operation from all parties to help facilitate working together in a positive and proactive manner. This is easiest achieved by utilising existing structures and relationships where possible, in order to minimise the difficulties associated with organisational change.

LEVERAGING FROM RELATED BEST PRACTICE FRAMEWORKS

In order to adequately defend stakeholder interests, there must first be an appropriate structure in place to help maximise the possibility of achieving this objective. This structure will act as the foundation on which a successful corporate defence program can be built and the framework for interaction with other related disciplines.

Organisations already have a variety of structures in place which intersect each other in numerous ways and on multiple levels.

- Parent Company
- Subsidiaries
- Business Units
- Divisions
- Departments
- Branches

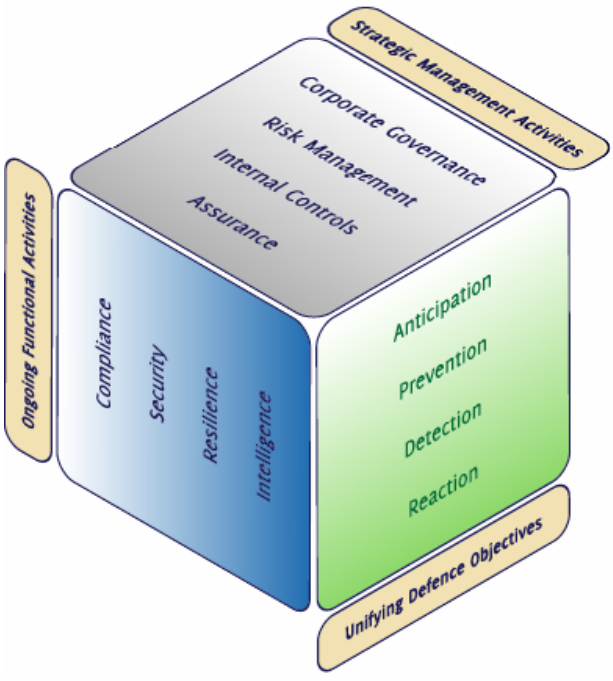
A number of best practice guidelines exist in relation to frameworks in the core strategic management areas of corporate defence. The implementation of these best practices and frameworks helps to assist in the achievement of the organisations objectives. CDM ideally should position itself in such a way that these related disciplines feed into the corporate defence process rather that creating yet another complex framework. The challenge for CDM is to align itself to these existing frameworks and harness these synergies in a constructive way, while also adding its own unique value in the process.

A CDM PARADIGM

To this end a CDM paradigm has been conceived to help integrate the necessary elements. By utilising existing components this paradigm presents a structure which allows for the application, understanding, implementation and cohesive integration of these existing components. Progressive organisations clearly recognise that it is no longer prudent to consider these component parts in isolation. This new paradigm (see below) is based on a three dimensional view of corporate defence. The three dimensions are outlined as follows:

- Strategic Management Activities
- Ongoing Functional Activities
- Unifying Defence Objectives

The CDM Paradigm



Strategic Management Activities

The 1st dimension relates to certain strategic management activities. In relation to CDM certain areas are considered to be the core strategic management areas. These relate to frameworks and best practices which should form the backbone of the organisation's corporate defence strategic activities, around which other related functional disciplines operate. These core areas relate to the following four pillars:

- Corporate Governance
- Risk Management
- Internal Controls
- Assurance (includes Investigations)

Each of these corporate defence pillars are considered to be fundamental strategic frameworks which are required to be operating effectively in order to successfully implement a robust corporate defence program. The critical frameworks put in place to enable the operation of each of these pillars, will in turn determine the operational effectiveness of other ongoing functional activities, which for the purposes of corporate defence are regarded as the 2nd dimension in the paradigm.

GOVERNANCE GUIDELINES

Directors
- The Board
- Chairman and Chief Executive
- Board Balance and Independence
- Appointments to the Board
- Information and Professional Development
- Performance evaluation
- Re-election

Remuneration
- The level and make-up of remuneration
- Procedure

Accountability and Audit
- Financial Reporting
- Internal Control
- Audit Committee and Auditors

Relations with Shareholders
- Dialogue with Institutional Shareholders
- Constructive use of AGM

See "The Combined Code on Corporate Governance" – July 2003 – www.fsa.gov.uk

INTERNAL CONTROLS GUIDELINES

Categories of Internal Control
- Operations
- Financial Reporting
- Compliance

Internal Control Components
- Control Environment
- Risk Assessment
- Control Activities
- Information and Communications
- Monitoring

Internal Control Areas
- Unit Level
- Activity Level

See "Internal Control – Integrated Framework" – 1992 – www.coso.org

Ongoing Functional Activities

The 2nd dimension focuses on essential ongoing functional activities. A number of these operational activities are considered to be key functional areas within corporate defence, in so much as they are required to be continuously operating on an ongoing basis throughout the organisation. These activities both intersect and are intersected by strategic management activities and are considered to be essential in the implementation of a robust program. The four core activities relate to the following:

- Compliance
- Security (includes Physical and IT)
- Resilience (includes Protection)
- Intelligence (includes KM)

As a multitude of best practice frameworks, bench marks and guidelines are available in these areas, the appropriate "best fit" should be considered in consultation with both in-house and external professionals in the related areas.

These core ongoing functional activities generally have a number of somewhat specialist disciplines (refer to the CDM continuum page 10) operating within their sphere of activity. The requirement for specialist disciplines is increasing constantly as more and more complicated and sophisticated techniques are required to keep pace with technological progress. The interaction between these disciplines and the reporting and communication lines in place will determine the robustness of the organisation's defensive capabilities.

Each of these specialist disciplines is in itself considered to be a valuable link in the corporate defence chain, and in turn weaknesses or vulnerabilities in one area can have a potentially damaging impact elsewhere within the organisation. The old maxim that "the chain is only as strong as its weakest link" certainly applies.

ASSURANCE GUIDELINES

Attribute Standards
- Purpose, Authority and Responsibility
- Independence and Objectivity
- Proficiency and Due Professional Care
- Quality Assurance and Improvement Program

Performance Standards
- Managing the Assurance Activity
- Nature of Work
- Engagement Planning
- Performing the Engagement
- Communicating Results
- Monitoring Progress
- Resolution of Management's Acceptance of Risks

See "International Standards For the Professional Practice of Internal Auditing" – Jan 2004 - www.theiia.org

RISK MANAGEMENT GUIDELINES

Entity Objectives
- Strategic
- Operations
- Reporting
- Compliance

Components of Risk Management
- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information & Communications
- Monitoring

Entity's Units
- Subsidiary
- Business Unit
- Division
- Entity-Level

See "Enterprise Risk Management – Integrated Framework" – Sept 2004 - www.coso.org

Unifying Defence Objectives

The 3rd dimension focuses on what are termed unifying defence objectives. From a corporate defence perspective the underlying objectives which must be continuously present throughout the organisation relate to the cornerstones of corporate defence:
- Anticipation
- Prevention
- Detection
- Reaction

These four enterprise wide objectives should be present in the mindset throughout the organisation. As individuals perform a variety of daily activities they should always be cognizant of these corporate defence drivers. Each staff member must fully understand the corporate defence cycle, be alert to the potential hazards and remain in a constant state of vigilance. The degree to which these unifying objectives are present in the corporate mindset throughout the organisation could be said to represent the "DNA" of corporate defence, and will ultimately determine the organisation's success in dealing with the challenges it faces.

FACILITATING SOUND PRINCIPLES

PROFESSIONAL STANDARDS

Professional Standards are clear statements that reflect the minimum qualifications for mastery and knowledge of processes, skills and practices, that professionals should have before undertaking work which may put an employer at risk, either physically or financially.

CDM as a new and emerging discipline must abide by the highest possible professional standards which are indicative of the responsibility of its station. At a minimum an organisation's expectation of the adherence of the CDM function to professional standards should be consistent with those existing professional standards of other related professional disciplines (e.g. Risk Management & Audit etc).

Such standards will contribute to the attainment of a reputation of competence by the profession. The standards will facilitate the obtaining of work by individual practitioner in the international arena. The field of CDM has already many domains, ranging from Corporate Governance to IT Security, to Forensic Accounting. It is unreasonable to expect any one individual to be considered "an expert" in more than one such domain. This needs to be recognized particularly in the body of knowledge required to be known by one person. The constant changes within these domains together with the dynamic development of new domains in corporate defence means that the standards themselves should be continuously developed and individuals should anticipate life long learning.

CDM is by its very nature is a strategic management discipline which requires its own specific managerial skills and expertise. The breath of experience, the depth of knowledge and the precise level of detail required by particular individuals within the CDM function will ultimately be dependent on the organisation and the business activities in which that organisation engages. Each organisation must therefore decide for itself.

Application of Professional standards

Professional standards should at a minimum address the following components

- Ethics of professional practice
- Established body of knowledge
- Education and Training
- Professional Experience
- Best Practice and proven methodologies
- Maintenance of competence

The benefits of applying professional standards include the following:

- Assurance that critical work is performed by competent individuals regardless of where qualifications and experience were obtained
- Assurance that the person who meets such standards is competent to perform tasks regardless of where work is performed or the output of the work is used.
- Assurance that theses qualifications and experience gained will be recognized internationally.

ETHICS, INTEGRITY AND CONDUCT

Each organisation should ensure that it has clear, unambiguous and, appropriate codes and policies in place to address ethical behaviour, professional and personal integrity, and standards in relation to conduct considered to be appropriate by staff members. At a minimum, recognized external codes should be applied to ensure compliance with best practice.

The CDM function should strictly comply with all codes and policies relating to ethics, integrity and conduct. Such codes and policies are considered necessary and appropriate for the profession of CDM, as they provide instruction to those operating within the CDM function. The purpose of such codes and policies is to promote an ethical culture within the organisation and in the CDM function itself.

GUIDING PRINCIPLES

Guiding principles represent prudent practices and their purpose is to provide education and guidance for those engaging in CDM. As organisations operate in different ways and because of their varying levels of sophistication, the application of different methodologies and the evolving nature of these methodologies, guidelines cannot offer specific guidance to be followed in all cases.

Each organisation should develop, adapt or adopt CDM methodologies which best suit its own business needs and capabilities, in addition to the needs and interests of its stakeholders. Consequently the application of these principles, the approach taken, the structure implemented, and day to day operations will vary by organisation. While these variations are considered to be appropriate and proper, the core principles do fundamentally address what the management of corporate defence should aim to achieve.

Accordingly each organisation should retain the flexibility and right to tailor the program where it sees fit and ultimately to prudently design a program which meets its own needs and capabilities within the spirit of these core principles.

When considering the approach and structure to be pursued in relation to CDM within your organisation, a number of issues must be clarified in advance. In order to be in a position to accurately determine the appropriate course of action, adequate advance consideration should be given in the initial planning phase.

Due advance consideration should therefore be given to the expected role of CDM, and its expected position within the organisation. Equally important however is the consideration of the organisation having realistic expectations of what the CDM function can achieve within its remit. The setting of unrealistic or impractical expectations can only result in eventual failure and ultimately a feeling of disillusionment among all parties concerned.

Core Principles

Prior to the establishment of a CDM function the following principles should be adequately considered in advance:

Independence
- The status of the CDM function
- Position of CDM within organisation
- Nomination of Head of CDM function
- Potential conflicts of interest
- Access to information and personnel

Resources
- Adequacy of resources required
- Competency of resources required
- Quality Assurance

Scope
- Activities within scope
- Entities within scope
- Systems within scope
- Jurisdictions within scope

Responsibilities
- Purpose, authority and responsibility
- Degree of advice, collaboration and direction
- Guidance and education expectations
- Identification, assessment and response to corporate defence threats
- Degree of delegation, supervision and direct engagement
- Reporting requirements
- Format of corporate defence program

Relationship with other disciplines
- Framework to be implemented
- Roles and responsibilities of partners
- Delegation and communication mechanisms

Other matters
- Monitoring of CDM function
- Possibility of outsourcing CDM
- Relationship with Audit / Risk committees
- Liaison with regulatory bodies
- International jurisdiction issues

CHARACTERISTICS AND ATTRIBUTES

Taking responsibility for defending people, property and other assets (e.g. information) requires that CDM employees respect and support the ethical philosophy of the organisation. The overriding concern should be to continuously improve service by employing appropriate individuals, and, developing their competence and level of professionalism in order to build trust and confidence in the CDM function throughout the organisation.

Attribute standards address the characteristics of both the organisation itself and the personnel performing the CDM activities. In order to operate in an effective manner, members of the CDM function should possess certain personal characteristics and professional attributes which are considered essential to the performance of their duties and responsibilities.

Core Attributes

The core attributes include the following:

Integrity: Integrity is required in order to create a culture of honesty, high ethics and transparency. It is a prerequisite within the CDM function and is also a necessary component in order to promote trust with fellow partners.

Objectivity: Objectivity is required in order to make balanced decisions based on strictly professional judgement and should not be unduly influenced by personal interests.

Impartiality: Impartiality is required in order to ensure that the parties engaged in CDM activities are sufficiently independent to remain unbiased, and avoid any possible conflicts of interest.

Confidentiality: Confidentiality is required in order to ensure that sensitive information obtained is only disclosed in a prudent manner.

Discretion: Discretion is required in decision making and in the application or exercise of authority.

Competency: Professional competence is required in order to ensure that individuals entrusted with responsibility for CDM possess the appropriate qualifications, skills and experience in order to proficiently perform their duties on an ongoing basis.

Professionalism: Professionalism is required in order to ensure that all activities are performed proficiently and with due professional care in accordance with professional standards.

Diligence: Diligence is required so that individuals develop the discipline and responsibility to work unsupervised and on their own initiative in an honest and professional manner.

Vigilance: Vigilance is required in order to ensure that CDM individuals are constantly attentive in their communication, observation and evaluation, thus fostering the development of a higher level of intuition and perceptual awareness.

Helpfulness: Individuals must respect the role of other disciplines and when required individuals must be prepared to lend help and assistance as part of ongoing efforts to defend the organisation and its stakeholders.

Specific Requirements

The existence of the attributes referred to above in staff participating in the work and activities of CDM function is considered essential for the required and expected functioning of the unit.

The precise attribute requirements should be assessed on a case by case basis taking into account the exact nature and role of the individual position, staff member, and organisation requirement.

Individual organisations should take all necessary measures to ensure that these required attributes are fostered, nurtured and maintained at all times, through periodic, systematic and continuous evaluation and education.

PURPOSE OF CDM

The overall purpose of CDM is to adequately defend the interests of the stakeholders. Defending the interests of the stakeholders means placing due regard on the welfare and wellbeing of these stakeholders, and ensuring that an appropriate duty of care is exercised concerning the health and safety of all of the stakeholders in the long term, and not just focusing on short term interests.

What is required is a long term commitment to stakeholders as valued partners. There must be a concentrated effort to protect and safeguard the stakeholders as human beings, and not purely their financial impact on the bottom line. Such a partnership fosters a reciprocal relationship of mutual trust and commitment.

To achieve this objective, CDM must project its own ideology, an ethos which espouses certain core beliefs which are considered fundamental to it as a discipline. This ethos must advocate a value system which regards moral fibre above the search for short term profit at all costs. Its philosophy must promote not only the aspiration of the highest ethical standards but the practical implementation of these standards. There must be a strong emphasis on the appropriate application of duty and responsibility, and above all, integrity must be at its essence, both individually and collectively.

CDM represents an opportunity to fortify the lower level motivational needs of the organisation (e.g. safety, shelter and security) and balance these long term needs against the relentless pressure to maximise short term profits.

The culture of an organisation can be positively influenced by CDM as it aligns itself to organisational strategy, and helps ensure long term success through the prudent application of corporate defence strategies. CDM can help ensure that the necessary system of checks and balances are operating effectively throughout the organisation, despite possible pressures to focus on short term gain.

CDM: High Level Objectives

The following high level objectives must be set in order to adequately defend the organisation from a multitude of potential hazards.

1. To ensure that appropriate mechanisms are in place to anticipate potential threats and vulnerabilities in advance of occurrence.
2. To ensure appropriate measures are in place to prevent the occurrence of identified threats and vulnerabilities.
3. To ensure appropriate measures are in place to detect the occurrence of activities which indicate potential threats.
4. To ensure that appropriate measures are in place to react in a timely, effective and efficient manner to activities identified as potential threats.

Role of CDM

The role of the CDM function is to help ensure that all defensive related disciplines are operating in unison towards the attainment of a common set of goals and objectives. This management, co-ordination and supervisory role relates to a diverse group of disciplines, and people as individuals, with a diverse set of knowledge and skills. It also relates to diverse processes, systems and technologies.

This difficult challenge requires a flexible strategic approach and a strategic agility which will allow the organisation to quickly adapt to an evolving environment and enable it to react in a speedy and integrated manner to incidents which occur in an ever-changing set of circumstances.

Each organisation will determine the precise model which best suits their needs, addressing issues such as structure, duties and responsibilities of the CDM function. Whether it should be resourced in a centralised or decentralised manner needs to be determined. The degree of participation in the organisations operations can potentially include policy decisions, education, advise, ratification, approval, collaboration and even task implementation.

CDM: OPERATIONAL OBJECTIVES

A CDM function should have the following operational objectives:

(A) Education: To help ensure that appropriate measures are in place so that all members of the organisation are appropriately educated in their ethical and professional responsibilities in relation to corporate defence.

(B) Recognition: To help ensure that there is appropriate recognition within the organisation of the dangers which can result from threats and vulnerabilities, and the resulting obligation to comply with corporate defence protocol.

(C) Identification: To help ensure that all significant threats and vulnerabilities facing the organisation are identified and documented in a timely manner.

(D) Evaluation: To help ensure that the inherent and residual risks represented by the identified threats and vulnerabilities are appropriately assessed and evaluated in terms of impact and probability.

(E) Deterrence: To help ensure that appropriate deterrent measures are put in place to mitigate those threats and vulnerabilities which have been determined to be of a low risk nature.

(F) Protection: To help ensure that appropriate physical and IT protective measures have been taken to secure the organisation and prevent the occurrence of any threats which have been determined to be medium to high risk.

(G) Interception: To help ensure that appropriate security measures are in place to intercept in a timely manner any activities deemed to be of a threatening nature or a breach of protocol.

(H) Resilience: To help ensure that appropriate resilience measures are in place to address threats to the health and safety of staff, destruction of facilities or disruption to the business operations.

(I) Capture: To help ensure that appropriate intelligence processes and systems are in place to capture and collect all required information in relation to potentially threatening activities.

(J) Monitor: To help ensure that appropriate controls are in place for the timely monitoring of information which indicates evidence of the occurrence of potentially threatening activities.

(K) Investigate: To help ensure that appropriate procedures are in place to adequately investigate any possible threatening activities in a timely & comprehensive manner.

(L) Communicate: To help ensure that appropriate mechanisms are in place to effectively communicate threatening activities to all the relevant parties in a timely manner.

(M) Options: To help ensure that appropriate measures are in place in order to identify the best available response options in the event that threatening activities have been identified.

(N) Decision: To help ensure that appropriate measures are in place in order to allow for timely decisions (i.e. tolerate, treat, transfer or terminate) in relation to the most appropriate response to identified threat.

(O) Action: To help ensure that appropriate measures are in place to allow appropriate mitigating action to be taken in a timely response to the identified threat.

(P) Correction: To help ensure that appropriate procedures are in place to obtain assurance that the root cause has been identified and appropriate corrective measures put in place to prevent these events re-occurring in the future.

Note: The most robust organisations will have the highest pre-emptive capabilities in place. It is the reaction times to potentially devastating events which will determine the magnitude of the initial impact and the subsequent collateral damage.

ESTABLISHING AN EFFECTIVE INTEGRATED CDM PROGRAM

A successful and effective integration program should involve understanding of the complex interdependencies and correlations which exist between the various defence related disciplines in order to avoid unnecessary duplication, omission or conflict. Effective enterprise-wide vulnerability and threat management will require co-operation from all of these areas.

CDM Partnership Alliance

Corporate Governance
- Board of Directors
- Audit Committee
- Corporate Responsibility Officer

Corporate Investigations
- Chief Inspection Officer
- Chief Fraud Prevention Officer
- Chief Forensic Officer

Risk Management
- Risk Committees
- Chief Risk Officer
- Operational Risk Officer

Corporate Assurance
- Operations Line Management
- Internal & External Auditors
- Regulator & Rating Agencies

Corporate Compliance
- Compliance Committee
- Compliance Officer / Legal Counsel
- Human Resources

Corporate Controls
- Internal Controls Committee
- Chief Controls Officer
- Financial Controller

CORPORATE DEFENCE MANAGEMENT

Corporate Intelligence
- Intelligence Committees
- Chief Intelligence Officers
- Chief Operations & IT Officers

Corporate Protection
- Health & Safety Officer
- Chief Insurance Officer / Corporate Actuary
- Head of Operations / Facilities

Knowledge Management
- Knowledge Management Committee
- Chief Knowledge Officer
- Chief Operations Officer

Resilience Management
- Resilience Committee
- Chief Resilience Officer
- Chief Operations Officer

Physical Security
- Security Committee
- Chief Security Officer
- Chief Operations Officer

IT Security
- IT Security Committee
- Chief IT Security Officer
- Chief IT Officer

APPROPRIATE ENVIRONMENT

A number of key elements are required in order to create an appropriate environment in which to establish an effective integrated CDM program.

Setting the Tone at the Top

For Corporate Defence Management (CDM) to operate in an effective manner it must first be understood and supported by those at the very top of the organisation. The Board of Directors should approve the establishment of the CDM framework and should also provide their senior management with clear guidance and direction regarding the principles underlying the framework.

Establishing Oversight

Senior Management is a key component of corporate defence in general and therefore should have responsibility for implementing the CDM framework approved by the Board of Directors. They should in turn assume an oversight role with respect to line management and its fulfilment of its corporate defence responsibilities and duties. This needs to be clearly understood from the outset.

Purpose and Vision
The purpose and vision of the CDM function should be sufficiently determined in order to adequately justify the necessity for such a function within the organisation. This vision should clearly outline the organisation's belief in the importance of defending the interests of the stakeholders within the organisation.

Status, Position and Authority
The appropriate status, position and authority of the CDM function should be guaranteed by a documented charter which ideally should be required to be approved by the Executive Committee and confirmed by the Board of Directors. This charter will act as a continuous reference point and will help enhance the standing and authority of the CDM function within the organisation.

Establishing Strategic Objectives
In determining its strategic objectives, care must be taken to ensure that these are aligned to the strategic objectives of the organisation, and its strategy and policies must clearly set out in broader terms how the organisation is hoping to achieve these high level objectives.

Establishing clear lines of responsibility and accountability
The Board of Directors should clearly outline the CDM responsibilities of the Board, and Senior Management. Senior Management should be responsible for establishing and implementing an accountability hierarchy, while being ultimately responsible to the Board for performance of CDM within the organisation.

Utilisation and integration of other disciplines
The precise nature of the relationship with other corporate defence related disciplines will also need to be determined so that it is not seen to be at variance with other disciplines, but rather a mechanism for leveraging and maximising their potential added value to the organisation. The seamless integration with these disciplines is critical to establishing an effective integrated program.

CDM PROGRAM GUIDELINES

Once an appropriate framework has been agreed upon, the next challenge is to successfully implement an integrated CDM program.

Creation of a CDM Committee
A permanent CDM committee should be created in line with the procedure for creating an Audit/Risk Committee or a similar roundtable. The composition, powers and functioning of this committee should be determined in advance and should be documented and approved by the Executive Committee and confirmed by the Board of Directors.

Mission Statement
A clear mission statement should be determined outlining the purpose of the CDM function within the organisation and clearly stating the requirement for its introduction.

Strategy
A CDM strategy should be established which clearly gives direction on how ongoing activities should be conducted in order to achieve its strategic CDM objectives.

Charter
A CDM charter should establish the standards, objectives and scope of the CDM function. In addition it should outline its position, authority, responsibility and accountability. The charter should state the terms and conditions under which the CDM function should operate within the organisation.

Resources
The resources to be provided to the CDM function should be both sufficient and appropriate to perform its duties and responsibilities effectively. CDM function staff should have the necessary qualifications, experience, professional and personal qualities, required to enable them to perform their specific duties. Maintenance and development of professional skills should be facilitated by regular and systematic education and training.

Annual Plan
An annual CDM plan should outline all work to be performed by the function, taking into consideration current activities and expected developments and innovations. This plan should include the nature, timing, frequency and required resources for planned work. The plan should be prepared by the CDM function and approved by the Executive Committee.

Policies, Procedures and Work Programs
The establishment of appropriate policies and procedures requires sufficient determination, development, documentation and approval, before being effectively communicated to all personnel involved in the CDM function. Professional work programs should also be prepared in advance for all work undertaken by the function. Policies and procedures should reflect the seamless integration of all corporate defence related disciplines.

Education Program
The CDM function should assist senior management in educating staff on corporate defence issues. An education program should be introduced to ensure that all staff members have a clear understanding of the purpose of CDM, and their own key role in relation to corporate defence. It is important that the ownership of corporate defence is seen to rest with all the members of the organisation, as the role of its members cannot be under estimated in order to ensure a successful corporate defence program.

Monitoring and Assurance
In addition to monitoring by the CDM committee, the CDM function should be subject to periodic independent reviews by the Internal Audit function.

The above guidelines represent a checklist of issues to be addressed during the implementation phase. Each organisation will be required to adapt these guidelines to best suit the objectives and requirements of that particular organisation.

KEY SUCCESS FACTORS

The Seven Deadly "C"'s

The following key success factors are considered critical to the successful implementation of a CDM program.

Commitment: There must be a sincere commitment to succeed from the very top of the organisation, this includes the Board of Directors and Senior Management.

Confidence: The nomination of responsibility and accountability for CDM must be of a suitable level of authority, seniority and status to inspire confidence in the above commitment.

Competence: The CDM function must possess the appropriate qualifications, experience, skills, attributes, and knowledge, necessary to fulfill its obligations.

Comprehensive: The scope of the CDM function must be comprehensive and include all aspects of the organisation including HO, Branches, Subsidiaries, Business Units, Divisions, and Departments

Co-ordination: Co-ordination of CDM must be from a centralized source whose role is to integrate, align and unite the various defence related disciplines.

Collaboration: The CDM function must collaborate with all defence related disciplines to optimize the experience and expertise possessed within the organisation and help form a partnership to ensure that all partners are operating in unison.

Continuous: The CDM function must be vigilant to ensure that the corporate defence program is operating on an ongoing basis, while continuously evolving and improving.

CROSS FUNCTIONAL CHALLENGES

CDM by its very nature must be considered a cross functional discipline as it seeks to unite a number of other functions within the organisation. This means that the CDM function faces unique challenges as it needs to address the diverse points of view and expectations of several partners, each of which will have their own independent objectives and strategies.

The challenge will be to develop a mechanism to ensure that these diverse functions are in a durable alignment with a common set of objectives and expectations. The CDM function will need to work closely with each of these functions, individually and collectively, to help ensure all are operating in unison.

The partnership alliance must consist of the appropriate positions and individuals within the organisation in order to get the requisite buy-in and support. The importance of "on the ground" involvement and commitment cannot be overly stressed as it is essential to the successful implementation of a corporate defence program.

Clear reporting lines and delegations of authority must be in place from the very outset. Extreme care must be taken to ensure a clear understanding by all, and to avoid any possible misinterpretations or ambiguities. This will enable the required timely decision making by the appropriately delegated individuals.

Sufficient time, effort and resources should be employed in the areas of education and communication, in order to ensure that a clear and consistent message is communicated to all concerns on a timely basis.

A successful corporate defence program requires that all of the partners in the alliance are operating within a framework of collaboration and with a spirit of co-operation.

Corporate Defence Diagnostic

It is recommended that an initial high level corporate defence diagnostic (health-check) be performed at the initial implementation stage of the corporate defence program. This should enable the early identification of existing vulnerabilities and allow for appropriate corrective action to be taken in order to address these vulnerabilities. This exercise will also assist in the prioritisation of work to be performed as part of the annual planning process. This exercise should at a minimum address the following areas:

Culture and Environment
- Directors
- Remuneration and Compensation
- Accountability and Audit
- Relations with Shareholders
- Executive Management Oversight
- Internal Environment and Control Culture

Strategy and Planning
- Strategic Objectives
- Responsibility and Accountability
- Oversight by Line Management
- Strategy and Business Objective setting
- Risk Recognition and Assessment

Business Activities and Operations
- Risk Management
- Compliance Management
- Business Intelligence & Knowledge Management
- Security Management
- Resilience Management
- Control Activities
- Assurance

Information, Communication and Monitoring
- Information and Communication
- Monitoring Activities
- Correction of Deficiencies

Benefits of CDM

The benefits to an organisation of introducing a robust and effective Corporate Defence Management (CDM) program are self-evident and too numerous to give a complete list.

Examples (a baker's dozen) of these benefits include the following:

1. Provides comfort to stakeholders that their interests are being appropriately addressed.
2. Acts as a tangible indication that the Board and Management are taking a proactive approach to corporate defence.
3. Unified management of all defence related domains.
4. Dangers reduced by maintenance of a more robust defence framework.
5. Stakeholder retention through stakeholder focus.
6. Fostering of a culture of collective responsibility.
7. Optimisation of synergies through partnership and integration.
8. Accelerated reaction times to reduce vulnerability.
9. Creation of a resilient enterprise through continuous improvement.
10. Creation of strategic advantage by unlocking latent potential.
11. Keeping pace with growth while still meeting compliance standards.
12. Cost reductions through increased operational efficiencies.
13. Protecting profitability by eliminating potential liability.

CONCLUSION

If we are to accept that this increasingly unpredictable corporate world is filled with uncertainty, then we must also accept that with uncertainty comes both threat and opportunity. Where the greatest threats will eventually come from is as yet unclear, such is the nature of uncertainty in an unpredictable environment, likewise for opportunities. It is the function of corporate strategy to take full advantage of the opportunities which present themselves, but equally to defend the organisation from dangers and threats.

With this in mind common sense alone would suggest that by its very nature corporate defence should be considered an integral part of any corporate strategy, as you simply cannot defend adequately, unless you know what you are defending, and what you are defending against.

Corporate Defence Management (CDM), with the help of advanced technologies, represents a proactive holistic solution to strategically managing corporate defence in a systematic manner. CDM is a mechanism which will enable organisations to integrate and co-ordinate their interrelated defensive activities so that they are functioning in unison, thereby protecting the organisation from potential hazards.

Progressive organisations realise that in order to continue to be successful they simply cannot continue to gamble with their stakeholders interests. Long term success requires mutual commitment and trust between the organisation and all of its stakeholders.

Whether the catalyst for corporate defence to play a more eminent role in corporate strategy will be of a voluntary nature or will be imposed by external parties remains to be seen. One thing however appears to be clear, defending the interests of the all stakeholders is a prerequisite for any future success, and Corporate Defence Management (CDM) is the best available option to achieve this objective.

APPENDIX

The following directory can be used as a reference guide to locate the required information.

The CDM Directory

Levels Questions	Strategic	Management	Operational
Who?	- Board of Directors - CDM Committee	- Reporting Lines - Head of CDM	- Delegated Authority - Per Annual Plan
What?	- Board Responsibilities - Mission Statement - Strategic Objectives	- Management Responsibilities - Annual Plan - Business Objectives	- Operational Accountabilities - Per Annual Plan
Where?	- Charter	- Annual Plan	- Per Annual Plan
When?	- Charter	- Annual Plan	- Per Annual Plan
Why?	- Strategic Objectives - Mission Statement - Charter	- Business Objectives	- Education Program
How?	- Strategy	- CDM Resources - Policies - Technologies	- Procedures - Work Programs - Configurations

About R.I.S.C. International (Ireland)

R.I.S.C. International (Ireland) is a management consultancy firm specializing in corporate defence advise. It's services include:

Risk :- Corporate Risk Management and Governance
Intelligence:- Corporate Intelligence and Investigations
Security:- Corporate Security and Protection
Control:- Corporate Control and Assurance

For further information:

contact - sean.lyons@riscinternational.ie
or
visit - www.riscinternational.ie

Graphics: www.dfx.pt