Caravel

LEADING THE WAY IN PROJECTS

Security Management

Projects

Caravel Group – protecting projects against security threats

THE SPECIALIST FOR LARGE COMPLEX MULTI-DISCIPLINED PROJECTS

Security - a Basic Organisational Need

The concept of security is considered a basic human need, second only after physiological necessities like food and water. For organisations alike, security is of central importance irrespective of the sector they operate in. Technological advances, such as the increased accessibility and portability of data, have further heightened our awareness of security matters and stakeholders demand a high degree of confidence that information is accurate and under strict control.

Issues such as the inadequate protection of data, organisational records and intellectual property rights can become a legal minefield, just like unsecured internet links or inadequate treatment of records.

Managing and controlling the environment within which security threats occur is therefore vital for organisational survival. However, the complexities and risks involved are not for the faint at heart. It requires a comprehensive understanding of the principles and practices of risk management and a thorough knowledge of security aspects.

The controlled environment deals with:

Physical security
– people, property, information

Human behavioural security
– disclosure of knowledge

Information systems security
– management and transfer of information

Caravel is conversant with the intricacies of Security Management Projects and understands
that the security environment has two sides, the internal controlled environment and the external uncontrolled environment.

While security threats come in many guises, they usually involve unauthorised activities, hence the prevalence of authentication processes to confirm people's identity.

Caravel has carried out many projects that have security as the dominant motivator. We have also extensive experience in safety critical projects that have security oriented sub-projects embedded within them.

Examples of Security Management Projects:

- An ICT project aimed at improving the information security at the perimeters of a banking system.
- The deployment of a train safety system which gathers information that has to be forensically defensible in courts of law. An embedded security sub-project may deal with security risk assessment, special business process design etc. to ensure the forensic defensibility of the data.
- Building a new data centre; physical, human and information security requirements have to be determined and met.

Basic parameters

Security Management Projects are often subsets of projects targeting other criteria and can occur almost anywhere. While they are often associated with government departments, the finance sector and defense organisations, they are equally commonplace in the health industry, in commercial enterprises and elsewhere, often involving business-to-business relationships.

Organisations involved in process outsourcing (e.g. call centres), third-party transaction services (e.g. billpay) or e-commerce are typically exposed to a variety of security threats that have to be evaluated and treated as a matter of course.

Fundamentally, Security Management Projects involve a system that is vital for the organisation insofar as its failure may potentially result in:

- Purposeful or inadvertent **disclosure** of information to unauthorised parties
- Purposeful or inadvertent **corruption** of information
- **Loss** or **deletion** of information
- Purposeful or inadvertent **falsification** of information
- **Denial of access** to information
- Loss of information **identity links**

Please note that this brochure should be read in conjunction with our brochure on Safety Critical Projects which extensively covers the treatment of risks.

Security Management Projects are often found as embedded sub-projects of other types of projects.

Maintaining integrity

Organisations often rise and fall on the strength of their integrity and the level of confidence they inspire in their stakeholders. Ensuring accuracy and control of information is absolutely vital in this respect.

Systems therefore have to integrate a variety of diverse factors such as hard copy, Enterprise Content Management, local datastores, Storage Area Networks, Network Area Storage, Wide Area Networks, overseas service providers, specialist management centres such as Call Centres and more.

In addition, organisations have to comply with regulatory demands. Systems and processes must meet local legislation and the owning country's legislation for all overseas of interstate deployed capabilities. Similarly, privacy laws stipulate that information held about people must be available to them to be reviewed, updated or deleted, depending on the situation.

Complexities of the project environment

Security Orientated Projects typically operate in a pronounced multi-faceted environment. This further compounds the level of complexities that the project manager encounters.

- Projects usually feature a significant ICT or technology component (eg CCTV, trusted computing environments, alarm systems, physical security perimeters)
- Underlying business processes are exposed to incidents of human error and corruption
- The involvement of third parties in overseas locations
- Shared or multi-tenanted environments such as call centre outsourcers or credit card processing centres
- The secure reconciliation of all forms of data and data handling systems, including hard copy filing
- Balancing cost vs risk – how much is enough?
- Threats, such as Spyware, viruses and worms, often evolve over time and place high demands on all aspects of the security system to ensure that it is up-to-date
- The need for increased connectivity between customers and suppliers has accelerated the trend towards just-in-time models and quasi real time processing
- Business practices of the connected world (hedging, spot pricing of resources etc) have lead to global integration of systems with common data which may be inadequately secured

Security

Management Matters

Standards and methodologies

Safety and security risk assessments have a number of associated standards and methodologies that guide projects carried out within this environment.

- AS/NZS ISO/IEC 27001:2006 Information Security Management
- Common Criteria for trusted computing systems
- Industry compliance standards such as Sarbanes/Oxley (USA)
- Technical standards govern PIN numbers, codification schemas and the like
- Encryption techniques incorporating public and private key system standards are employed to prevent intelligible access to data
- Authentication systems are used to ascertain legitimate users to perform authorised activities

Assessing the risk

The ability to perform accurate security risk assessments is prerequisite for any Security Management Project and cannot be overstated.

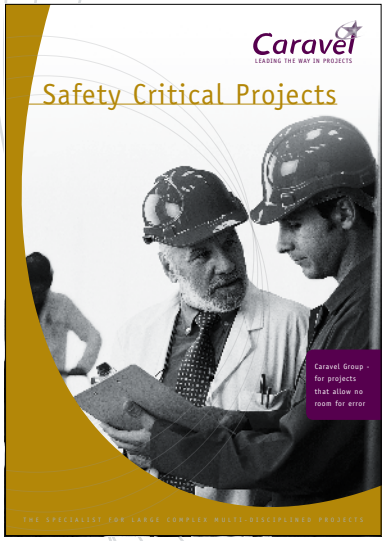
Important concepts that govern the assessment and control of security risks are extensively outlined in our brochure on Safety Critical Projects. While the risks being considered may be different, the approach is fundamentally the same.

Concepts such as safety layers – preventative and defensive barriers designed to prevent or mitigate accidents – apply to the safety critical and security management environment alike.

A key issue is the adequate treatment of risks to ensure that threats are “as low as reasonably practicable” (ALARP). This plays a key role in determining to what extent security risks have to be treated. It also ensures that the security risks are being treated in a manner consistent with the probability of occurrence and the consequence of the risk occurring. This provides a documented, structured approach that helps satisfy legal liabilities and ensures forensic defensibility of the implemented solution.

The process of independent verification and validation (IV & V) also extends into the security arena. It ensures that the right system is built, and that it is built the right way.

Further Reading



The need for checks and balances

News media regularly report prominent incidents of malicious data use involving hacking, industrial espionage, trading scams and similar occurrences. In recent notorious cases single rogue traders have brought merchant banks to their knees.

The impact of such activities is often drastic and long-lasting as far as an organisation’s reputation is concerned.

While deployed systems usually undergo a thorough systems design activity, it is unlikely that they are subjected to a security risk assessment to determine the most appropriate risk controls to be implemented.

Caravel's Solution

Adopting a proven Change Management approach

Security management projects usually involve changes to the existing operating environment. This represents substantial changes for an organisation as these changes have to be addressed throughout the business:

new system → new business processes → new maintenance systems → new management reporting → new/updated ICT systems

This is often represented as the transition from the current Business-as-Usual mode of operation to the future Business-as-Usual mode of operation of the organisation. Depending on the complexity of the change, it is likely that there may also be a transitional phase as new systems or processes are gradually brought into operation.

While these steps reflect the security management project, they in fact represent a special case of a change management project and therefore need to address change management aspects such as:

- Organisational readiness for change
- Operator training, maintenance personnel training
- Spares and logistics
- Disaster Recovery
- Business Continuity
- Assessment of security measures impacts

Project security vs Operational security

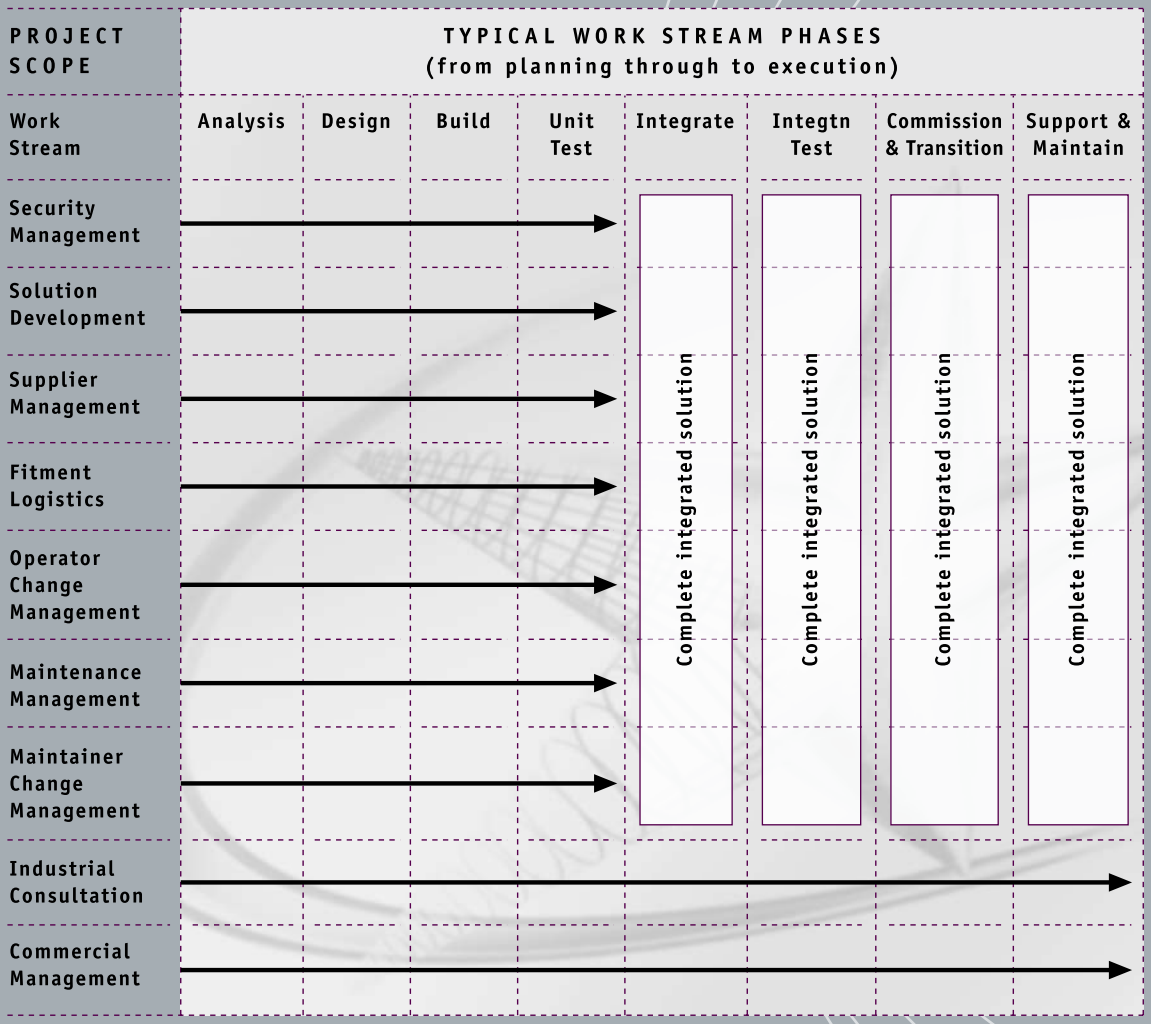
Project security risks affect the organisation while the project is underway. This applies in particular during the commissioning of the project solution or its transition into service. Risks can arise from latent systems defects or from negative human activity such as the installation of Trojan malware.

Operational security risks arise from the use of the target technology solution for business-as-usual operation.

The Caravel Methodology

The Caravel methodology draws upon the proven change management approach that has been successfully deployed on numerous projects including those with specific or derived security aspects. The change management approach is defined in our Change Implementation brochure.

THE CARAVEL METHODOLOGY



Each work stream will include some or all of the following considerations:

- Security management solution encompassing the full context of the security environment (physical, information, personnel, systems)
- Security engineering and compliance requirements – particularly where B2B, C2B or privacy aspects must be considered (eg banking and finance)
- Project planning, monitoring and control, organisational interface management throughout the programme of works
- Solution specification and development with the security management requirements integrated into the procurement or system specifications
- Disaster recovery and Business Continuity – both during project execution and after implementation
- Supplier solution procurement and management
- Installation, logistics management, testing and quality assurance during deployment
- IV&V and Quality Assurance processes
- Operational systems change management including business process development or change where required
- Maintenance management solution
- Organisation change management including training, recruitment, industrials etc for both operators and maintainers
- Commissioning and transition support management
- Post commissioning there may be a need to establish a new governance arrangement and put in place a new operations and maintenance manual to support the solution

When Caravel starts work on a Security Orientated Project, we initially assess the overall needs of the project and address a number of key points:

1. What skills and resources are required to support the project?

2. Where should those skills and resources come from?

3. How should we work together? Do we buddy up with client resources to provide the detail knowledge, skills transfer and continuity after the project?

4. Assess the project solution technical requirements, scope & schedule.

5. Assess the project organisational interface management requirements.

6. Assess the operational and organisational change management requirements for both operators and maintainers alike. Are there any new business processes to be defined?

7. Is the organisation ready for change? The benefits from the Security Orientated Project may be significantly reduced if the organisation cannot cope with the proposed changes.

8. Security is integral to any project – the security project is in practice a subset of the larger organisation change process. We are experts in both.

9. We separate the physical security aspects, data security etc with respect to how these integrate in a project. We do this in our document control plan where we nominate the drive version as the master, hard copy as the slave and the security aspects based on client network security etc. We may develop this further in a workshop and explore some practicalities in the application of a security management project.

Our Services includes:

- Understanding of the need and balance to be struck
- In-Scope
- Out of Scope
- Facilitation of risk modeling
- Workshop facilitation
- Management of subject matter specialists (security experts, legal and financial advice etc.)
- Specialist partners

Please refer to Caravel's related brochures:

- Change Implementation
- Strategic Management of Projects
- Business Process Innovation
- Enterprise Management Solutions
- Project Assurance
- Operational Management Centres
- Safety Critical Projects

Caravel
LEADING THE WAY IN PROJECTS

Caravel's range of project services

As a leader in projects, Caravel offers a range of specialised consultative and implementation services that span the entire life cycle of a project from inception, through implementation to final hand-over. Caravel adds value at every point along the way through project management services for:

Strategic Management of Projects
Core services include:
- Multi-project Management
- Organisational Resource Management
- Value Management
- Project Feasibility Studies
- Critical Chain Modelling
- Organisational Project Management Maturity Assessment

Project Assurance
Core services include:
- Project Governance
- Project Audits
- Project Health Checks
- Recovering Troubled Projects
- Project Risk Assessments
- Post-implementation Review
- Mentoring and Training

Project Planning and Execution
Change Implementation
Business Process Innovation
Business Partnering
Enterprise Management Solutions

Operational Management Centres
Core services include:
- Customer Contact Centres
- Service Management Centres
- Operational Control Centres
- Mission Critical Moves

Safety Critical Projects
Bid and Tender Management
P³MO™ Project Management Office (PMO)
Security Management Projects

Caravel can tailor a range of industry-specific services to suit the exact needs of your organisation.

Please refer to our website for your nearest Caravel office: www.caravelgroup.com