

Risk Management

Table of Contents

1	INTRODUCTION.....	2
1.1	AUDIENCE	2
1.2	CONTRIBUTORS	2
1.3	SECTION STRUCTURE	2
2	DEFINITIONS	3
3	RISK MANAGEMENT RESPONSIBILITIES.....	4
3.1	ROLES	4
3.2	RISK REPORTING.....	4
3.3	POINTS FOR CONSIDERATION.....	4
4	RISK MANAGEMENT LEVELS	6
	APPENDIX A RISK CATALOGUE	8
	APPENDIX B RISKS IN MANAGING THIRD PARTIES.....	12

1 Introduction

This paper expands on the risk management section of DSDM. It is not a replacement for that section or any other risk-related material within the framework, but is intended to complement and supplement the manual.

1.1 Audience

The paper is intended to be read by anyone concerned with the safe management of one or more DSDM projects. This includes the Project Manager, Team Leader, and Visionary roles together with any member of a DSDM project governing body such as a project board or steering committee.

1.2 Contributors

This White Paper was originally put together by Jennifer Stapleton, Independent Consultant, Karl Whittle of Phoenix Database Limited, David Tuffs of Warburg Dillon Read and Barbara Roberts, Independent Consultant.

Ideas were collected for additional material during a National User Group meeting and review comments from the Technical Work Group have been incorporated.

The paper was updated for conformance with DSDM V.4.1 in 2003 by Jennifer Stapleton.
Note: Much of the original paper is now part of the standard content of DSDM.

1.3 Section Structure

Section 2 defines some risk management terms that are used throughout the White Paper.

Section 3 defines the key responsibilities for risk management activities within a project team.

Section 4 defines an approach to managing risk at two levels: the project level and the timebox level - macro and micro risk management.

Appendix A contains a risk catalogue that can assist in risk identification in any DSDM project.

Appendix B contains a catalogue of risk related items for consideration when DSDM development is outsourced.

2 Definitions

A **risk** is something that may happen in the future that will adversely affect either the way a project is expected to proceed or its outcome.

The purpose of **risk management** is to actively control all the risks facing a project or the implementation of the solution it is delivering. This includes:

- Identification of any and all risks that may threaten the project for business, systems or technical reasons (see section 4.2 on categories of risk).
- Assessment of the impact of those risks on the success of the project should they arise. This assessment involves deciding on the likelihood of the risk occurring and if it does on the severity of its impact on the project.
- Management of those risks through defining specific countermeasures that are aimed at either avoiding the identified risks or accepting them and minimising their detrimental effect on the project.
- Applying the appropriate countermeasures when a risk materialises.

The **level** of a particular risk is calculated as follows:

Level of risk = likelihood of occurrence x severity of impact

where likelihood and severity are defined as high, medium or low (for calculation purposes use 3, 2 or 1 respectively).

A **countermeasure** is a defined response to a given risk or set of risks. A countermeasure can be one of the following:

- Risk avoidance: eliminating the risk by eliminating the source of the risk.
- Risk reduction: reducing the probability of the risk occurring or the impact if it does occur.
- Risk acceptance: accepting that if the risk occurs the project will take a different course and defining that course. This is basically a conscious decision to take no action.
- Transfer: transferring all or part of the risk to another party. The probability and impact remain the same but their management is now someone else's problem.

3 Risk management responsibilities

3.1 Roles

- The Project Manager prepares and maintains the Risk Log throughout the project. This is done in collaboration with the Executive Sponsor, Visionary, Technical Co-ordinator and Team Leader roles.
- The Project Manager plans countermeasures. This should be done jointly with the owner of the risk. The "owner" can be a group of individuals within the business or the IT/IS organisation, but one person should be the "risk manager" for each risk. The risk manager is someone within the project team who is responsible for monitoring the risk and calling for action as necessary.
- The treatment of key risks must be reviewed and approved by the Executive Sponsor, Visionary, Technical Co-ordinator and any steering committee or project board.
- The Team Leader(s) create and maintain "mini" Risk Logs for each timebox.

3.2 Risk reporting

Reporting good news seldom causes any problems within any project but, even in the no blame culture of a DSDM project, reporting bad news often does. If the framework is being applied correctly, there should be no secrets in a DSDM project but it can be very attractive to anyone involved in managing a project to attempt to keep the bad news within the confines of the core project team. However, the aim at all times should be to be open about risk identification, assessment and reporting.

At the timebox level, the daily meetings should highlight risks as they occur, such as an Ambassador User not being able to undertake testing or review activities at the time expected within the timebox because of pressures from the business. The timebox team leader should report immediately to the Project Manager on any areas which will either affect the success of the timebox or will have an impact outside the timebox.

It is the Project Manager's responsibility to report on risks as they arise to the Visionary and/or the Executive Sponsor, depending on their severity of impact on the overall success of the project. This channel of communication needs to be open always so that risks are not allowed to grow.

In all projects except the very small, the top five to ten risks list should be reported on regularly by the Project Manager to senior management, such as the Executive Sponsor, Visionary and any programme or project steering committee.

For large, formally controlled projects, a Risk Management Plan provides a key tool for reporting risk against.

3.3 Points for Consideration

Projects that are very short indeed have increased risks in the ability to deliver on time if they are substantial in content and the ability to prioritise requirements is low. Normally

in a DSDM project, tight timescales are not considered a risk, but in these projects, it is worth spending time considering what will inhibit the delivery target.

Conversely projects that are very long have an increased risk that the original business vision and associated benefits will be lost or watered down over many incremental deliveries. The project will gain a life of its own. In these projects, the Project Manager should ensure that the risk assessment focuses on achievement of business benefit.

Two of the biggest sources of failures on projects are:

- Projects being affected by unforeseen risks;
- Risks not being addressed because Project Managers assume that the risks will be resolved without action.

The first source of failure can be avoided by specifically addressing risk in a workshop, since as many views as possible will be present. The focus of the workshop should be on the most likely risks with medium or high severity of impact. It can be very dreary and demotivating to consider minor risks that are unlikely to happen or even risks that will have significant impact but are extremely unlikely.

Because the time between deliveries of operational software is short on DSDM project, the second source of failure should not appear if risk management is considered a vital part of the Project Manager's role. The Project Manager should identify key de-commit criteria and fallback scenarios for the project if high-level risks should materialise. If they do, then the Project Manager should implement the strategy rather than hoping that it will turn out all right in the end. For a fallback scenario to be valid it should have an expiry date after which it cannot be implemented. Similarly, de-commit criteria should be defined in a clear and measurable way.

Project Managers should not use the Risk Log as a set of excuses for poor project performance. It is simply a tool to avoid such poor performance.

If any important lessons are learnt during the project with respect to risk management these should be fed into the organisational pool via a feedback mechanism, such as the Project and Increment Review Documents, or another method that is either standard to the organisation or that has been defined at the start of the project.

4 Risk management levels

To ensure that all risks are identified and addressed effectively by the right people, there needs to be two levels of risk management: at the project level and at the timebox level.

Project level

Project level risk management applies to all risk management activities, which are not related to a specific timebox. These include assessing the project against the Suitability/Risk List at the outset of the project and at the end of the Business Study, running workshops to assess the possibilities, which could cause the business benefits not to be achieved, and ongoing monitoring and reviewing of the risks.

The Risk Log is where project level risks are recorded and used by the project manager to monitor the ongoing risks to the project. The project manager monitors the contents of the Risk Log regularly. Its contents should be formally checked at least

- on a weekly basis
- at the outset of a timebox and at the end of a timebox
- at the end of an increment, i.e. when software has been delivered into the operational environment.

At the end of an increment, the Risk Log should be carefully considered to see whether any of the risks in it are relevant to any of the expected future increments. If they are not, they should be removed and any new risks relating to the imminent increment should be added.

By the end of the project, all risks must have been contained or avoided.

Timebox level

At the start of a timebox, the project manager delegates monitoring and control to the timebox team leader any risks in the Risk Log that are relevant to the timebox team, activities and deliverables.

Inside each timebox, the team leader responsible for the work within the timebox should keep a mini risk register of the risks to the activities within the timebox (starting with the delegated risks from the Risk Log). While the timebox leader is the nominated risk controller, every member of the timebox team shares the responsibility for ensuring that risks are identified and recorded in the mini risk register and are monitored effectively. The timebox risks should be considered on a daily basis at the daily team meetings.

At the end of each timebox, the timebox team should agree whether or not the risks in the mini risk register are closed or not. There are two ways that a timebox risk can be closed:

1. It has been dealt with by the timebox team and is no longer a risk
2. It was only relevant to the activities within the timebox and therefore is now redundant.

If any risk on the mini risk register is not able to be closed at the end of the timebox and will therefore affect the work in other timeboxes then it should be passed up to the project

level risk management and recorded in the Risk Log. Similarly, if during a timebox, the timebox team identifies a risk that is obviously beyond the scope of the timebox it is immediately escalated to the project level with the agreement of the project manager.

Appendix A Risk Catalogue

This appendix provides a catalogue of risks that should assist in the process of risk identification. Since DSDM is all about delivering systems that the business needs at the right time, the focus of the risks listed here is on risks that will endanger the proposed delivery date(s). Many of the risks covered here are special cases of inability to satisfy the DSDM critical success factors and of weak application of the nine principles.

General schedule risks

- The schedule has been dictated by the customer or senior management rather than produced collaboratively
- The schedule is optimistic rather than realistic
- The schedule is based on particular staff being available and they are not
- The Must Haves represent too much of the estimated effort so there is no room for manoeuvre
- The original effort estimates and guaranteed delivery dates were based on too limited an understanding of the system and are now "set in concrete"
- The delivery dates are moved nearer to the present time without the scope being decreased or the prioritisation renegotiated
- A delay in one task causes cascading delays in dependent tasks
- Unfamiliar areas cause take more time than originally envisaged

Organisation risks

- It is discovered during the project that key business roles are held by inappropriate people, e.g. an Ambassador User is not as able to make key decisions as originally expected or the Executive Sponsor does not occupy the management position needed for coverage of all business areas
- The project manager is a new project manager and has no mentoring support
- The project manager is experienced but is new to DSDM and has no mentoring support
- The Ambassador Users are not as available as initially agreed
- Developers have unexpectedly onerous support and maintenance duties concurrent with their development activities
- Cutbacks in contractor headcount reduce the project team size
- The management review cycle is longer than initially agreed
- Infrastructure staff (e.g. network support) have not bought into the project

Development environment

- The development area is crowded, noisy or disruptive

- The facilities required by the project are not in place, e.g. video conferencing, external email, project server
- Development tools are not in place at the required time
- The tools used on the project are dictated by organisational standards rather than chosen for their suitability to the project
- A development tool that is new to the organisation is used
- A new version of a development tool is used
- There is poor/no tool support for configuration management
- The techniques used on the project are dictated by organisational standards rather than chosen for their suitability to the project

Customer

- Customer insists on new requirements without renegotiating the priorities of existing requirements
- The Executive Sponsor or Visionary have expectations for development speed that are unrealistic
- Ambassador Users and Advisor Users do not participate in prototyping sessions at the agreed times
- Ambassador Users and Advisor Users do not participate in reviews/testing at the agreed times
- Key customers *persistently* do not attend facilitated workshops as agreed or arrive late or leave early
- Insufficient coverage of all relevant business areas is provided by the Ambassador Users and Advisor Users
- Ambassador Users are not allowed the time by their managers to visit other parts of the business, e.g. other sites where key users work
- Ambassador Users, etc. are uncomfortable with "accepting" partial work
- Advisor Users have not bought into the project

Third party sub-contractors

- Contractors do not deliver when promised
- Contractors are geographically very distant, e.g. India
- Contractor deliverables are not of the required quality

Software deliverables

- All classes of testing are not addressed as soon as possible, resulting in error-prone software requiring more design, implementation and testing work to be done than originally scheduled

- Development of the unnecessary, extra functionality leads to important functionality being squeezed out
- Meeting the key non-functional requirements (e.g. performance) takes longer than expected
- Operation in an unfamiliar software environment causes unforeseen problems
- Operation in an unfamiliar hardware environment causes unforeseen problems
- Dependence on other projects which run late brings unexpected delay

External constraints

- The deliverables are based on government (or similar) regulations which change unexpectedly
- The deliverables are based on technical standards which change unexpectedly

People

- Training for project staff (user and developer) is not available when needed
- There is insufficient time in the project schedule for familiarisation with new software
- There is insufficient time in the project schedule for familiarisation with new hardware
- Key developers are delayed on previous project work which is delayed
- Team members do not buy into DSDM and keep to their old ways
- Team members do not buy into the project and so do not perform at their best
- People with critical skills cannot be found
- The staff most qualified for the work are not available to work on the project
- The staff most qualified for the work are not available to provide part-time support to the project
- Hiring contract staff takes longer than expected
- Contract staff leave before the project is complete
- Team members do not work together efficiently
- Problem team members are not removed from the team promptly, damaging overall team motivation
- There are insufficient development staff available for the project
- There is insufficient time available from business staff
- Staff work slower than expected

Design and implementation

- A too simple design fails to address important issues
- A too complicated design leads to unnecessary work in building the system
- The programming language chosen inhibits prototyping
- The programming language chosen slows down coding
- The selected code or class libraries are of poor quality necessitating more testing work than expected
- Schedule savings from code generators, etc. are over-estimated

Controls

- An agreed, published approach to timeboxes is not present, leading to developers and Ambassador Users "reinventing the wheel"
- The organisational standards for paperwork slow down progress
- Daily meetings are seen as an overhead and are not held, leading to poor communication and rework
- Quality control activities are short cut in the early stages leading to more work later
- Testing activities are not sufficiently monitored and controlled leading to testing being squeezed out until late in the project
- Testing activities are too closely monitored and controlled leading to unnecessary overheads
- Lack of adherence to software policies and standards leads to quality problems
- Bureaucratic adherence to software policies and standards leads to unnecessary overheads
- Poor configuration management leads to unnecessary work in stabilising and baselining products
- Poor risk management leads to major project risks not being identified
- Risk management takes more time than expected

Appendix B Risks in managing third parties

This appendix provides ideas for risks to consider when third parties are involved in a DSDM project and identifies some potential new roles to cover specific risks.

General Risks

- The culture of the supplier and customer organisations – do they have the DSDM mentality, processes and training in place?
- Non-agile supplier for an agile project
- Separate suppliers who have no contact with one another (possibly for legal reasons)
- Use of remote suppliers – either because of cheaper resources or specific resource skills elsewhere, for instance, offshore or elsewhere in UK
- Virtual internal teams (internationally within an organisation e.g. UK /Japan)
- Virtual teams from the supplier (e.g. home workers)
- Dual project managers (no clear responsibility)

Customer Risks

- Are the requirements sufficiently well understood to be communicated to a third party while still flexible enough for the DSDM approach?
- The quality of the Invitation to Tender (ITT) in terms of its accuracy and completeness.
- Will it be necessary to build in time for the learning process on the part of the proposed Ambassador Users, etc.?
- Lack of knowledge/trust in contractual relationships for DSDM projects, especially during the ITT/Proposal negotiations
- Maintaining trust – each ITT/Proposal cycle may be treated in isolation, producing problems in building up an on-going relationship
- Getting the supplier in early enough. (Some customers buy in consultants to write their requirements for them, and have already invested time and money. Suggesting a Business Study to clarify requirements can be very difficult even though the supplier may feel that the requirements are less than adequate. There are fewer risks to a DSDM approach if the involvement starts, at latest, immediately after Feasibility Study.)

What Customers should ask for from DSDM Suppliers

- Staff with Certified Practitioner status– but this is only appropriate if the customer is aware of DSDM. If the IT/IS department is the customer, they may be more aware of DSDM, although this is not necessarily true.

- Specifying DSDM (as oppose to a generic agile approach) offers a common starting point, with training available to bring all parties up to the same understanding. Suppliers wishing to use a DSDM approach may provide DSDM Awareness training to the customer.
- How do they handle Configuration Management? This provides a good indication of supplier's maturity. Question supplier on how they would roll back (cf. Principle 6)
- Use the section in the manual on paths through the lifecycle to assess the nearness of the supplier's proposed approach to DSDM. Potentially disqualify those who do not bring out the key points for differentiation between waterfall development and DSDM.

How to measure success

- Customers don't actually care about DSDM – what they want is software that works, meets the business objectives and is delivered on time and within budget. Reference sites may be a useful measure of previous success. This will help to mitigate the risk of an inexperienced supplier (in DSDM) and to raise confidence.
- DSDM's formality helps. In particular having a list of products with pre-defined quality criteria gives customers an effective way of judging success and direction as an on-going process. It also helps set the scene for what is going to happen. This will help to mitigate the risk of the project drifting off track and not providing the relevant products.
- Monitor the closeness to DSDM as the project progresses. This too will help to mitigate the risk of the project drifting off track and not providing the relevant products.

Risks related to Contracts

- Choose a contractual arrangement that will fit with least risk to DSDM. Wherever possible use the DSDM contract template (available from the DSDM website) as a starting point.
- The legal staff in both the customer and supplier organisations need an awareness of DSDM, as it is contrary to the more usual contract. A contract which has been drawn up with a "waterfall mindset" will be counter-productive.
- Mitigate the risks of the costing being wrong via the contractual arrangement. For instance, issue a Fixed Price contract for the Business Study, with a ballpark figure (or best guesstimate) for the rest of development. After the Business Study, the ballpark figure can be re-estimated and become a Fixed Price for rest of development through to Implementation, if only one or two increments are envisaged. Beyond a couple of increments, accept a ball park figure for the later work. A potential problem could be that work has to be re-tendered after the Business Study. Suppliers cannot give any sort of Fixed Price estimate for the full project until Business Study is complete – but customers often ask for this, even though it means that they may well pay heavily through contingency which the supplier will build in to cover their own risks.

- There must be a clear definition of requirements out of the Business Study or the ensuing work will be poorly defined and the supplier/customer relationship could deteriorate.
- Specifying measures of success/completion is difficult contractually. ‘Works to user satisfaction’ is the right culture, but difficult to measure. Once a project resorts to the small print of a contract it has failed, but there still needs to be definition of SMART objectives, i.e. Specific, Measurable, Achievable, Realistic and Time-related. The MoSCoW rules will help, or specifying the ability to carry out business functions. The contract should not be tied back to a requirements specification, otherwise Change Control becomes a weapon and hinders the collaborative nature of DSDM.
- It is necessary to clarify that there may be technical requirements that are high on the MoSCoW list as well as the business ones. If this is not done, there is a risk that the technical requirements will be driven underground and will surface later to endanger the project. This is a key area where the collaborative nature of DSDM should rely on the technical knowledge and competence of the supplier - rather than viewing the supplier as an organisation with its own quite separate agenda.
- On any customer/supplier project, change control must be handled more formally. This can endanger the collaborative nature of DSDM if it is not recognised that changes can be negative as well as positive, i.e. some changes will mean less work, not more.
- If early process investigation during the Business Study (and possibly within the Functional Model Iteration) negates the project, there is a risk that the supplier will not be paid for the work to date. This can be handled through building staged payments into the contract otherwise the longer term customer/supplier relationship will be endangered.
- Ownership of the IPR for collaborative ideas can be a source of problems. It should be discussed during the set up of the contract and the ground rules put in place.

Who checks the Suitability/Risk List?

- Ideally the Customer and Supplier should complete it together. They may complete it separately and then validate any grey areas with each other either during the bid process or as part of the Business Study, depending on the maturity of the customer/supplier relationship.
- The Project Manager must validate it, if he/she didn’t complete it. If the Suitability/Risk List Filter indicates that DSDM is the wrong approach, the contract should allow for de-commit criteria to be applied and an alternative approach to be used. (This is similar to the estimate; it is the PM who is responsible for the successful delivery of the project.)

Potential Additional Roles and Responsibilities for Risk Management

- Supplier Liaison: this role may be needed if remote/offshore teams are part of the project. Care needs to be taken with this role to ensure that barriers are not placed between the supplier and the customer.

- Co-ordinator of Interfaces: someone to manage the interfaces outside the teams control (this includes people/business interfaces as opposed to the technical interfaces which should be assigned to the Technical Co-ordinator)
- Configuration Manager/Co-ordinator: where CM is applied across several sites or organisations.