# Quick Guide to Disaster Recovery Planning

This quick reference guide provides an introductory overview of the key principles and issues involved in IT related disaster recovery planning, including needs evaluation, goals, objectives and related parameters. The whitepaper also includes a glossary of key disaster recovery planning terms.

## Table of Contents

*The disaster recovery planning process must begin with an accurate assessment of individual goals, requirements and capabilities. This balanced assessment is essential to process success, providing direction and scope. To ensure required results, this process must take an even-handed approach, combining goals, requirements and capabilities into a complete picture of* ***disaster recovery needs****.*

## STEP 1: DEFINE THE NEED AND VISION

Disaster recovery planning exists as both an independent management exercise and an ongoing business activity. Assuming that no current plan exists, the initial work effort will be significant, involving extensive planning and careful analysis. But beyond these initial efforts, disaster recovery planning is also an ongoing management process, subject to continual verification and review as business needs change and technology develops.

Therefore, as you embark upon on your individual planning initiative, you must sort out, identify and clarify all essential goals and objectives, to ensure that your current mission is clearly defined and fully aligned with the IT management vision.

As initial planning goals and objectives are established, three key questions must be addressed. These questions will help you set process direction, and establish your process "starting point".

### Goals and Objectives

**What are you trying to accomplish?**

The driving purpose behind any disaster recovery planning initiative will become clear as you consider your current state of readiness, coupled with past crisis management performance, and any related strategic directives:

- þ Do you need to create a "first-time" disaster recovery program?
- þ Do you need to modify existing disaster recovery plans in response to business or technology changes?
- þ Do you need to verify existing plan validity and effectiveness?

## Information for Analysis

**Do you have all of the preliminary information necessary to begin your planning efforts?**

There is a direct correlation between disaster recovery planning success, and the related quality, and quantity, of available information needed to establish goals and objectives. To provide tangible value, disaster recovery plans and solutions must be based on vetted, corroborated business and technical data. As the process begins, all available information must be collected, organized and evaluated to identify and evaluate any "information quality gaps":

**What type of information is available to you as you begin your planning efforts……..?**

- þ Do you have access to all current hardware & software inventories?
- þ Are you aware of all business needs and priorities?
- þ Do you understand how current systems are being used?
- þ Do you have access to existing outage impact data?
- þ Do you have access to all existing Service Level Agreements and Vendor Contracts?
- þ Do you have access to all existing technical and procedural documentation?

**Based on the availability of this preliminary planning information, how will you begin your planning efforts?**

Information quality and availability will determine the starting point for your planning process. Depending upon the information available, and the degree to which planning needs are filled, your planning process may begin at either one of the following points:

- þ Data Collection: To gather the data needed for disaster recovery needs analysis. Data collection will involve systems inventories, interviews with end-users, the creation of systems documentation, and the review of problem records to determine past outage consequences.

þ Data Organization: To organize all available data and information into a useful structure for efficient review and analysis.

Having established this framework for further analysis and action, your next step is to identify and evaluate specific technical and business requirements.

## STEP 2: IDENTIFY THE REQUIREMENTS.

How well do you know your technical environment and related business requirements? Disaster recovery requirements are defined by both logical and physical elements, forming the basis for business continuity, asset protection and life safety practices. These requirements are comprised of three primary elements:

þ Technology Requirements

þ IT Operational Requirements

þ Business Impact Analysis

### Technology Requirements

In order to identify the essential technology requirements for your disaster recovery program, you must be fully aware of the types of systems in use, their intended function and value to the organization, as well as their physical location and current configuration.

þ What types of systems are currently in place?

þ How are these systems configured?

þ Where are these systems located?

þ What role do these systems play in business operations (i.e. how are they used, by whom, and for what purpose)?

þ Which systems can be deemed critical and essential to business continuity?

### Operational Requirements

IT operational requirements relate to the services provided by the internal (or outsourced) technology support organization. Going beyond daily operations, IT services play a key role in business resumption. Technical services (both support and strategic planning) are essential to disaster recovery, covering analysis, product selection, design, configuration, policy development and problem resolution.

- þ What types of services does IT provide to the organization?
- þ What role do these services play in the disaster recovery and business resumption process?
- þ How will IT services be maintained during a disaster event, considering the number of resources required, resource contact procedures, and specific technical and management skills required?
- þ Will external or temporary resources be required to maintain IT support services during a disaster condition?
- þ If IT operations are decentralized, will recovery plans and activities be consolidated and coordinated, or will separate plans be maintained?

The goal of the business impact analysis is to evaluate the consequences that technology related disasters can bring.  In order to complete this assessment, the *dots must be connected* between **mission critical**[1] business operations, and the corresponding technology dependencies.

This impact analysis can be summarized in four questions:

- þ How does your business/organization operate?
- þ What are the most critical business and technical operations?
- þ What are the most critical job functions?
- þ How is technology used to support these critical operations and job functions?

Using this information as an analytical foundation, you can then move on to the related "**what-if analysis**".   There are three primary factors in the "what-if" process: **consequences**, **time** and **tangibles**.

[1] Mission critical systems typically include those that generate revenue, provide customer service, maintain cash flow and financials, maintain unique data, provide security and/or meet regulatory requirements.

**Considering Consequences**: If a technology disaster event were to occur, how would the business be impacted in terms of ____________________?

- þ The ability to continue key business operations?
- þ The ability to maintain sufficient operational revenues and profits?
- þ The ability to achieve business objectives?
- þ The ability to meet long term revenue objectives?
- þ The ability to maintain budgets and control expenses?
- þ The ability to comply with contractual obligations?
- þ The ability to comply with regulatory requirements?
- þ The ability to serve customers?
- þ The ability to maintain a consistent public image and customer confidence?

**Considering Time Factors**: If a technology disaster were to occur, for how long could the business withstand an outage in one or more systems before negative consequences occur…?

- **Duration Level 1**: Less than 1 Hour
- **Duration Level 2**: Less than 4 Hours
- **Duration Level 3**: Between 8 – 24 Hours
- **Duration Level 4**: Up to 2 Days
- **Duration Level 5**: Between 2 – 4 Days
- **Duration Level 6**: Up to 1 Week or longer

***TIP: Focus on duration**. Consider the extent to which outages can be withstood will determine overall recovery priorities.*

**Considering Tangibles**: What type of hardware and software (including data) will be required to establish and maintain critical business operations in the event of a technology related disaster?

- þ Types
- þ Quantities
- þ Manufacturers

þ Configuration<br>
þ Licensing Requirements<br>
þ Compatibility<br>
þ Usage<br>
þ Locations

The results of this *multi-dimensional* requirements analysis will provide the factual basis for your *Disaster Recovery Plan*, setting the stage for a subsequent review of key financial and resource capabilities. Disaster recovery management can be costly, and all planning and recovery efforts must be scaled to suit critical needs and priorities.

In the first moments, hours and days of a crisis event, you may not be able to restore full systems functionality, but you must be able to restore <u>critical</u> functionality as soon as possible. To meet that goal, all critical systems must be located, quantified, and matched to the appropriate mechanism for recovery and restoration.

## STEP 3: ANALYZE CAPABILITIES

Once planning goals and requirements have been identified, internal capabilities must also be placed under the analytical microscope: **Do you have the resources needed to meet identified goals and requirements?**

When reviewing these capabilities, two primary factors must be considered:

þ **Finances**: What are the costs associated with disasters and disaster recovery?

þ **Staffing**: What resources and skills are required to create, manage and execute the required disaster recovery plans and programs?

### Financial Capabilities

Disaster recovery costs will vary based on technical environment, business characteristics, and overall recovery and business resumption objectives. As can be expected, there is a direct correlation between available funding and available recovery alternatives.

For example, the most aggressive approach to disaster recovery involves the complete replication of systems and facilities in a secondary location. While this solution provides optimum recovery potential, the costs may be prohibitive, placing it outside the bounds of "affordability" for many business organizations. As a practical matter, the goal of this financial analysis is to find the **point of affordability**:

þ Estimate disaster recovery costs.

þ Conduct a cost/benefit analysis.

þ Identify financial capabilities.

### Cost Factors

**What are the expected costs of disaster recovery management considering resources, tasks and tools?** To answer this question, you must consider all the possible cost factors listed below:

þ **Physical Assets**: Costs for hardware and software tools for systems management, backups, telecommunications, configuration redundancies (i.e. disk mirroring and database shadowing), and resumption equipment, in terms of hardware spares and rentals.

þ **Staffing**: Costs of permanent and temporary staffing in the event of a disaster, including consultants, meals, travel and temporary housing.

þ **Facilities**: Costs to maintain or outsource business and/or technology resumption facilities.

þ **Supplies**: Costs for technology, telecommunications and office supplies that may be needed to support business resumption and disaster recovery activities.

þ **Administrative Overhead**: Costs to support the communications, purchasing and administrative activities relating to disaster recovery planning and business resumption.

þ **Training**: Costs to provide IT staff and end-users with the skills and information necessary to support and execute disaster recovery and business resumption activities.

þ **Documentation**: Costs to prepare, duplicate and distribute the documentation, and related information, needed to support and execute disaster recovery and business resumption activities, including technical documentation, policies and procedures documents, and instruction manuals.

### What costs will be incurred if and when "disaster strikes"?

To answer this essential question, you must go back to the existing business/ technology relationship for further analysis. Specifically, you have to consider technology uses, and related operational dependencies, to uncover the potential "costs" incurred should that technology become unavailable.

þ **Revenue**: Is the system directly involved in revenue generation?
þ **Operations**: Which internal operations does this system support?
þ **Customer Service**: What role does this system play in customer service?
þ **Regulatory Requirements**: How does this system help to meet regulatory requirements?

In addition to the costs incurred when a given system or platform is "down", asset replacement costs must also be estimated (in the event that hardware and/or software assets are damaged and/or destroyed). Viewed from this perspective, disaster costs can be calculated according to related consequences:

**How much will a disaster cost?**
**A= Projected Revenues**
**B= Business Days Per Year**
**C= # Work Hours Per Day**
**Hourly Cost of Disaster = A / (B x C)**

Table 1 Consequences and Cost Calculations

| Consequences | Cost Calculations |
|---|---|
| Lost Revenue | · The inability to process revenue based transactions.<br>· Specific failed or incomplete transactions.<br>· Lost "potential" income (i.e. An inability to submit a contract bid). |
| Lost Productivity | Specific costs associated with operational disruptions: (*lost work hours x employee costs*) |
| Lost Stature | Intangible damage to company reputation and market position resulting from a disaster event, possibly translating into lost revenue. |
| Regulatory Fines | Specific costs incurred as a result of a disaster event (*fines, fees and interest*). |
| Lost Assets | Costs to replace or recover hardware, software and data. |

## Find the Point of Affordability

How much can you afford to spend on disaster recovery? The following questions will help you to pinpoint your **point of affordability**: *i.e. the specific point at which disaster recovery plans and activities will yield sufficiently successful results, meeting essential recovery goals at a realistic cost basis*:

þ If any of your anticipated disaster conditions were to occur, what are the likely costs to the business?

þ Can these costs and consequences be absorbed without permanent damage to the business?

þ Can disaster recovery and business resumption activities be used to reduce these costs and consequences?

þ How do the **costs of action** compare with the **costs of inaction**?

Once these questions are answered, the balancing process can begin… comparing potential costs to risks and benefits, with an eye towards affordable recovery strategies. In practice, a critical balance must be struck between protection and financial reality. You must be able to afford the strategies you create, and you must be able to create strategies you can afford. And, above all else, one key question must be addressed…. **Can you afford “not” to take the necessary steps to protect the business and its technology assets?**

Ultimately, disaster recovery planning cannot be ignored or discarded simply because of the costs involved. In all likelihood, disaster recovery is essential to business survival. You must strike that “balance”…. to adopt the right set of strategies and practices for prevention, anticipation and mitigation, considering actual needs and available budgets.

## STEP 4: DETERMINE RESOURCE REQUIREMENTS

Disaster recovery planning is a multi-dimensional process, requiring substantial time, and dedicated resources. This process is best achieved through a combination of diverse skills (business, technical, management and organizational), applied to produce tangible management solutions.

**Do you have the skills and resources needed to get the job done?**

þ What types of resources and skills are required to properly plan and support disaster recovery activities?

þ How many staff resources (in numbers and/or hours) are required to plan, develop and test your disaster recovery program?

þ How many additional staff resources (in numbers and/or hours) are required to manage and maintain systems in accordance with disaster recovery and business resumption best practices?

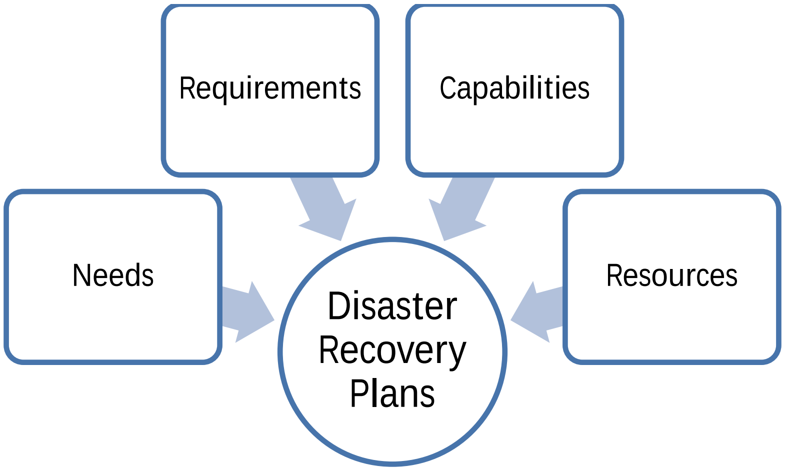
þ Does IT have the skills needed to plan, support and execute disaster recovery and business resumption plans?

The comparison of internal capabilities to internal requirements is a key element of the needs assessment process. If your disaster recovery program is to be of any value, it must be relevant and realistic. If you lack the skills and resources to carry it off, you must react accordingly, looking to external consultants and outsourcing to meet critical needs.

On the other hand, if you have the resources, but lack the funds, you must make that fact known as well. At the very least, this kind of careful analysis will afford the opportunity to establish, and justify, **realistic recovery expectations** for management personnel, end-users and if needed, external customers.

## Conclusions

Table 2 Inputs to Plans



Once the analysis is complete, the resulting information and conclusions are used to formulate specific disaster recovery steps, strategies, tasks and decisions. This is essential to ensure that all resulting plans are relevant to the identified business and technical needs. In addition, all resulting plans must be fully "do-able" considering identified capabilities and resource considerations.

## DISASTER RECOVERY PLANNING GLOSSARY

### A

**Activation Process**: The pre-defined set of criteria, procedures and practices used to assess a potential disaster event and initiate appropriate response procedures as per the documented Disaster Recovery Plan (DRP).

**Alternate Operating Procedures**: The defined set of temporary procedures used to maintain critical business processes and services during a disaster event. These alternate procedures, including the use of standalone systems or manual workarounds, are used until primary systems and operations can be restored.

**Alternate Workspace**: Any temporary work location(s) to be used in the event a primary workspace becomes unavailable. See Business Resumption Site; Reciprocal Agreement.

**Anticipation Strategies**: The disaster recovery planning strategy used to identify and analyze potential disaster events. Anticipation techniques are used to identify disaster scenarios and conduct the related “what-if” analysis.

**Audit**: The process by which disaster recovery plans, procedures and systems are reviewed and evaluated to ensure compliance with all internal and external best practices, requirements, regulations and contracts.

### B

**Business Assets**: The physical, technical, informational, and financial goods and properties to be protected as part of the disaster recovery management program.

**Business Continuity**: The degree to which a given business entity, or individual department, is able to sustain business processing during an unforeseen problem incident or disaster event.

**Business Impact Analysis**: The process by which systems, operations and services are evaluated to identify likely negative consequences due to a potential disaster event. The business impact analysis is used to establish disaster recovery planning priorities.

**Business Resumption Site**: A pre-selected location used to conduct critical business operations during a declared disaster event. Business resumption sites can be used for technology operations, business operations, or both, and must be outfitted with all required systems, equipment, furniture, and supplies as needed to support interim operations. See Hot Site

## C

**Chain of Command**: The pre-defined reporting relationships and decision making authority to be exercised during a disaster event. Depending upon the type of disaster, and related impact, decisions will be escalated through the designated “chain of command”.

**Cold Site**: see **Hot Site**.

**Contingency Planning**: The process by which temporary operational and service procedures are developed. These alternate procedures are put into effect only in response to declared problems and/or disasters, and are contingent upon specific incident parameters and conditions.

**Command Center**: The defined location(s) out of which the Disaster Recovery management team operates during a declared disaster event. The Command Center can be a single physical location, or multiple physical and/or virtual locations connected via telecommunications.

**Crisis Management**: The set of practices and strategies used to respond to any disruptive event, covering problem management and disaster recovery. The goal of crisis management is to ensure timely recovery with minimal damage to physical assets, internal operations and customer relationships.

## D

**Damage Assessment**: The process by which disaster event "damage" is evaluated to quantify specific impact, and to determine appropriate steps for response and recovery. Depending upon the nature and extent of the disaster event, the damage assessment process will cover staff safety, facilities, systems, data, records and related information and equipment.

**Data Backup**: The process by which electronic information (data, systems configuration, and application files) are duplicated onto alternate media that can be stored off-site. Backups are used as the primary vehicle for data restoration and recovery, offering protection for hardware failures, equipment damage, applications crashes, virus incident recovery, and any other circumstance leading to data corruption, erasure, or other unrecoverable error.

**Data Replication**: Any process by which data is copied from an original storage repository to a secondary, duplicate storage system. Replication methodologies include file shadowing and disk mirroring.

**Disaster**: Any sudden event causing an unplanned disruption in, or damage to, essential business facilities, technology and/or processes, causing some permanent physical or financial loss, and/or an unacceptable interruption in corresponding operations and services.

**Disaster Impact**: The consequences of a given disaster event to people, facilities, systems, operations and services, characterized by a varying degree of severity, timing and duration. Disaster impact can be minor, moderate or severe.

**Disaster Recovery Organization**: The hierarchical structure of internal and external personnel tasked with the planning, testing, execution and maintenance of the disaster recovery program.

**Disaster Recovery Program**: The complete set of logical and physical components used to provide disaster recovery services and solutions, including practices, policies, procedures, strategies and related systems, equipment, vendors and facilities.

**Downtime**: The specific period of time during which a given system (or systems) is unavailable. Downtime can be planned (maintenance) or unplanned (disaster or problem event).

**Duration**: The specific length of time during which a disaster condition exists. The event duration comes to a close when recovery is realized.

## E

**Emergency Reporting Location**: The pre-specified locations (physical or virtual) to which internal personnel are expected to report in the event of a disaster. Depending upon the nature of the event, the emergency reporting location can be a physical building or virtual contact point (call-in center, web site, voice mail system, etc.)

**Escalation**: The process by which decisions are raised to a higher level of authority according to the designated Disaster Recovery Organization, and related roles and responsibilities.

**Exposure Assessment**: The process by which the overall disaster “threat potential” is evaluated to determine current risk levels and vulnerabilities (according to event probability, systems design weaknesses, life safety risks, security controls, and recovery capabilities).

## F

**Fault Tolerance**: The systems design process used to eliminate any Single Point of Failure through built-in redundancy. Fault tolerant systems will remain operational in the event of a component failure through the use of redundant hardware and/or software. These redundant components stand ready to assume primary operational status in the event of a counterpart failure (e.g. servers, processors, disks, backups).

## G

**Governance Policies**: Any policies and practices used to manage technology usage and implementation. Governance policies are utilized as part of preventative disaster recovery management.

## H

**Hot Site**: A fully equipped Business Resumption Site ready for immediate use in the event of a disaster. The hot site must be continually maintained and updated as needed to ensure suitability. In contrast, a **Cold Site** acts as a business resumption "shell", which must first be prepared, equipped and configured, and therefore is not available for immediate use in the event of a disaster.

## L

**Life Safety**: The process by which the safety and security of all company personnel is ensured and maintained in the event of a disaster, covering evacuation, emergency reporting procedures, communication, training and testing.

## M

**Mission Critical**: Any data, process, application, system, or job function deemed necessary to, and for, business continuity. Mission critical components form the strategic and procedural foundation of any disaster recovery program, establishing physical response and recovery priorities.

**Mitigation Strategies**: The disaster recovery planning strategy used to create disaster response and recovery solutions. The goal of mitigation planning is to minimize negative disaster consequences, and to restore essential systems and services in the shortest time possible.

## O

**Off-site Storage**: Any alternate location (internal or outsourced) used to house duplicate files, documents and records (electronic and/or paper).

## P

**Prevention**: The disaster recovery planning strategy used to avoid and minimize disaster frequency and occurrence to the extent possible.

**Priority**: The criteria by which critical processes and consequences are quantified and ranked to identify, organize and execute disaster recovery planning tasks, targets and objectives.

## R

**Readiness**: The degree to which a given organization, or individual business unit, is prepared to respond to, and recover from, a declared disaster event.

**Readiness Gap**: The extent to which readiness "weaknesses" exceed readiness "requirements". The readiness gap exists whenever disaster recovery requirements cannot be met with existing capabilities.

**Reciprocal Agreement**: Any negotiated (cooperative) agreement between business departments (or locations) to use the each other's workspace, systems and related resources during a declared disaster event.

**Recovery Practices**: The set of strategies and procedures used to restore normal operations, data access, and systems functionality after a disaster event.

**Response Practices**: The set of strategies and procedures deployed in response to a declared disaster event. Response practices are designed to ensure life safety, to assess and minimize damage impact, and to achieve temporary restoration of critical operations, data access and systems functionality pending long term recovery.

## S

**Scenario**: Any pre-defined set of hypothetical conditions and circumstances used to anticipate and evaluate potential disaster events. Disaster scenarios are used to evaluate impact, set priorities, plan response and recovery strategies, and establish "conditions" for disaster recovery plan testing.

**Single Point of Failure**: Any critical system, operation or service component which, if lost or damaged beyond repair, will cause a complete loss of overall functionality or operability. Single points of failure should be eliminated or minimized to the extent possible via redundancies. See Fault Tolerance.

## T

**Technology Centric Disaster**: Any disaster event limited to technology outages, damage or service disruptions, with no life safety or facilities implications.

**Test**: The set of pre-defined activities and conditions used to verify, measure, and evaluate the quality and effectiveness of the overall disaster recovery program. Testing activities are executed via a documented DRP Test Plan.

**Test Script**: The pre-defined sequence of steps and tasks to be followed by DRP test participants to simulate work activities, data entry, systems usage, and operational processing as part of DRP testing.

**Transaction Journaling**: A database design and management process used to record and track database changes via a time sequenced record of all related updates and entries. The transaction journal can then be used to recover and restore the database system after a failure.

the IT-manage

# Service Strategy Toolkit

Available for purchase and download at ITtoolkit.com

## 20+ Service Strategies....

- Start with the basic “vision concept”.
- Define your vision for mission, value & relevance.
- Organize IT staff to fulfill the established vision.
- Plan service portfolios to suit vision needs.
- Create actionable IT Management Vision Statements.
- Use SLA’s to set realistic IT service expectations.
- Govern your “vision” through sound IT policies.
- Strategize based on end-user interests & influences.
- Identify, analyze and prioritize IT management risks.
- Recognize the constraints that limit IT possibilities.
- Make decisions using scenario & impact analysis.
- Build collaborative IT/End-User partnerships.
- Use ROI as a measure of “vision” value.
- Organize steering committees to lead the IT vision.
- Eliminate & avoid IT service expectation gaps.
- Maximize IT planning & project capabilities.
- Work with end-users to deliver successful IT projects.
- Take a proactive approach to problem management.
- Execute IT service reviews to evaluate & improve.
- *And much more.....*

| | STANDARD | EXTRA | BUNDLE |
|---|---|---|---|
| Practices Manual *(200+ pages)* | ü | ü | ü |
| Vision Statement Template *(20 page layout)* | | ü | ü |
| Steering Committee Charter *(30 page layout)* | | ü | ü |
| Service Review Process Plan *(16 page layout)* | | | ü |
| Satisfaction Survey *(8 worksheets)* | | | ü |
| Survey Results Spreadsheets *(4 worksheets)* | | | ü |
| Review Analysis Template *(25 page layout)* | | | ü |

## Practices and Techniques

Define, Align & Approve (DAA)
Role, Interest & Influence (RII)
Scenario Planning & Impact Analysis
Manage by Process (MBP)
Fast Track Project Management (FTPT)
Proactive Problem Management (PPM)
IT Service Review Process (ITSR)

## Reference and More

Service Strategy Workflow
Service Review Checklists
Satisfaction Survey Statements
Action Word Glossary
Steering Committee “Code of Conduct”
Risks and Constraints Checklists
Management Skills Checklists

**The Service Strategy Toolkit** (*Standard Edition*) is provided in PDF format, fully compatible with Adobe Acrobat or Reader 9.0 or higher. The *Extra* and *Bundle* Editions include templates and spreadsheets, in Microsoft Office Word and Excel format respectively, compatible with Microsoft Office Word and Excel 2007 or higher. The *Extra* and *Bundle* editions also include Instruction Manuals, and all components are contained in PDF portfolios.