Data Backup, Retention and Restore -Guidance Note

Michael Barwise

Strategy

Data backup/retention/restore (BRR) is not an independent strategic issue- it is an integral part of corporate information management, and closely coupled to issues of business continuity (BC), disaster recovery (DR) and compliance with information integrity and retention requirements under statute. Therefore BRR strategy, BC strategy and DR strategy should be components of an overall coherent information management strategy which is informed by statute as well as perceived business objectives.

The BRR component of this strategy must describe and justify all the purposes and goals of data backup, data retention and data restoration, and must be supported by policies that specify the methodologies and targets for defining, managing and auditing detailed BRR processes to fulfil those goals. The processes themselves must be documented as formal procedures to assist operators in complying with the policies, and to provide a basis for audit evaluation of their fulfilment and adequacy.

Due to its mission-critical nature, is not safe to operate a BRR regime without all three tiers of control in place. For consistency and effectiveness, the strategy, policies and procedures must be defined in this sequence, so that each layer of definition informs the development of the layer below. If this process is not followed, objectives will become ill-defined, resulting in inconsistencies between strategy, policies and procedures, with consequent confusion and loss of control over processes.

Goals

The optimum BRR regime from the business continuity perspective will be one that offers maximum assurance of data retention, maximum convenience and speed of data recovery, and minimum time and resources to perform backup. When defining BRR processes, it may be necessary to review the way data is managed in service, as there is often massive and unnecessary redundancy in backups where they are defined with inadequate reference to the local management of data by business process owners, or where data management within the business processes is not optimised.

Management Guidelines

1. BRR strategy and policies must be defined in technology-independent business oriented terms, as both strategy and policy must by definition be relatively stable. It is crucial to success that required BRR options are not restricted by the limitations of specific technologies or vendor offerings. Technologies must be selected and implemented that demonstrably fulfil the business requirements.
2. BRR processes must be defined with reference to corporate business imperatives as a whole, rather than on the basis of the independent expectations of individual business units. A method must be devised, proved and documented that allows information assets critical at the corporate scale to be identified and prioritised for backup and restore under each of the various recovery scenarios (global DR, partial loss of service, server failure, individual file restore &c.). The resulting priorities must be addressed by BRR processes that are proven to effectively support corporate data management. Issues to be considered include maximum business process downtime, required data currency, acceptable data loss and legal implications of unavailability. The identified global corporate priorities must take precedence, even though they may not always accord with the subjective views of individual information owners.
3. Measures must be put in place to ensure that data retention periods comply with any statutory minima or maxima for specific data, in addition to the requirements imposed by corporate business needs. These measures will include activities at all levels from business policy to technical procedures, including data review and purging schedules, media verification regimes, archive migration plans.
4. If technical BRR services are outsourced, their management at the strategic and policy levels must nevertheless remain the under the control of the organisation itself, and they must at all times demonstrably comply with the corporate strategy and policy in force. An at least minimal procedural component will also remain in such cases to cover compliance monitoring and interfacing between the organisation and the outsource.

5. Process owners must be appointed to manage the validity of, and compliance with, corporate BRR strategy, policies, and procedures. The appointed process owners must possess the requisite skills and experience, and should preferably be formally trained and certified, to fulfil their specific BRR management roles.

Technical Guidelines

1. A universal naming convention must be established, tested and documented to allow easy and accurate identification of data sets on backup media.
2. Documented and auditable systems must be established to minimise the probability of backup loss. Precautions may include physical dissociation of the backup engine from the data source, immediate validation of backup integrity, multiple replicate backups in offsite storage, careful selection of technologies and methods for data encryption and/or compression to minimise the possibility of restoration failures, strict adherence to safe working life criteria for media, regular cyclic verification of backup integrity in store, timely migration of backup data to new technologies, and rigorous determination of appropriate backup cycles with reference to critical business requirements and information value.
3. If remote backups are performed over an untrusted infrastructure, measures must be implemented to ensure that data in transit are subject to an equivalent degree of information security to that applied to the data when in use by the business process that owns it. Where data subject to differing security requirements travel on the same infrastructure, measures ensuring the most stringent requirement is met must be applied.
4. Backup media in transit and storage must be subject to an equivalent degree of security to that applied to the data when in use by the business process that owns it. Where data subject to differing security requirements are stored on the same medium, measures ensuring the most stringent requirement is met must be applied.
5. Backup media must be validated in compliance with a proven regime using methods that ensure the integrity of the data they contain, in addition to readability of the media.
6. Backup and restore rule sets must be fully documented in a human readable manner, independently of any software that may implement them. It is not sufficient to rely on the survival of parameters stored by backup software, even if these are themselves backed up. It must be possible in emergency to completely recreate backup and restore rules without recourse to backup archives and on completely different backup software.

Critical Process Requirements

1. Documented, standard decision making processes should be employed when defining goals, requirements, obligations and methods for BRR, with due reference to the overall information management strategy of the company.
2. All strategic, policy and procedural decisions regarding BRR must be justified by documented rationale, and, where possible, by independent supporting evidence(e.g. conformity to best practice or results of robust risk analysis).
3. All BRR decisions and processes must be auditable for effectiveness, and independently for compliance, against finite criteria.
4. Records must be maintained of all BRR management and technical transactions, identifying the nature of the transaction, the authority for, and the performer of, the transaction.
5. Any outsource facility must be independently evaluated for effectiveness and security prior to commencing use of any service it supplies.
6. Because of the relative ease with which data on backup media may be accessed, all staff, contractors and agents engaged in BRR must be vetted and security cleared to a level that covers them legally to be exposed the most sensitive data on the media and systems they handle in the course of their BRR duties.
7. In support of both technical and legal obligations, it is suggested that metadata should be established to describe the information assets that are subject to BRR.

Originally released as client guidance, January 2003