

A Des-Res for your data?

Data is any organisation's most valuable asset, and should always be high on the risk management agenda. A data centre need not be a purpose-built major building on a fortified estate. Indeed, it can be anything from a broom cupboard upwards. It may therefore come as a potential surprise that the risks are more or less the same, no matter what its size.

Risks

Some of those risks are more obvious than others – if asked to list them, most people would immediately think of physical security and resilience. Maybe not so many would consider governance, change control and problem management in this context.

Yet from a risk perspective, a data centre is no different to any other part of your IT infrastructure. Matters such as physical security and access control are important, of course. But so are all the other aspects of control, such as the management framework, capacity planning, availability management, environment, staff training etc.

Governance

Perhaps the most vital control to have in place is effective governance. Whatever its size, the data centre should be run professionally with a sufficient level



of formal management control in place to determine, define and sponsor the day to day operations.

Relevant management information should be reported regularly to interested parties. This will mitigate against misinformed decisions, failed communication, loss of service provider support, financial mismanagement, regulatory non-compliance, operational ineffectiveness and inefficiency.

Even if your physical IT infrastructure is outsourced to a third-party, the

risk remains yours. Responsibility, accountability and regulatory obligation are among the few things that cannot be passed on to others.

Thus if your data centre is in the hands of a supplier, you should still take a proactive interest in its design and operation. This includes performing regular reviews of their control environment. If you do not have the specialist skills available for this, you should seriously consider engaging those services externally.

Asset management

An inventory must be in place which covers equipment and infrastructure, services provided, installed software, etc. This should be supplemented by a process linked to change management, so that the inventory is updated when *any change* takes place which affects the data centre.

This is particularly important where mirrored data centres are in place for resilience purposes. It is all too common for multiple sites to become out of step; this may well defeat the objective, and can easily lead to a continuity incident having far greater impact than would otherwise be the case.

Similarly, it is not easy to maintain or secure assets which you don't know you have!

Physical considerations

From a physical perspective the site selection and layout is crucial. If the data centre is located within an existing building, are any water or sewerage pipes routed over the space? In any case, it is vital to ensure dual routing of essential services – data communications, power, water – in case of interruption. That routing should be separated both inside and outside the building, with no overlap or common areas.

Most installations will include an uninterruptible power supply (UPS). This must be regularly tested; a

schedule is invariably recommended by the manufacturers. In the absence of testing, there is no assurance that it will operate as designed in an incident. It should be remembered that a UPS is not intended to keep everything running whilst the normal electricity supply is unavailable. It is designed to provide time for either a controlled and tidy shutdown of systems without loss of data, or for handover to an alternative supply – eg from an on-site generator. If a generator is to be used, does it work? Is sufficient fuel available for prolonged operation? Again, it is important to test the process regularly.

Facilities management includes maintaining the data centre building, location, power and communications as fit for purpose and in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.

Environment

Environmental threats should be assessed and countered where appropriate. High temperatures are not the only thing to bear in mind; much IT equipment is also sensitive to humidity and dust. It should be self-evident that appropriate fire detection and extinguishing measures are in place.

Some organisations may also need to consider their carbon footprint, energy efficiency (PUE) etc. Such controls are important not just for

the operational cost-effectiveness of the data centre; they are also valuable inputs to any responsible organisation's corporate social responsibility programme, with consequent positive reputational impact. Further, they will contribute to the Carbon Reduction Commitment of larger organisations where appropriate.

Security

Physical security measures which are in line with business and regulatory requirements should be defined and implemented. These should include, but are not limited to, the layout of the security perimeter, security zones, location of critical equipment, and delivery areas.

In particular, a low profile should be maintained regarding the presence of critical IT operations. Signs and other identification at the data centre should be non-existent or at least discreet; and they should not obviously identify the site from the outside. Internal phone directories and site maps should not identify the location of the data centre. There should be no windows in computer rooms.

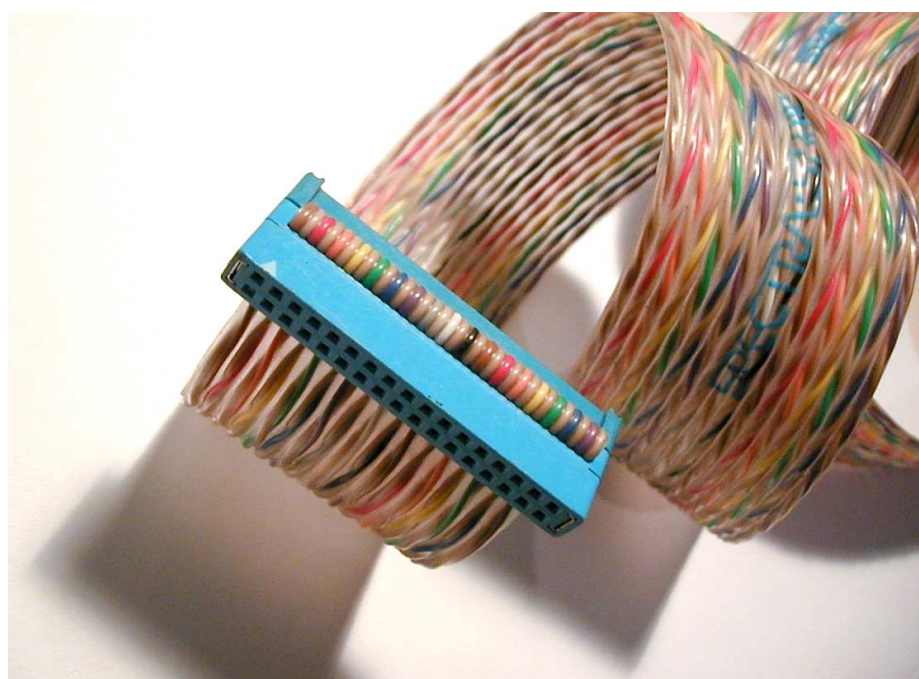
Responsibilities for site security and monitoring, and procedures for reporting and resolving physical security incidents, need to be established.

In the case of larger data centres, there is generally a greater need to implement measures which prevent controls being bypassed (eg by staff tail-gating).

Changes and maintenance

It is a well-established fact that most IT downtime is caused by unauthorized or improperly implemented changes. Changes to the data centre infrastructure – including physical maintenance and system patching – should only be undertaken using formal change management procedures.

Change requests should be formally assessed in a structured way for impacts on operational data centre performance and functionality. This assessment should include categorization and prioritization of changes. Prior to implementation a change should be appropriately tested and authorized.



When emergency changes cannot follow the standard change procedure there should be an established process for defining, raising, assessing and authorizing the emergency change.

The change process should include consideration of updating the relevant business continuity plans, so that these remain current and fit for purpose.

Problem and incident management

Incidents and underlying problems should be effectively managed and controlled via an established process. This should include mechanisms to report, classify and communicate relevant information.

Incidents should be managed via a system which provides an adequate audit trail that tracks, monitors and records all incidents, including root cause analysis and correction. Problems should be continually monitored and reported until they are formally closed.

You should ensure that when any environmental or security alarm is triggered, an appropriate alert is raised. If appropriate, 24x7 cover should be available to react to such alerts.

Personnel

Data centre management should ensure that all staff supporting the physical operation of the data centre

– eg security staff, mechanical and electrical staff, cleaners, delivery staff – behave appropriately and undertake their jobs in line with the operating procedures applicable to their line of work and those of the data centre. Consideration should be given to adequately vetting those with data centre access to a level commensurate with its security status.

There should be a formal, cost-effective plan to assess, schedule, deliver, validate and maintain the training and personnel requirements for all data centre physical support staffs.

Can we help?

Obviously this paper can only scratch the surface of the risks and controls associated with data centres. Kingston Smith Consulting is able to provide a range of data centre solutions to protect your business. We can perform full-scale reviews of all the areas outlined above, and advise on pragmatic measures appropriate to the size of your infrastructure. We also have staff experienced in data centre moves – projects which in themselves carry a unique set of risks.

If you are considering a new facility, we can provide specialized design and planning expertise to work with your own staff. This will ensure that cost-effective and fit-for-purpose controls are in place from day one.

To learn more, please contact Mark Child:
Direct Line +44 (0)20 7566 3731
Fax +44 (0)20 7689 2475
Mobile +44 (0)7515 107005

About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice associated with the top 20 accountancy firm Kingston Smith LLP. Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010
info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD