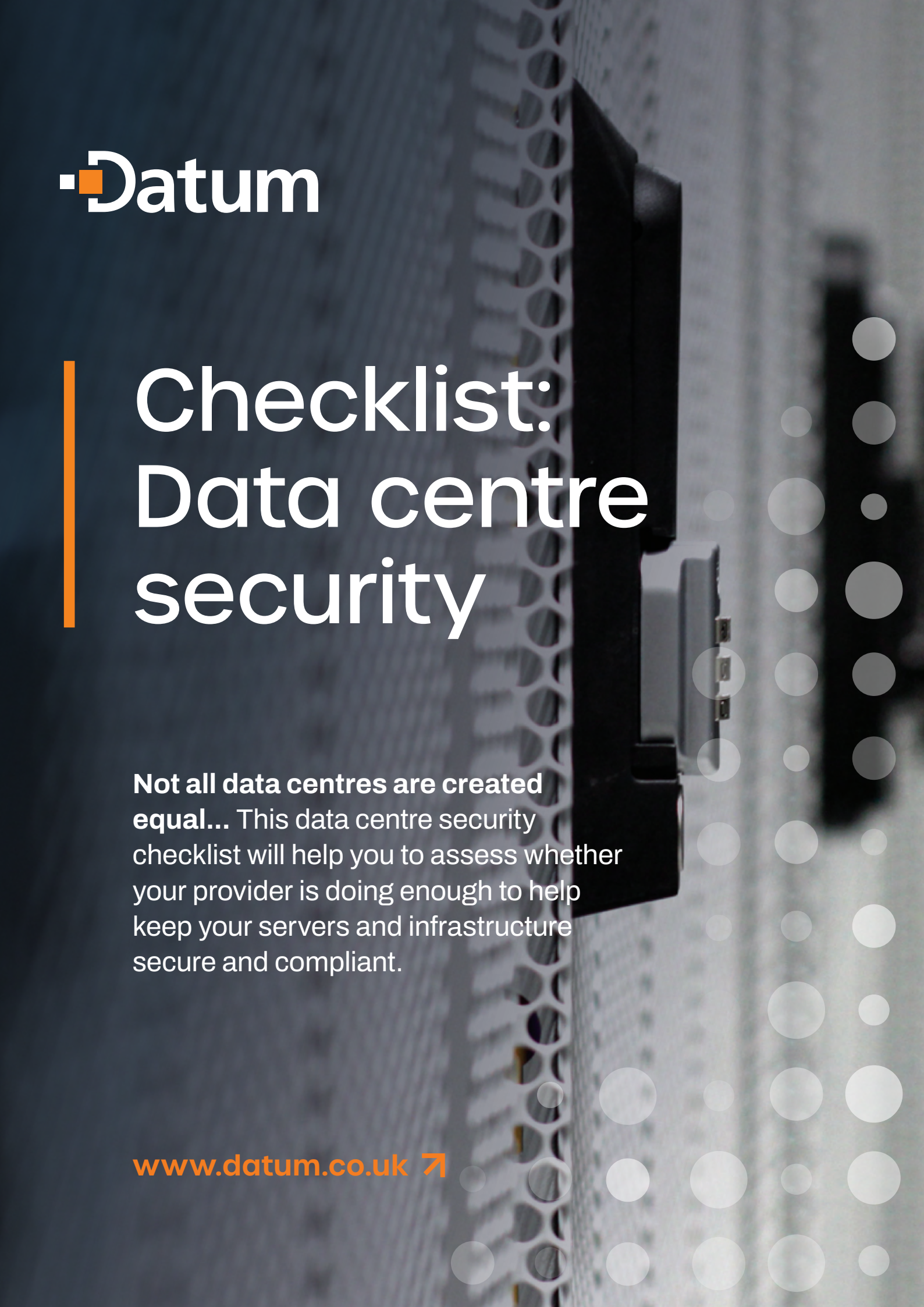


Datum

Checklist: Data centre security

Not all data centres are created equal... This data centre security checklist will help you to assess whether your provider is doing enough to help keep your servers and infrastructure secure and compliant.

www.datum.co.uk

Contents

Introduction

Not so long ago, the use of third-party data centre services in regulated industries like law and finance was considered a security risk.

Today, it's much more common — and many industry experts now acknowledge that colocation and cloud providers are capable of higher levels of security than most firms would deliver in-house.

However, not all data centres are created equal, and not all will stand up to the full range of security audits required by clients and regulators — even if their credentials look the part on the surface.

> **That's why we've produced this data centre security checklist. Are your suppliers doing enough to help keep your servers and infrastructure secure and compliant?**
>
> Checklist: Data centre security

Accreditations

Accreditations aren't the be-all and end-all of data centre security, but checking for compliance with standards like ISO27001 is still most firms' first port of call when it comes to choosing a data centre — and with good reason.

- Is the data centre compliant with ISO27001 (the international standard for information security management)?
- Is the data centre compliant with any other required standards such as PCI DSS?
- Are high quality CCTV systems installed, with live monitoring where required?
- Are security personnel background-checked/approved by industry bodies such as the SIA?

Building security

On the most basic level, every visitor to your data centre should be required to pass through multiple layers of building security, with additional access controls on racks and cages where necessary.

- Are there a wide range of access controls in place (such as perimeter fences, infrared tripwires, swipe cards, biometric scanners and mantraps)?
- Are the access controls configured to provide multi-factor authentication?
- Are data centre halls windowless, with the minimum safe number of entry points?
- Are the racks and cages in the data centre kept anonymous?
- Is access to racks and cages controlled by electronic locks or keys?
- If keys are used, where are they stored? Is access controlled and monitored?
- Is access to sensitive areas in the data centre monitored via 24-hour CCTV?
- Is CCTV monitoring carried out by an on-site NOC?
- In the event of a break-in, would security staff be compromised (and become part of the incident) or would they be able to react to it?
- Is the data centre directly linked to police control rooms?

Policy & process

Good management is essential for effective building security. As such, you should ask the personnel of your data centre to walk you through their security policies and processes, and provide examples of their use.

- Is a suitable process in place for customers to grant and remove access to their racks and cages for both internal and external personnel?
- Are access records kept up to date and retained for the required length of time?
- Are data centre staff granted access to halls, racks and cages on a need-only basis?
- Are visitors to the data centre accompanied by staff or tenants at all times unless authorised by a person with any relevant credentials?
- Are third-party engineers and contractors required to gain access through the NOC, and is the authorisation process secure?
- Are ID badges used to differentiate between data centre staff and visitors?
- Are badges assigned and managed by a suitable authority (e.g. NOC)?
- How thorough are the data centre's ID checks and security induction for new customers? Do staff sound confident in their own procedures?
- Is the movement of equipment in and out of the data centre controlled and monitored?

Staff

Great security isn't just about great infrastructure and management, but also people. Look for data centre staff who are knowledgeable, hands-on, and willing to take the time to understand what security means for your business.

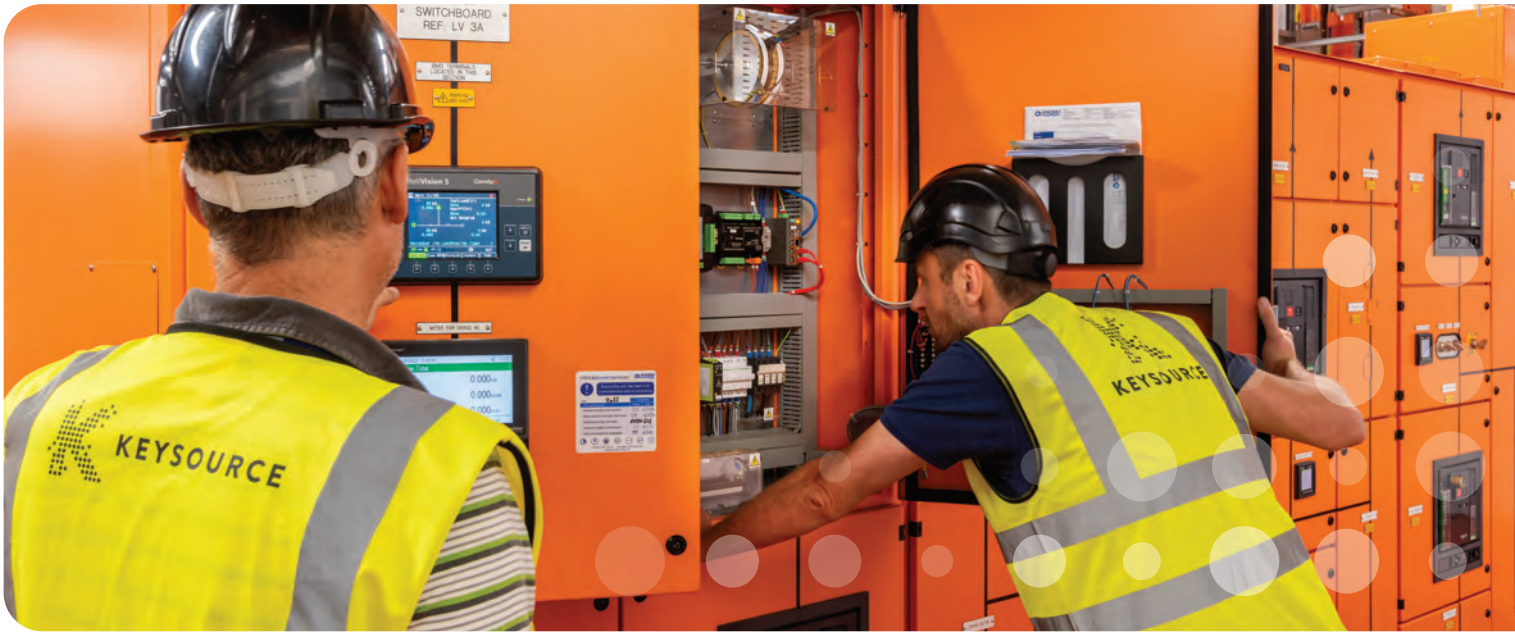
- Is the data centre able to offer an audit-friendly service, and answer a full range of auditors' questions and produce certifications?
- Are data centre staff able to share general advice around data centre security and compliance?
- Are senior security personnel based at the data centre itself rather than a remote site?
- Are the data centre staff required to undergo background checks where necessary?
- Are they sensitive to customer's confidentiality requirements (not disclosing customer names as part of a sales pitch, for example)?

Are senior security personnel based at the data centre itself rather than a remote site?

Contractors

If your data centre uses third-party engineers and contractors (such as cleaning companies), check their credentials and ensure due diligence has been carried out.

- Are third-party suppliers or contractors ever allowed to enter the data centre unaccompanied?
- If so, is the data centre willing to share the relevant supplier information with customers?
- Are third-party engineers and contractors accredited or vetted to any required standards?
- Are customers able to access basic information on supplier agreements, authorisation levels, and any policies and processes in place to control and monitor their activity within the data centre?



Flexibility

Finally, one of the most important factors to consider when it comes to data centre security is flexibility. Can you count on your provider to deliver a service designed specifically around your own security needs?

- Can the data centre provide assurances as to which staff will have access to customer racks and cages (e.g. background-checked personnel only)?
- Is it possible to block access to data centre staff entirely (unless a health and safety risk is detected)?
- Is the data centre willing and able to provide dedicated caged areas where necessary?
- Can the data centre offer bespoke rack security as a lower-cost alternative to caged areas (such as individual biometric scanners or card readers)?
- Is there a wider range of services (such as cloud and DR) that allow customers to use the facility to meet other IT objectives besides security?

Is the data centre willing and able to provide dedicated caged areas where necessary?

Datum: unrivalled data centre security

Our multi-layered approach to data centre security provides our clients with confidence in our ability to deliver a robust service. It also has a strong impact on our clients' commitments to their customers and helps to ensure that our facilities will meet and exceed the expectations of an enterprise class data centre facility.

This security resilience has attracted clients to Datum from across IT and cyber security, defence, construction, finance and the public sector. Our security approach is unrivalled and processes across our facilities have been designed to meet the requirements of industry-recognised certifications including ISO 27001, PCI DSS, BS5979, NSI Gold and PASF.

Book now

Take advantage of one of our no-obligation data centre tours and see our first class security processes for yourself — contact us to book a data centre tour for any of our UK facilities:

www.datum.co.uk
info@datum.co.uk
0333 2023 195

Datum

Contact us

Datum Datacentres Limited
Cody Technology Park, Old Ively Road
Farnborough, Hampshire, GU14 0LX

UK 0333 2023195
INT +44 (0) 1252 391980