

DCSRTM

Data Center Security Review



Introduction

The impact of a serious datacenter security incident is potentially massive. Regardless the size of the datacenter, they often house the organization's most valuable information assets comprising IT hardware (mainframes and other computer servers, SAN storage devices, tape robots, networking equipment *etc.*) and, of course, enormous quantities of extremely valuable business data and highly-skilled IT workers.

Based on different studies while considering aspects of security 'technologies' that are most overlooked, data center/physical security is topping the list, resulting in critical information processing environments that are literally waiting for security incidents to happen. Key conclusion out of these studies is that many data centers take big steps on IT security, but tend to overlook the core layer for data center/physical security to be implemented.

Data Center Security Review

Benchmarked against leading international data center and security standards, a seasoned data center auditor will review the data center security. Although the emphasize will be on physical security, organizational and technical aspects will be considered as well.

The DCSR will focus on the security arrangements in and for area's which include, but are not limited to:

- Data center perimeter
- Computer room
- Restricted area's such as generator room, telecommunication entrance room, network operations center *etc.*

Apart from the physical review, a detailed assessment on processes and documentation pertaining to the overall operational control on data center security is included as well.

Do you know how secure your data center really is?

Does your data center comply to international data center and security standards?

Review

The data center security review will take place in one day and consists of an in-depth physical inspection of the data center and supporting facilities. Additional interviews with staff operating the datacenter and reviewing applicable documentation such as policies and procedures will complete the review.

The review will be followed by a report with findings, a risk analysis and possible solutions for improvements which will lead to risk mitigation and therefore improved hi-availability and cost reduction.

Main benefits

- Analysis of current data center security shortcomings
- Independent review / second opinion on implemented security controls
- Benchmark against international compliance standards for data center
- Allows for future investment planning while mitigating risk of security breaches in the data center
- Report providing input for gap remediation
- Prepare the data center for international certification

Reporting

The output of the audit will be a concise report which will highlight the findings and gaps versus various international standards such as SS507, TIA/ANSI-942 and ISO27002 where applicable towards data center security. The report contains recommendations for improvement and constructive information on how to reduce the risks in the data center which could lead to downtime. The report will be delivered online (PDF format), typically within 5 days after the audit.

Where to use DCSR?

The DCSR can assist your organization in multiple situations:

New Data Center:

The DCSR can be conducted shortly after your new data center has been built to evaluate the design and implementation works provided by the contractor or data center builder.

Due to contractors oversight trying to cut corners in order to increase their margins, security controls might be not or wrongly implemented, causing the data center to face risks as per day one.

The DCSR will reveal the design flaws and will enable the organization to force the contractor to make changes necessary before approval of the final invoice and move your mission critical data center into production.

Rectifying problems whilst running production can prove to be costly and disruptive so it is better to be safe than sorry.

Existing Data Center:

The DCSR could add tremendous value to existing data center's which have been running for a number of years.

Due to personnel changes, the organization might not always be aware of information security risks emerging over a period of time, due to the lack of proper working controls or poor execution of SOP by your staff.

Data center's are dynamic places and are exposed to constant changes which could affect the effectiveness of current security controls or even worse, not having them in place because they were overlooking in the release of the change.

New vulnerabilities might exist, such as falling victim to social engineering or the threat of serious physical attacks. Considering all the unknown risks being present, the organization wants to act upon this before it is too late. DCSR will find these risks to assist in implementing timely and adequate security controls.

Organizational benchmarking:

Organizations might struggle in achieving the right set-up for data center security and this is sometimes caused by a number of factors, such as not having the desired staff in the right place or difficulties with designing, implementing, maintaining and executing the organizational policies and procedures towards the security in the data center.

The DCSR will touch upon these issues and the outcome will provide the organization with weaknesses if present. The DCSR report will further strengthen the organizational resilience if gaps revealed are addressed in a timely and expected manner.

Compliance to standards:

More and more organizations are being forced in implementing standards / best practices due to regulations or industry standards respectively released by government bodies or industry coordinating instances.

The DCSR is based on international certifiable standards and assists organizations that seek or retain compliance towards these standards, where applicable to security in the data center.

Customized reviews

The DCSR service offering can be customized to fit your needs. The standard DCSR is comprehensive enough for most customers however, should you need to broaden the scope and/or depth in certain areas to be audited then this can be accommodated. Please feel free to discuss with us your specific needs.

Asia/Pacific Headquarters:

Enterprise Product Integration Pte Ltd

37th Floor, Singapore Land Tower, 50 Raffles Place, Singapore 048623.

Tel: + (65) 6733-5900 Fax: + (65) 6735-6400,

e-mail: sales@epi-certification.com [http:// www.epi-certification.com](http://www.epi-certification.com)

Local offices in ; Malaysia, China, Vietnam, India, UK, France, Canada

Partner offices in ; China, Hong Kong SAR, Taiwan, Malaysia, Singapore, Indonesia, Philippines, Thailand, India, Pakistan, Vietnam, Trinidad Tobago, Hungary, Ukraine, The Netherlands, Spain, United States of America, Canada