



*Real value in a changing world*

advance 

# Critical Care for Critical Environments

Investing in reliability and protecting your bottom line

## Introduction

In recent years, several high-profile incidents have occurred with call centers and trading floors becoming inoperable, resulting in significant amounts of lost revenue and customer goodwill for corporations. In such cases, companies have been known to experience millions of dollars in losses for every hour a vital system is down.

## System down-time can cost companies millions of dollars in lost revenue.

The September 2008 crash of the computer system that powers the London Stock Exchange is one example of the impact a system failure can have on operations. The seven-hour shutdown during one of the year's heaviest trading days

resulted in non-effected transactions worth billions of gross business profit.

This, combined with the economic crisis impacting on the bottom lines of many corporations, has seen the issue of critical environment (CE) integrity gain increasing levels of attention. While companies are closely watching every dollar spent in the current market, they recognize that no expense can be spared when ensuring the hardiness and reliability of those systems that represent a firm's lifeblood.

However, infrastructure and technology malfunctions account for less than half of the instances of system failure; over 70% of failures are due to human error (Uptime Institute 2008). Many organizations today face significant CE risks despite their significant investment in infrastructure because they do not have an adequate program in place to prevent human-error incidents.

Table 1: The Critical Environment - What Qualifies?

Critical Space	Critical Equipment
Trading/dealing floors	Uninterruptible power supply
Data and call centers	Emergency generator
Manufacturing locations	Utility power systems distributing to critical areas
Telephone and data closets	Critical cooling equipment
Critical equipment rooms	Fuel oil, grounding, building automation, and fire protection systems

Source: Jones Lang LaSalle

Over 70% of system failures in critical environments are due to human error.



### No Program, No Problem?

In 2007, a major bank experienced a loss of power to the system managing its network of automated teller machines (ATMs) and internet banking systems. The robust back-up system acted as designed, switching operations over to auxiliary power. However, it was reported that a well-intentioned employee attempting to correct the situation hit an incorrect switch and inadvertently crashed the entire system.

Another example is the loss of trading capacity at an international bank. An external fire systems contractor was engaged to repair a faulty alarm and control unit. Believing he was proactively responding to an alarm on an uninterrupted power supply (UPS) system, the contractor accidentally shut down the power supply to the servers in the middle of trading hours. In this instance, the contractor was not in fact authorized to make repairs on this system. This human error incident cost the bank millions of US dollars in lost revenues.

There are two major rationales that discourage companies from implementing a CE program to ensure system integrity. This first occurs when the CE owner has not experienced any problems with its system and therefore concludes that its operating program is adequate. The second is budgetary, a factor that is becoming especially prevalent in the current economic environment, when cost lines are being more closely scrutinized.

Unfortunately, both of these rationales, while logical, are short-sighted. Past performance is not necessarily an indication of future operational excellence or even adequacy. Without undertaking a diagnostic examination of your CE protocols, it is impossible to know to what degree satisfactory performance is a by-product of rigorous management and to what extent it is most accurately attributed to luck.

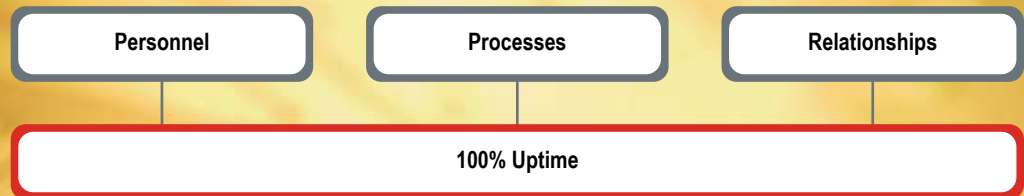
**A diagnostic examination of your CE protocols will determine whether your system performance is supported by rigorous management, or whether you are relying on luck.**



Examinations undertaken by Jones Lang LaSalle have frequently discovered that companies have unknowingly experienced multiple near-misses, narrowly avoiding instances of system failure. This includes one example where a system had actually gone down without being noticed because the failure was self-corrected and occurred during the weekend when the volume of transactional activity was low.

Failing to establish and maintain a program for ongoing CE management because of the cost involved in keeping them rigorous is a huge gamble. If no incident results from risks a manager may take, in the absence of a rigorous program, some small cost savings may be achievable. However, if system failure results from human error, then these small savings will be dwarfed by the costs of business down time and customer dissatisfaction.

**Figure 1:** Three elements of a rigorous CE Program required to hold up your goal of 100% uptime



Source: Jones Lang LaSalle

A qualified and experienced engineering manager costs around only USD 50,000 per annum in Singapore, representing as little as 0.3% of IT costs. This is based on the cost of the facility and infrastructure typically making up about 8% of all IT costs in a company (McKinsey & Company 2008). This represents millions of dollars' worth of infrastructure that is vital to your company's operations. Add to this the potential business loss in the event of data failure and it becomes clear that investing in a sufficient program and resources to manage risk is money well spent.

---

**CE infrastructure typically makes up 8% of IT costs, while a qualified engineering manager represents as little as 0.3% of IT costs.**

---

### Getting It Right

There are three key components of a rigorous CE program to support your goals of 100% system up-time: the right personnel, the right processes, and the right relationships (Figure 1).

### The right program

Eliminating the likelihood of CE incidents resulting from human error need not be a prohibitively expensive exercise. An effective intervention almost always requires attention and diligence more than incremental cash outlay. The vital steps you can take to minimize the possibility of human error compromising your CE are:

- Employ or engage the right personnel in the CE
- Institute rigorous processes governing who has access to the CE and what tasks they are authorized to do
- Foster improved working relationships between all CE stakeholders - CRE staff, Raised Floor Management' to 'corporate real estate (CRE) staff, raised floor management
- Create back-up plans and systems to effectively respond to system failure

Following these steps can result in significant cost savings, both in terms of reducing the need for expensive technology-centric solutions and, more importantly, by minimizing the possibility for system failure due to human error.

### The right personnel

Vital for maintaining a robust CE is having the best personnel operating it. Even the most technologically advanced system is prone to malfunction if it is manned by unqualified or unmotivated staff. Therefore, it is important to first employ the right staff and service providers and then ensure that they remain committed to their tasks. This applies to all personnel operating within the CE, including the following:

- All facilities management staff, including operations and facilities managers
- Critical vendors for the area, including those who service the systems connected to the power supply, cooling equipment and fire protection

- Construction personnel who work in the CE, including electricians, plumbers and general laborers
- Custodial staff such as security and cleaners who have access to the CE

Crucial steps include:

- Having a clear idea which attributes to look for when staffing the CE
- Instilling to the staff the importance of CE to the company and the likely costs of system failure
- Training the staff to understand the consequences of acting beyond their remits
- Maintaining the requisite level of motivation to stay vigilant within the CE

**Table 2: Getting the Staff Equation Right in the Critical Environment**

Qualifications	<ul style="list-style-type: none"> <li>• In the past, CE staff were typically, low-salaried and under-valued</li> <li>• Recently, awareness has increased of the potential cost of having unqualified staff operating in the CE</li> <li>• A previous trend saw engineering staff posts being filled by degree-holders or, at the minimum, diploma-qualified staff</li> <li>• There is increasing interest in attracting and retaining staff with trade qualifications and experience (e.g. electrical, electronic, or mechanical)</li> <li>• Qualified and experienced staff have better real-world knowledge of how systems operate, both on their own and as part of a complete operating system</li> </ul>
Training	<ul style="list-style-type: none"> <li>• Mandatory training for any personnel, including outside vendors, working in or in proximity to the CE</li> <li>• Regular refresher courses on what to do and, more importantly, what not to do in the CE. Conducting “what if” sessions will help to pre-empt issues that may occur</li> <li>• Training assists staff in understanding how their actions impact the operability of the CE, as well as the impact of system failure to the business</li> </ul>
Motivation	<ul style="list-style-type: none"> <li>• Motivation to protect the CE is aided by ensuring that the staff are equipped with all the tools they need to do their jobs</li> <li>• Instigating a reward system linked to meeting KPI requirements that are broader than just uptime, i.e. maintenance activities completed on time, audit result achieved etc.</li> <li>• Staff morale is aided by supervisors’ regular demonstration of the importance of their role and the mission; maintaining CE operability</li> <li>• Training is a key part of ensuring staff are motivated to maintain the integrity of the CE; by positioning the training as a privilege staff are more engaged</li> <li>• Presenting CE training to service providers as an exercise to deepen the supplier-client relationship will ensure a more committed response</li> </ul>

Source: Jones Lang LaSalle



### The right processes

Equally important as qualified, motivated staff in ensuring continuous up-time in the CE are the processes that govern what tasks/activities are permitted and by which parties. Although micromanagement is increasingly seen as ineffective in the workplace, it is essential that the CE *not* be managed like a normal workplace. Indeed, micromanagement is essential in keeping the CE free of possible human error. Key processes that should be included in a CE program are outlined in Table 3.

Processes are especially important in cases where the infrastructure is not as robust as newer equipment. With rigorous management, even a less-hardy system can attain outstanding reliability performance.

Solid processes can also overcome the dangers of complacency and lethargy amongst the staff. By instituting a checklist-type process, CE managers will more closely monitor the actions of staff and vendors inside the area, never assuming “they know what they’re doing” or that their own professionalism will preclude complacency. Rigorous processes will heighten the awareness and acuity of all personnel involved in CE activities.

**Table 3: Processes to Maintain Critical System Reliability**

- Employees must know *exactly* how and when they are expected to perform their duties in the CE
- Performance expectations can be established and formalized with the institution of work method statements
- Risk assessments help all participants understand how their actions positively and negatively impact the reliability of the CE
- Obtaining vendor participation in all components of the program is essential as their exclusion opens the door to myriad types of potential system failure
- Practice, testing and more practice in completing various operational tasks sequentially is key to a deeper understanding of what to do in a variety of scenarios, whether it be for maintenance or in an emergency

Source: Jones Lang LaSalle

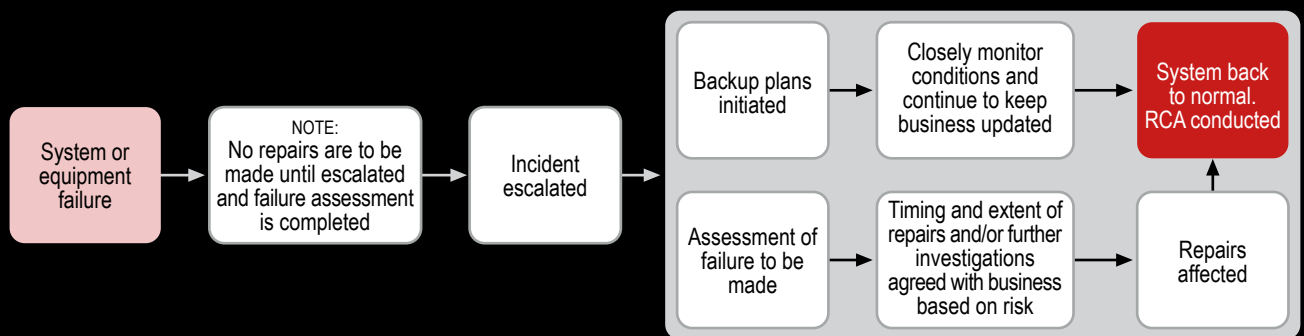
### Incident Response Program

While everyone works towards 100% uptime, directing staff how to behave in the event of an incident is fundamental to minimizing impacts and revenue losses from system failures. Not infrequently, well-meaning but unqualified staff attempt to rectify a system failure, but end up compounding the original fault with additional technical errors.

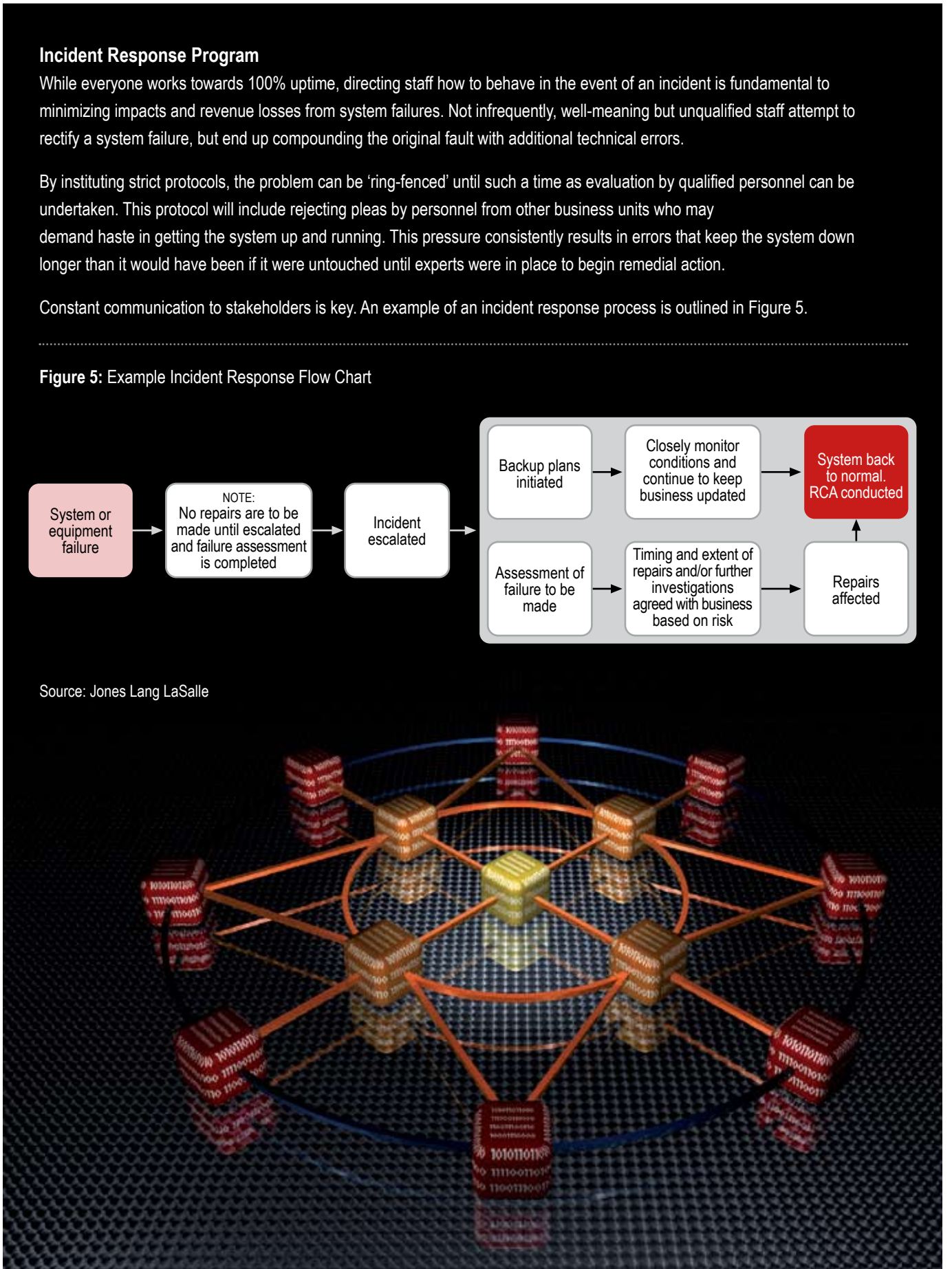
By instituting strict protocols, the problem can be 'ring-fenced' until such a time as evaluation by qualified personnel can be undertaken. This protocol will include rejecting pleas by personnel from other business units who may demand haste in getting the system up and running. This pressure consistently results in errors that keep the system down longer than it would have been if it were untouched until experts were in place to begin remedial action.

Constant communication to stakeholders is key. An example of an incident response process is outlined in Figure 5.

Figure 5: Example Incident Response Flow Chart



Source: Jones Lang LaSalle





### The right relationships

A long-standing area of friction in the CE has been in the relationship between those managing the information technology (IT) systems and those managing the physical area. In order for human error to be reduced to zero, the often adversarial nature of this relationship must be replaced by a culture of openness, communication and co-operation.

The roles of the IT and real estate departments are becoming more and more interdependent. For example, IT departments are requiring increasing levels of power and cooling to support their infrastructure, both of which they must coordinate through the real estate department. Both parties must recognize that cooperation and openness are the best way forward.

Real estate professionals must fully understand the nature of the work that their counterparts from the IT department undertake. A working understanding of the peak/off-peak operating period schedule, for example, will eliminate much of the conflict between the two sides. Requests for access to equipment can then be timed to minimize aggravation.

Likewise, IT professionals must fully understand requests from the real estate department to shut down systems to perform routine maintenance and regular full load testing on the ancillary systems, especially the power supply. While there is acknowledged complexity involved in shutting down a system or transferring operations to a secondary site, the IT department must recognize the necessity of doing so in order to build in the required level of reliability for standby systems.

One way of fostering better understanding between the two sides is hosting a forum in which all members from the two departments participate. Through formal discussion, both sides will gain a better understanding of the needs of the other and be more accommodating towards their requests for assistance, as well as in framing their own requests for help.

With enhanced communication, both sides will view the CE holistically rather than through the prism of their own remits. This will instill an appreciation of the importance of maintaining not just their own systems but also of the supporting infrastructure. It will also help impart an understanding that if all players communicate and cooperate then downtime, a blemish on everyone's record, can be significantly minimized.

### Periodic Testing

Periodic testing is vital as insufficient testing of the equipment and its interaction with the rest of the system can have serious impacts. This factor grows in importance as systems become more sophisticated and complex and is a major rationale behind annually scheduled integrated testing. This means not only testing the individual components but also ensuring that they are working together as intended in operation.

An example of the consequences of insufficient testing is when an interactive-component failure occurred at an airline. It was reported that the fault caused the online booking platform to be inoperable for over seven hours in the middle of the day during a peak travel period. While the individual components were all working as designed, the interface between two of them was faulty. When one unit failed, the redundant unit did not operate due to a lack of communication between the two units. This fault, which periodic integrated testing would have identified, resulted in significant customer dissatisfaction.

### Conclusion

For all the investment in technical support for the CE, the absence of a program to govern activity within it can bring the relevant system-and your business-to a screeching halt.

Investing in a program that mandates who may be in the CE, what they may do there, and how they should do it requires minimal financial investment. Close collaboration between the real estate and IT teams, for example, will only require an investment of time.

The minimal outlay required to put in place a rigorous CE program is insignificant when compared to the initial cost of installing the infrastructure and the ongoing cost of maintaining it, not to mention the potential cost of the critical system failing because of human error.

---

**With the right program, personnel, processes and relationships in place, you can be confident that mistakes will be minimized, and incident response will be optimized.**

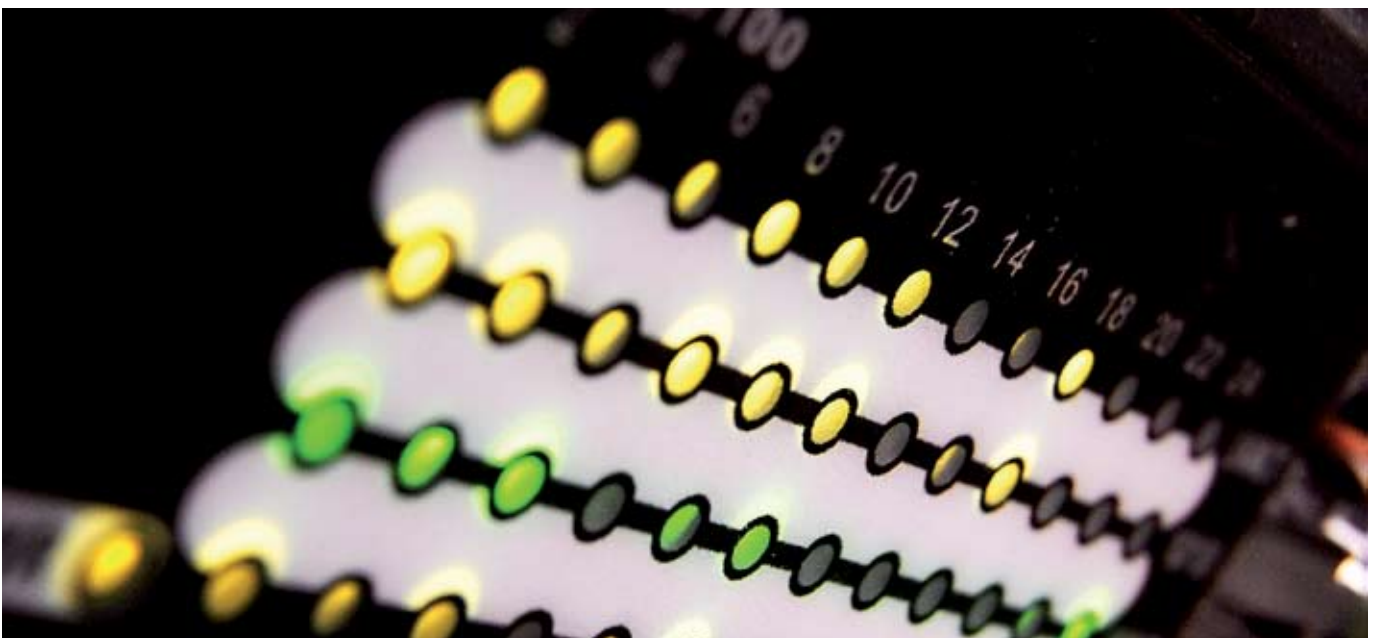
---

While you may not eliminate all human errors, when the right program, personnel, processes, and relationships are in place, you can be assured that mistakes due to lethargy or complacency will be minimized. A robust program will further ensure that when incidents do occur, a calculated and measured response will minimize or avoid any further impact to your business operation. The following five steps are essential to begin building the right program for any CE:

1. Audit your existing systems
2. Review your personnel
3. Introduce personnel development programs
4. Implement a training program for all staff and contractors
5. Set up a working group with real estate and IT representatives to discuss and collaborate

Maintaining a rigorous CE program is a continuous improvement process and should not be treated as a one off exercise.

By taking proactive steps today to assess the management of your CE and to implement a rigorous program, you will benefit from minimized risks, greater efficiencies, and performance enhancements that will underpin the viability of your business both now and over the long-term.



### About Jones Lang LaSalle Critical Environment Management

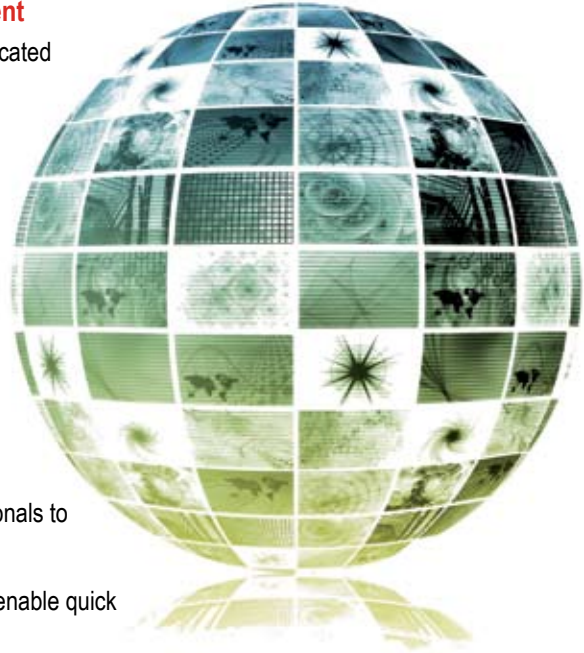
Jones Lang LaSalle has a specialized team of 630 professionals dedicated to critical environment management (CEM) in Asia Pacific. Our CEM team manages over 2.7 million sq ft of commercial critical space on behalf of 54 clients across the region.

With an overarching goal of system reliability and continuous, uninterrupted operation, we implement a tailored approach to managing each client's critical environment, featuring:

- Diagnostic analysis of existing systems and procedures
- Preparation of a comprehensive transition plan to facilitate the migration of the system over to new protocols
- Appointment of specialized management and engineering professionals to lead the implementation of the new system
- Provision of state-of-the-art management and engineering tools to enable quick and effective implementation of new CEM practices
- Programmed reviews and benchmarking exercises of the new CEM system

Our CEM team provides clients with minimized risk of system down time, maximum efficiency of the installed infrastructure and benefits from the team's strategic global relationships with contractors and suppliers.

Furthermore, clients stand to enjoy the benefits of our ongoing experience managing critical environments in a variety of industrial sectors, experience which facilitates constant exposure to the industry's latest innovations and best practices.



**Rob Timmermans**

Head of Engineering & Operations Solutions, South Asia  
Chair, Critical Environment Management Board, Asia Pacific  
robert.timmermans@ap.jll.com

Rob leads Jones Lang LaSalle's Engineering & Operations Solutions group in South Asia. In this role, he is responsible for the operational performance of the Firm's managed properties on behalf of owners and investors. A key focus is the development and implementation of standard operational policies and procedures.

Rob has been with the Firm for over 14 years and has held a number of positions in the areas of both property and facilities management. He has worked with a number of the world's largest investment banks. Rob also chairs the Asia Pacific Critical Environment Management Board and has led the development of the company's regional and global critical environment management program.



### Jones Lang LaSalle offices

#### Asia Pacific

9 Raffles Place  
#39-00 Republic Plaza  
Singapore 048619  
tel +65 6220 3888  
fax +65 6438 3361  
www.joneslanglasalle.com.sg

#### Americas

200 East Randolph Drive  
Chicago IL 60601  
tel +1 312 782 5800  
fax +1 312 782 4339  
www.joneslanglasalle.com

#### Europe

22 Hanover Square  
London W1A 2BN  
tel +44 20 7493 6040  
fax +44 20 7408 0220  
www.joneslanglasalle.co.uk

### Jones Lang LaSalle worldwide

#### Asia Pacific

Adelaide	Macau
Auckland	Manila
Bangalore	Melbourne
Bangkok	Mumbai
Beijing	New Delhi
Brisbane	Newcastle
Canberra	Osaka
Cebu City	Pasig
Chandigarh	Penang*
Chengdu	Perth
Chennai	Phuket
Coimbatore	Pune
Guangzhou	Quezon City
Hanoi	Seoul
Hokkaido	Shanghai
Ho Chi Minh City	Shenzhen
Hong Kong	Singapore
Hyderabad	Sydney
Jakarta	Taguig
Johor Bahru*	Taipei
Kolkata	Tianjin
Kuala Lumpur*	Tokyo
Liverpool	Wellington

#### Americas

Atlanta  
Austin  
Baltimore  
Boston  
Buenos Aires  
Chicago  
Cincinnati  
Cleveland  
Columbus  
Dallas  
Dayton  
Denver  
Detroit  
Ft. Lauderdale  
Houston  
Kansas City  
Los Angeles  
McLean, VA  
Mexico City  
Miami  
Minneapolis  
Monterrey  
Montreal  
New Orleans  
New York  
Orange County  
Orlando  
Parsippany, NJ  
Philadelphia  
Phoenix  
Pittsburgh  
Portland, OR  
Rio de Janeiro  
Sacramento  
St. Louis  
Salt Lake City  
San Diego  
San Francisco  
Santiago  
Sao Paulo  
Seattle  
Tampa  
Toronto  
Vancouver  
Washington DC

#### EMEA

Abu Dhabi  
Amsterdam  
Antwerp  
Barcelona  
Berlin  
Birmingham  
Brussels  
Bucharest  
Budapest  
Dubai  
Dublin  
Dusseldorf  
Edinburgh  
Eindhoven  
Frankfurt  
Glasgow  
Gothenburg  
The Hague  
Hamburg  
Helsinki  
Kiev  
Leeds  
Lisbon  
London  
Luxembourg  
Lyon  
Madrid  
Manchester  
Marbella  
Milan  
Moscow  
Munich  
Norwich  
Paris  
Prague  
Rotterdam  
Seville  
Stockholm  
St. Petersburg  
Tel Aviv  
Utrecht  
Valencia  
Warsaw  
Wiesbaden

\*Services in Malaysia are provided through a strategic alliance with Jones Lang Wootton Malaysia.