



Trusted Information  
Sharing Network  
for Critical Infrastructure Protection

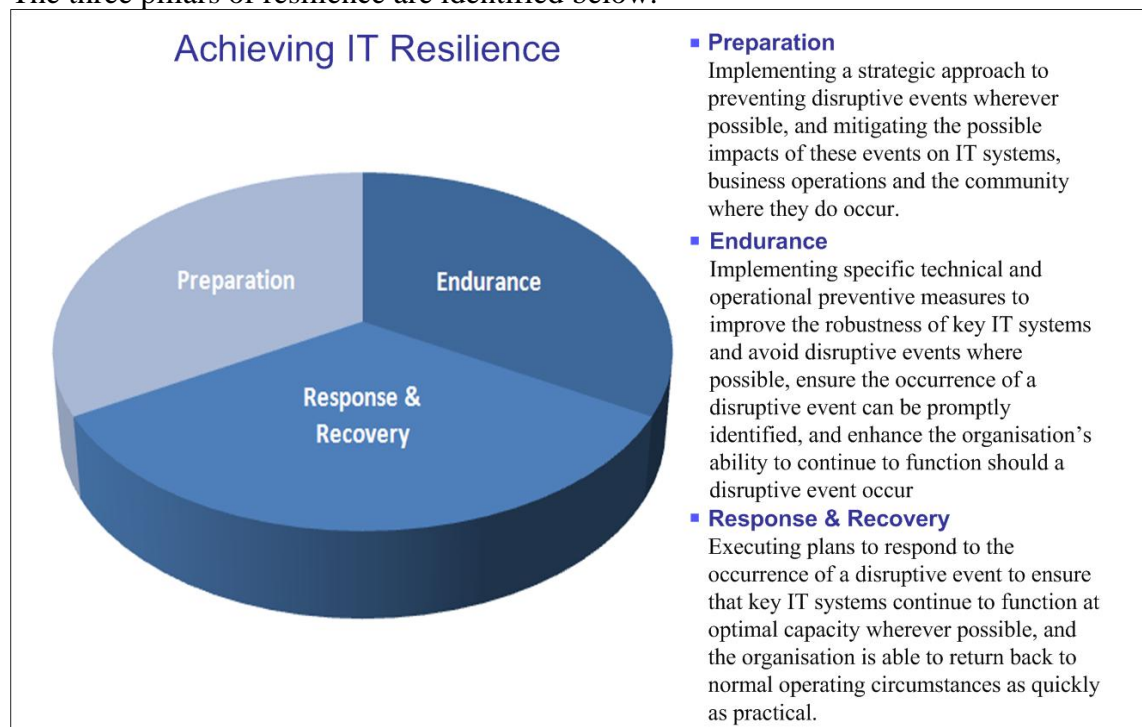
## Achieving IT Resilience – Overview for CEOs

In today's 24 x 7 world, the community expects all organisations with a role in essential services to be resilient in the face of threats to their continued operations. This requires a culture of resilience in the organisation: a culture that is supported by concrete actions and processes.

Hazards that pose a threat to IT systems arise from a vast number of areas, ranging from natural disasters to crime, and from equipment failures to terrorist attack. To address this threat requires organisations to combine thinking from areas ranging from risk management, emergency and business continuity management and information security and audit.

However, resilience does not need to be a purely defensive concept. With resilience also comes opportunity. Organisations that recover quickly after a disaster will find a market ready to embrace them, turning crisis into growth and success.

The three pillars of resilience are identified below.



The Trusted Information Sharing Network (TISN) Resilience Community of Interest has identified eight resilience enablers. These enablers raise important considerations for the organisation's IT environment:

**DISCLAIMER: To the extent permitted by law, this document is provided without any liability or warranty. Accordingly, it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgement of users. The document is intended as a general guide only and users should seek professional advice as to their specific risks and needs.**

Enabler	Considerations
Awareness	<ul style="list-style-type: none"> <li>IT leaders must be aware of potential threats to operations from <i>all hazards</i>, and have a considered plan for response.</li> <li>The organisation should have an understanding of the thresholds beyond which the organisation's response plans will be overwhelmed.</li> </ul>
Agility	<ul style="list-style-type: none"> <li>Established response plans must be able to adapt and evolve in an actual incident situation.</li> </ul>
Communication	<ul style="list-style-type: none"> <li>Internal communication channels must be clearly defined and understood.</li> <li>The IT team should engage with external communities of interest and advisory groups (e.g. CERT Australia) and should have mechanisms to identify emerging threats and trends.</li> </ul>
Leadership	<ul style="list-style-type: none"> <li>IT leaders must take 'ownership' of their need for resilience, identifying weaknesses and appropriate solutions.</li> </ul>
Culture	<ul style="list-style-type: none"> <li>Resilience is not 'set and forget'. The culture of the IT organisation must be one that is constantly learning, and is able to adapt and innovate in times of crisis.</li> </ul>
Change	<ul style="list-style-type: none"> <li>As new ways of working are implemented – such as teleworking, cloud computing, software as a service and virtualisation – your IT team needs to stay on top of the implications to resilience and continuity.</li> <li>Such knowledge takes time to develop, so making time available above and beyond 'business as usual' operational tasks will be rewarded with a flexible team.</li> <li>Speed to change can be critical in a time of crisis – developing an ability to make rapid system changes when required is essential to manage unclear threats.</li> </ul>
Integration	<ul style="list-style-type: none"> <li>Resilience crosses teams within the organisation – risk, audit, IT, facilities management and more – and all of these groups need to have an open dialogue.</li> </ul>
Interdependency	<ul style="list-style-type: none"> <li>Your IT systems will almost certainly rely on other companies as suppliers, outsourcers, and partners. These firms are just as important to your resilience as your own internal capability and need to be engaged as such.</li> </ul>

Any approach to achieving IT resilience will require action to be taken at both technical and operational levels. Implementing a strategic approach for handling hazardous events – and, wherever possible preventing them entirely – best equips your organisation to maintain operational capacity during a crisis.

However, resilience also flows from a strong governance framework that is spearheaded by the leaders of the organisation and which takes into account legal and regulatory requirements. Establishing a culture of resilience is central to satisfying community expectations and to foster an approach for handling hazardous events that takes into account emerging threats and technology trends.

**End of Document**