

PAS 60518:2020

Developing and implementing enterprise risk and resilience management (ERRM) in utilities – Guide



هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority



bsi.

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2020.

Published by BSI Standards Limited 2020.

ISBN 978 0 539 12480 4

ICS 03.100.01

No copying without BSI permission except as permitted by copyright law.

Publication history

First published July 2020

Contents

Foreword	iii
0 Introduction	1
1 Scope	4
2 Normative references	5
3 Terms, definitions and abbreviations	6
4 Utility operating models	8
5 Enterprise risk and resilience	10
6 Risk	13
7 Resilience	21
8 Developing organization-wide resilience	25
9 Risk and resilience reporting	29
Annex	
Annex A (informative)	
Risk and resilience, examples, templates and development tools	33
Bibliography	44
List of figures	
Figure 1 – Cost versus risk decisions	2
Figure 2 – Integrated enterprise risk and resilience management (ERRM) model	3
Figure 3 – Generic utility model	8
Figure 4 – BS ISO 31000:2018 risk management process	9
Figure 5 – Risk escalation	11
Figure 6 – Risk matrix for evaluation and prioritization of risks	17
Figure 7 – Example timeframes for risk mitigation actions related to major assets	19
Figure 8 – Example of business unit risk register headings for recording risk information	19
Figure 9 – Linking risk and resilience	21
Figure 10 – Identifying where BCPs are to be used	23
Figure 11 – Overview of the resilience actions to resist, respond, recover and reinforce	25
Figure 12 – Example of a resilience framework	27
Figure 13 – Societal support to reduce demand to address capability gaps	28

Figure 14 – Example of an environmental heatmap 30
Figure 15 – Example of governance template headings 30
Figure A.1 – Example of likelihood levels 33
Figure A.2 – Example of consequence criteria 33
Figure A.3 – Example application of legislation to existing and new infrastructure 35
Figure A.4 – Example of a process criticality development template 36
Figure A.5 – Example of loss of site and supporting business continuity and recovery plans 37
Figure A.6 – Assessment system to decide criticality of staff for redeployment 38
Figure A.7 – Example of incident escalation levels 38
Figure A.8 – Generic incident management structure 39
Figure A.9 – Functions and responsibilities in a generic incident management structure 39
Figure A.10 – Actions a utility can take to improve its resistance, to withstand shocks or extreme events 41
Figure A.11 – Actions a utility can take before an event to improve its response capability 42
Figure A.12 – Actions to recover from an event 43

List of Tables

Table 1 – Examples of high-level controls 15
Table 2 – The four phases of the IMP 24
Table 3 – Example of an initial risk and resilience maturity assessment method for utilities 32
Table B.1 – Recovery team responsibilities 37



Foreword

This PAS was sponsored by the Dubai Electricity and Water Authority (DEWA). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on 1 July 2020.

Acknowledgement is given to the following organizations that were involved in the development of this PAS as members of the steering group:

- Dubai Electricity and Water Authority (DEWA);
- Électricité de France (EDF);
- National Grid;
- Rheinisch-Westfälisches Elektrizitätswerk AG (RWE);
- Right Stone Consulting;
- United Utilities; and
- Watercare Services Limited New Zealand.

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

The British Standards Institution retains ownership and copyright of this PAS. BSI Standards Limited as the publisher of the PAS reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This PAS will be reviewed at intervals not exceeding two years, and any amendments arising from the review will be published as an amended PAS and publicized in Update Standards.

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a guide to be rapidly developed in order to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Use of this document

As a guide, this PAS takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it.

It has been assumed in the preparation of this PAS that the execution of its provisions will be entrusted to appropriately qualified and experienced practitioners and professionals, for whose use it has been produced.

Information about this document.

Copyright is claimed on Figure 2, Figure A.8 and Figure A.9. Copyright holder of Figure 2 is Watercare Services Limited. Copyright holder of Figure A.8 and Figure A.9 is the New Zealand Government.

Presentational conventions

The guidance in this standard is presented in roman (i.e. upright) type. Any recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. “organization” rather than “organisation”).

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.

0 Introduction



NOTE HH Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the United Arab Emirates and Ruler of Dubai, inaugurates the 200 MW second phase of the Mohammed bin Rashid Al Maktoum Solar Park in Dubai.

0.1 Utilities guide for the development and implementation of enterprise risk and resilience management (ERRM)

Electricity, gas and water utilities across the world are facing an array of challenges. They are expected to manage risks to their services, meet their obligations and manage existing liabilities while improving organizational resilience in order to resist, respond to, and recover from unexpected events. Governments, regulators, customers and the public expect utilities to maintain services, and when a service is interrupted, quickly fix the problem while minimizing the impact.

Meeting these expectations is challenging and requires utilities to adopt a proactive approach to risk and resilience management – identifying risks, understanding consequences and the speed at which these can occur, and taking appropriate short-, medium- and long-term actions to increase organizational resilience.

This drives requirements for continuous development in the skills of utilities leadership and staff, and the upgrading of existing and provision of new high-cost infrastructure to provide increased resilience. While infrastructure requirements and associated costs continue to rise, customers expect to receive more services at a reduced price.

This position is further complicated by changes in climate, population growth, the rapidly changing technological landscape, social norms and the continual push for utilities to encourage customers to be economical.

Customers expect organizations to take notice of, and act to address, their concerns and complaints. Failure to do so can result in escalation of complaints to the organization's management and the media. Transfer of dissatisfied customers to competing utilities is often quick and easy, so utilities need to assess customer sensitivity, e.g. in terms of numbers of customer complaints about an issue, to develop reputational trigger points for action.

Utilities are moving into a new and more complex environment. For example, electricity generation is becoming more distributed, and through technology, is moving closer to the consumer. Smarter solutions are required to effectively manage network operations and the digital ecosystem.

For utilities to thrive, forecasting needs to identify disruptive technologies that have the potential to change investment pathways, reduce demand and alter the way services are provided.

This PAS is designed to lead utilities through the process of:

- developing and driving risk management capability;
- identifying threats, opportunities and related trends;
- assessing the requirements for a range of business continuity plans (BCPs);
- evolving the crisis/incident management capability to manage all potential disruptive events;
- building adaptive capacity, including an enterprise learning capability for resilience; and
- understanding risk, so that utilities can focus their limited resources on areas where enhanced resilience is most needed.

0.2 Navigating the challenges

Utilities need to find ways to navigate through the array of business, social and environmental challenges by understanding and managing risk and increasing resilience in the context of:

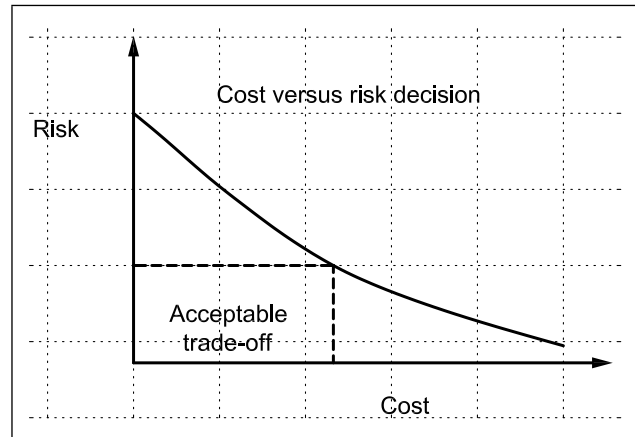
- achieving organizational objectives;
- meeting customer expectations;
- acting in accordance with key business values;
- assessing risk tolerance and appetite;
- meeting regulatory requirements;
- keeping up with technological advancement; and
- responding to unpredictable, disruptive and sometimes extreme events.

These challenges can exceed what can be achieved with available funding, therefore a range of factors are to be taken into account during decision making. These factors include cost if the risk impacts and cost of mitigating the risk, risk tolerance and potential reputational impact. In addition, some level of risk will be accepted where the cost of further risk reduction does not make economic sense.

Risk-based decision making and performance management are essential considerations for utilities as they make key strategic decisions on future business models, innovation, asset investment, revenue protection and diversification.

Figure 1 provides an illustration of cost versus risk decisions.

Figure 1 – Cost versus risk decisions



In changing times with increasing uncertainty and complexity, utilities need to develop the key areas of proactive risk management, risk-based decision making and processes to improve resilience. This enables them to build adaptive capacity to resist, respond to and recover from an increasing array of foreseeable and unexpected dynamic and disruptive challenges.

Resilience comprises a range of short-, medium- and long-term measures that help a utility build the adaptive capacity needed to withstand stresses and shocks. By developing ERRM capability, utilities can also identify opportunities where benefits (related to objectives) can be realized.

0.3 Enterprise risk and resilience management (ERRM)

Enterprise risk management (ERM) can be defined as the methods and processes used by utilities to manage risks, increase resilience and identify opportunities related to the achievement of their objectives.

ERRM builds on ERM and is designed to be an integrated and joined-up approach to managing risk and improving resilience across a utility and its extended networks. It provides a way to determine the level of organizational investment to be made to increase organizational resistance, as well as response and recovery capability.

ERRM can identify positive benefits related to achievement of objectives. ERRM can also:

- maximize organizational capability;
- identify potential opportunities and encourage innovation;
- improve situational awareness;
- inform risk management, including areas where more risk could be accepted;

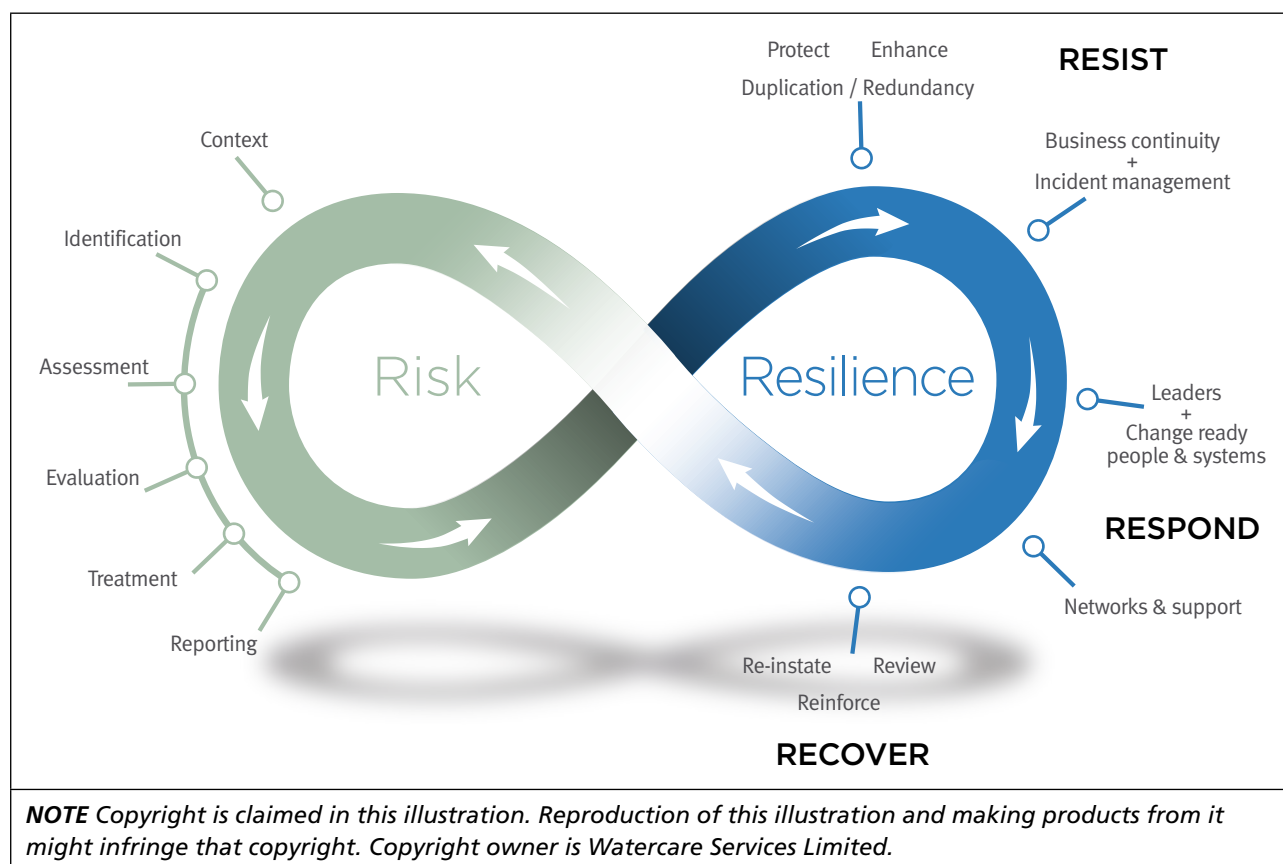
- identify areas where business continuity and incident management plans are required;
- improve resilience, including response and recovery capability;
- aid decisions on capital investment to increase organizational resistance; and
- provide assurance that business plans are robust and satisfy regulatory scrutiny.

Effective risk and resilience practices take time to build and are driven by the leadership team which is responsible for making these practices part of the utility's culture, championing change through personal demonstration of their commitment. It is a continuing journey as the social and technological environment changes.

This PAS is designed to provide a path to ordered development, improving risk, business continuity and the resilience of utilities over time.

Figure 2 provides an overview of the integrated ERRM model.

Figure 2 – Integrated enterprise risk and resilience management (ERRM) model



1 Scope

This PAS gives guidance on developing and implementing enterprise risk and resilience management (ERRM) and supporting business continuity and incident management plans, in order to improve the resilience to help withstand unexpected future shocks and extreme events. It is designed for use by electricity, gas, water and wastewater utilities of all sizes in public and private sectors.

This PAS is an overarching guide designed for use by utilities which encapsulates relevant risk and resilience-related guidance and their application using industry examples.

This PAS is designed for use by:

- electricity and gas providers, including generation, transmission, distribution and supply organizations; and
- water and wastewater providers, including supply, treatment, transmission and network operation organizations.

This PAS does not cover:

- governance and compliance with specific national and international legislation and regulations; or
- nuclear safety case risks, except for those areas common to all power generators.

ERRM is intended to work with the utility, aiding controls, governance, oversight and improving support and performance.

This PAS accepts that utilities across the world are at different stages in their risk and resilience journeys and have differing maturity levels.

This PAS is structured to guide utilities along the path to enhancing risk and resilience capabilities and to allow a basic assessment of maturity to guide on the next development steps to take.

This PAS also guides on approaches to risk and resilience reporting to communicate the utility's position in respect of ERRM.

This PAS reflects the change in resilience thinking, which was previously thought of in terms of the ability to recover quickly from difficulties, but is now increasingly regarded as the ability to survive a crisis and thrive in a world of uncertainty.

It is also designed to guide the development of:

- an overarching incident management plan to respond to unforeseen extreme events when they occur; and
- a range of ways to build adaptive capacity and increase utility resilience.

Annex A of this PAS provides some related examples to aid understanding.