Industrial control system (ICS) security

Operations technology and ICS

Operations technology (OT) is the term used in industrial operations. It comprises control systems, networks and other industrial automation components that control physical processes and assets. Control systems are at the heart of the nation's critical infrastructure, which includes electric power, oil and gas, water and waste water, manufacturing, transportation, agriculture and chemical factories.

ICSs, which are a part of the OT environment in industrial enterprises, encompass several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and other smaller control system configurations such as programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices (IEDs) and other field devices.

ICSs were originally designed to increase performance, reliability and safety by reducing manual effort. Security was achieved by physical isolation, or a so-called air gap (security by obscurity).

Today, the world is talking about connecting everything to the Internet. The fourth industrial revolution (Industry 4.0), a term used to draw together cyber-physical systems, the Internet of things (IoT) and Internet of services, has started to find more resonance with OEMs, system integrators and asset owners. Thus, it is only a matter of time before a lot of ICS information is routed to sophisticated applications across enterprises through a wide area network where security by obscurity no longer offers valid protection. Governments plan to connect ICSs to the Internet for projects such as smart grids and smart cities, which will significantly increase the risk of intrusion from malicious actors.

Threat to ICS sector

With ICS increasingly getting integrated with the corporate network and Internet to meet business requirements, the sector is obviously opening itself to the world of attackers. This is evident from many global information security surveys, including the widely followed one by ICS-CERT. As highlighted in the figure below, almost all critical infrastructure is targeted.

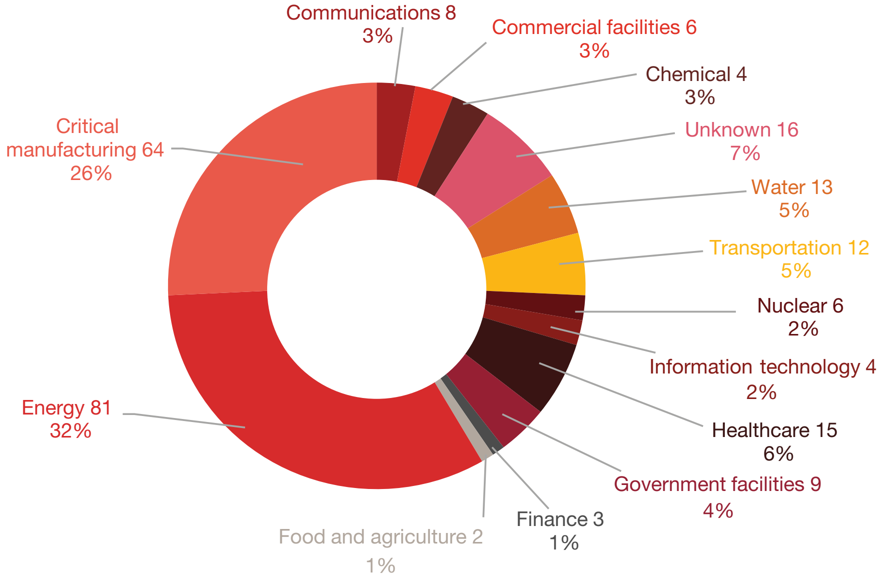
There are two major types of security threats associated with ICS:

Inadvertent

- Safety failures
- Natural disasters
- Equipment failures
- Human mistakes

Deliberate

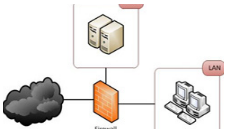
- Disgruntled employees
- Industrial espionage
- Cyber hackers
- Viruses and worms
- Terrorism



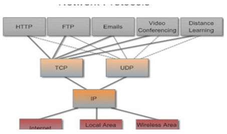
Source: ICS CERT

ICSs have various weaknesses, which make them easy targets for attackers:

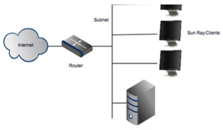
Legacy control system



Lack of cyber security considerations in network architecture/segmentation

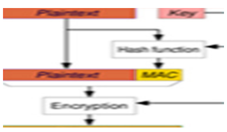


Poor network protocol implementation



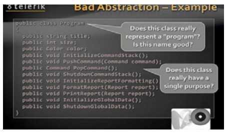
Weak network component configuration

Plain text traffic



Insecure encryption and authentication for wireless ICS networks

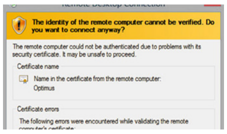
Weak protection of ICS systems from the enterprise IT network


telerik
Bad Abstraction – Example
Does this class really represent a "program"? Is this name good?
Does this class really have a single purpose?

Poor programming and code quality

Vulnerable web services

Poor passwords practices and weak authentication



The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

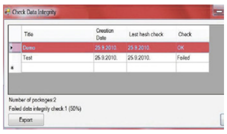
Certificate name

Name in the certificate from the remote computer:
Optimus

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

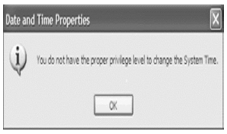
Insecure remote connectivity to ICS networks



No integrity checks at critical asset level

Software patches are playing an increasingly important role as organizations look to plug holes in their applications before the bad guys can exploit them.
Baseline

Poor patch management



Date and Time Properties

You do not have the proper privilege level to change the System Time.

Least user privilege violation

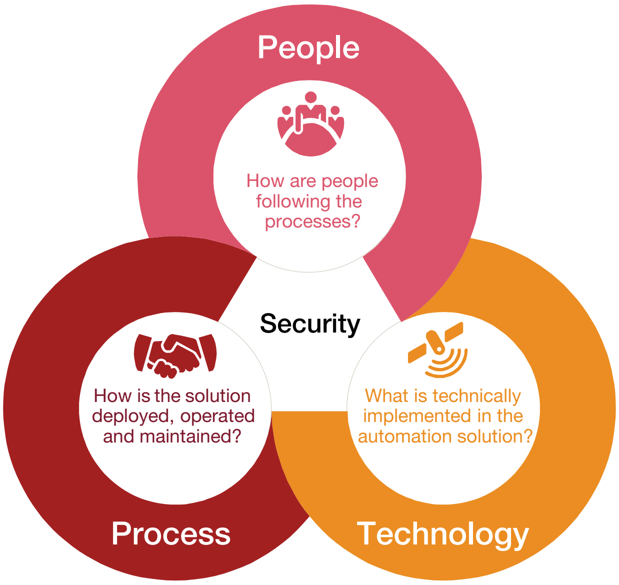
With cyberattacks continuing to escalate in frequency, severity and impact year after year, ensuring the cyber security of these systems is of paramount importance.

Adapting standards

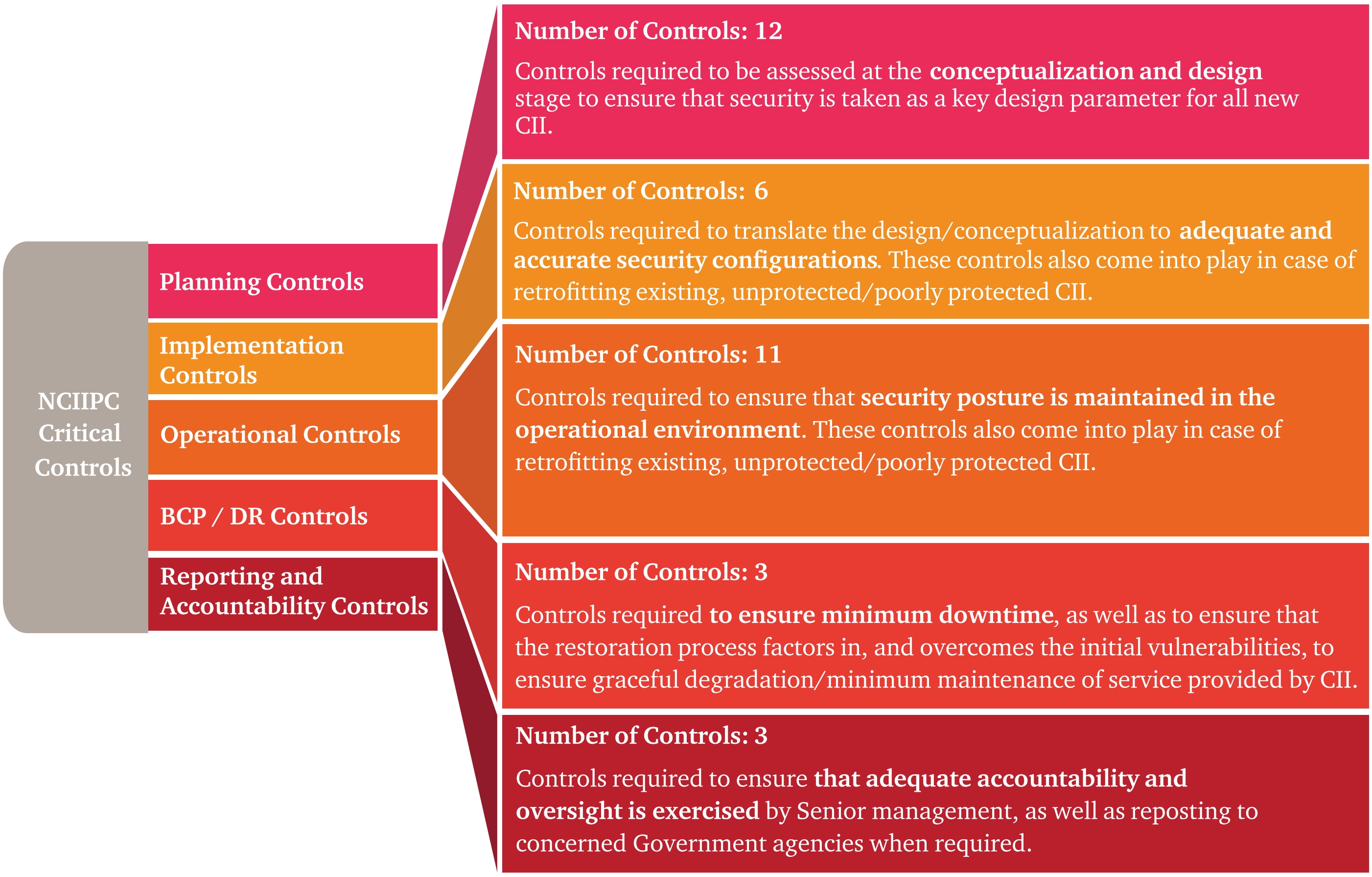
To overcome ICS threats, many government agencies, non-profit organisations and nation states have developed different standards over the years. A few of the standards are country specific, while a few others are globally applicable.

These standards provide guidance for developing ‘defence-in-depth’ strategies to organisations that use ICS components. These standards provide information related to secure configuration, best practices, security policy, secure network architecture and secure operating procedures.

Three factors are very critical to these standards: process, technology and people. Together, they are responsible for the security of the system.


People
How are people following the processes?
Security
How is the solution deployed, operated and maintained?
Process
What is technically implemented in the automation solution?
Technology

In India, the National Critical Information Infrastructure Protection (NCIIPC) guidelines are used by the public and private sectors to secure the critical national infrastructure.



NCIIPC Critical Controls

Planning Controls

Number of Controls: 12

Controls required to be assessed at the **conceptualization and design** stage to ensure that security is taken as a key design parameter for all new CII.

Implementation Controls

Number of Controls: 6

Controls required to translate the design/conceptualization to **adequate and accurate security configurations**. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.

Operational Controls

Number of Controls: 11

Controls required to ensure that **security posture is maintained in the operational environment**. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.

BCP / DR Controls

Number of Controls: 3

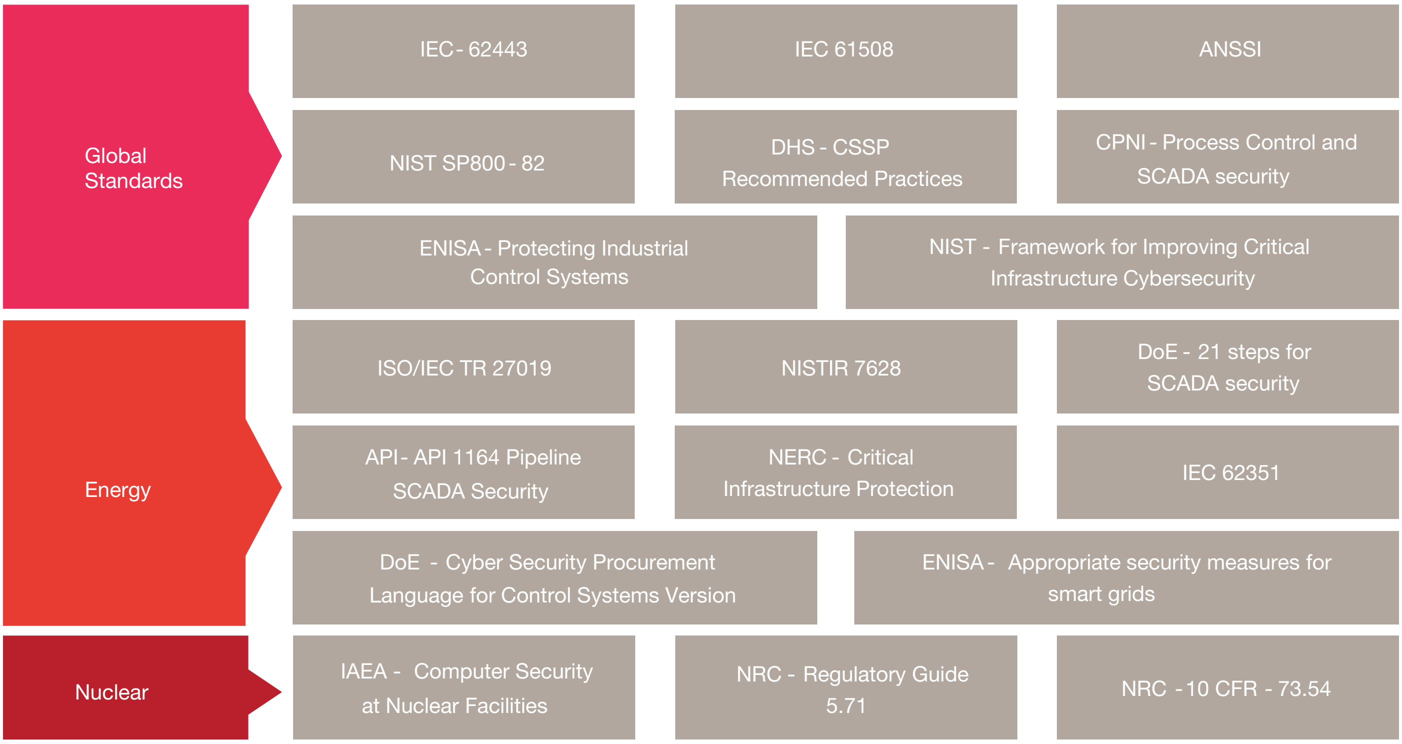
Controls required **to ensure minimum downtime**, as well as to ensure that the restoration process factors in, and overcomes the initial vulnerabilities, to ensure graceful degradation/minimum maintenance of service provided by CII.

Reporting and Accountability Controls

Number of Controls: 3

Controls required to ensure **that adequate accountability and oversight is exercised** by Senior management, as well as reposting to concerned Government agencies when required.

Global ICS security standards:



Global Standards

IEC - 62443

IEC 61508

ANSSI

NIST SP800 - 82

DHS - CSSP Recommended Practices

CPNI - Process Control and SCADA security

ENISA - Protecting Industrial Control Systems

NIST - Framework for Improving Critical Infrastructure Cybersecurity

Energy

ISO/IEC TR 27019

NISTIR 7628

DoE - 21 steps for SCADA security

API - API 1164 Pipeline SCADA Security

NERC - Critical Infrastructure Protection

IEC 62351

DoE - Cyber Security Procurement Language for Control Systems Version

ENISA - Appropriate security measures for smart grids

Nuclear

IAEA - Computer Security at Nuclear Facilities

NRC - Regulatory Guide 5.71

NRC - 10 CFR - 73.54

Each sector faces different challenges and threats, and the standards vary accordingly. For example, NERC CIP applies to the energy sector, while a few standards are globally applicable, such as IEC 62443.

How PwC can help

1 ***Strategy and governance***
Defining a comprehensive cyber security strategy, prioritising investments and aligning security capabilities with strategic imperatives of the organisation

2 ***Security architecture***
Defining business-driven security architecture to protect business critical information

3 ***Security implementation***
An integrated approach towards selecting and implementing security solutions

4 ***Threat and vulnerability management (TVM)***
Establishing a TVM programme to protect, detect and respond to vulnerabilities in technologies

5 ***Risk and compliance***
Effective management of compliance with organisational policies and industry-specific regulatory requirements and standard like NIST and IEC62443

6 ***Incident management***
Establishing a cyber response framework to contain security incidents and minimise damage

7 ***Managed services***
Establishing and managing best-in-class security operations centres for clients

8 ***Identity and access management***
Taking into account business requirements and trends to provide a holistic view for managing and maintaining identities

PwC tailors its services based on the sector and its criticality. PwC provides cyber security services to increase the security posture of your ICS/OT systems from threats. Some of the services are as follows:

1) ICS risk assessments

As a first step, we conduct a security assessment of the ICS infrastructure based on custom or relevant standards to assess the current state vs security best practices.

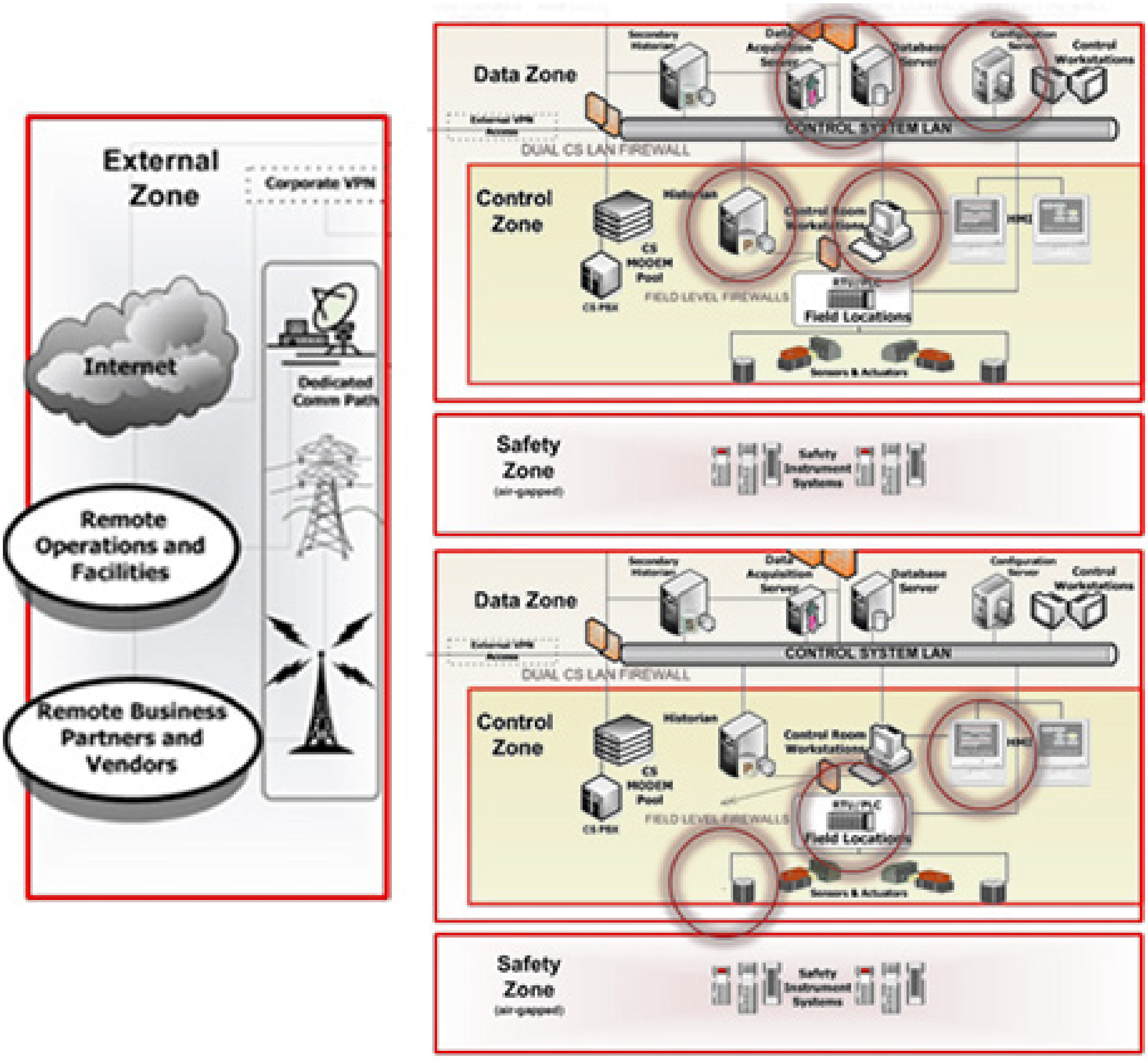
The assessment covers system records and activities to determine the adequacy of system controls. The activities include a review of network architecture and network security systems configuration to assess the operating efficiency of technical controls.

2) ICS vulnerability assessment (VA)/penetration testing (PT)

Our cyber security team is well versed with the ICS environment and its challenges. We have subject matter experts in VA/PT of ICS components.

A three-step approach is followed to examine the ICS security posture:

- Test ICS network from the Internet
- Test ICS network from IT
- Testing selected offline ICS systems for vulnerabilities



Source: ICS-CERT US

3) Compliance assistance

PwC can help industries in adapting the international and country-specific security standards mentioned in a previous section of this document. We can also can help industries to develop their own ICS standards and policies based on the environment's criticality.

4) Security operations centre (SOC):

PwC provides services SOCs to set up a combined ICS-IT environment, which will enable you to monitor and act upon the treats and attacks.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,08,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

Contacts

Sivarama Krishnan
Leader, Cyber Security
Tel: +91 (124) 626 6707
sivarama.krishnan@in.pwc.com

Siddharth Vishwanath
Partner, Cyber Security
Tel: +91 (22) 66691559
siddharth.vishwanath@in.pwc.com

Manu Dwivedi
Partner, Cyber Security
Tel: +91 (0) 80 4079 7027
manu.dwivedi@in.pwc.com

Sundareshwar Krishnamurthy
Partner, Cyber Security
Tel: +91 (22) 6119 8171
sundareshwar.krishnamurthy@in.pwc.com

Hemant Arora
Executive Director, Cyber Security
Tel: +91 (124) 626 6717
Hemant.arora@in.pwc.com

PVS Murthy
Executive Director, Cyber Security
Tel : +91 (22) 66691214
pvs.murthy@in.pwc.com

pwc.in

Data Classification: DC0

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

MJ/August2016-7136