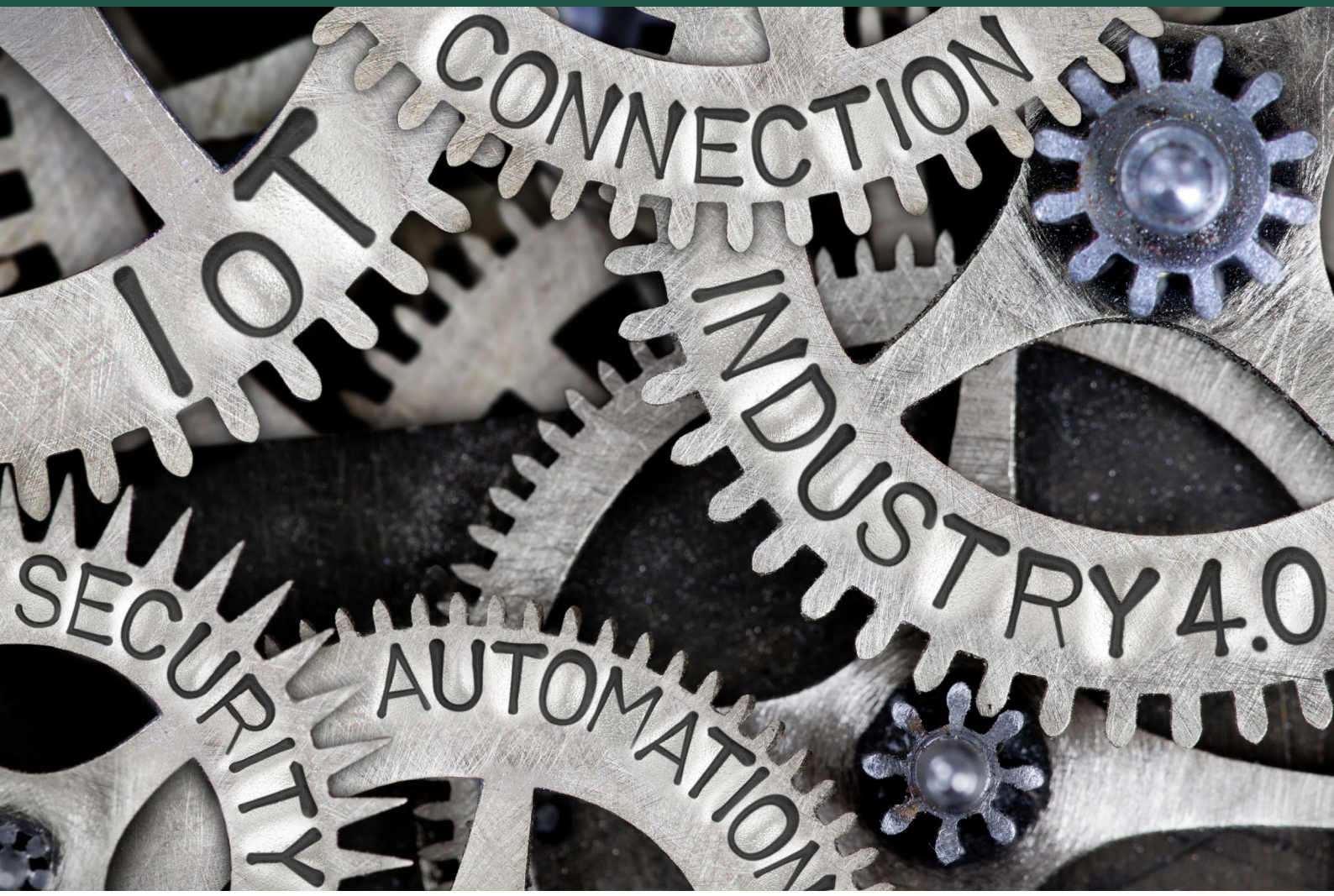
PAS 1085:2018

Manufacturing – Establishing and implementing a security-minded approach – Specification



Innovate UK

bsi.

Publishing and copyright information

ISBN 978 0 580 52421 9

ICS 03.100.50, 25.040.40, 35.030

Publication history

First published May 2018

Contents

List of figures

Foreword

This PAS (Publicly Available Specification) was sponsored by Innovate UK. Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on 31 May 2018.

Acknowledgement is given to Hugh Boyes of Bodvoc Ltd., as the technical author and the following organizations that were involved in the development of this PAS as members of the steering group:

- Arup
- B.H. Development
- Bodvoc Ltd
- BuroHappold Engineering
- Centre for Process Innovation (CPI)
- Co-opted member
- Costain Group plc
- Cranfield University
- Digital Catapult
- High Value Manufacturing Catapult (HVMC)
- Innovate UK
- The Manufacturing Technologies Association (MTA)
- National Cyber Security Centre (NCSC)
- Rockwell Automation
- Warwick Manufacturing Group (WMG)

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

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 It will be withdrawn upon publication of its content in, or as, a British Standard.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 specification 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

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

Presentational conventions

The provisions of this PAS are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the principal auxiliary verb is "shall".

Commentary, explanation and general informative material is presented in 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").

Requirements in this PAS are drafted in accordance with *Rules for the structure and drafting of UK standards*, subclause **G.1.1**, which states, "Requirements should be expressed using wording such as: 'When tested as described in Annex A, the product shall ...'". This means that only those products that are capable of passing the specified test will be deemed to conform to this PAS.

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.

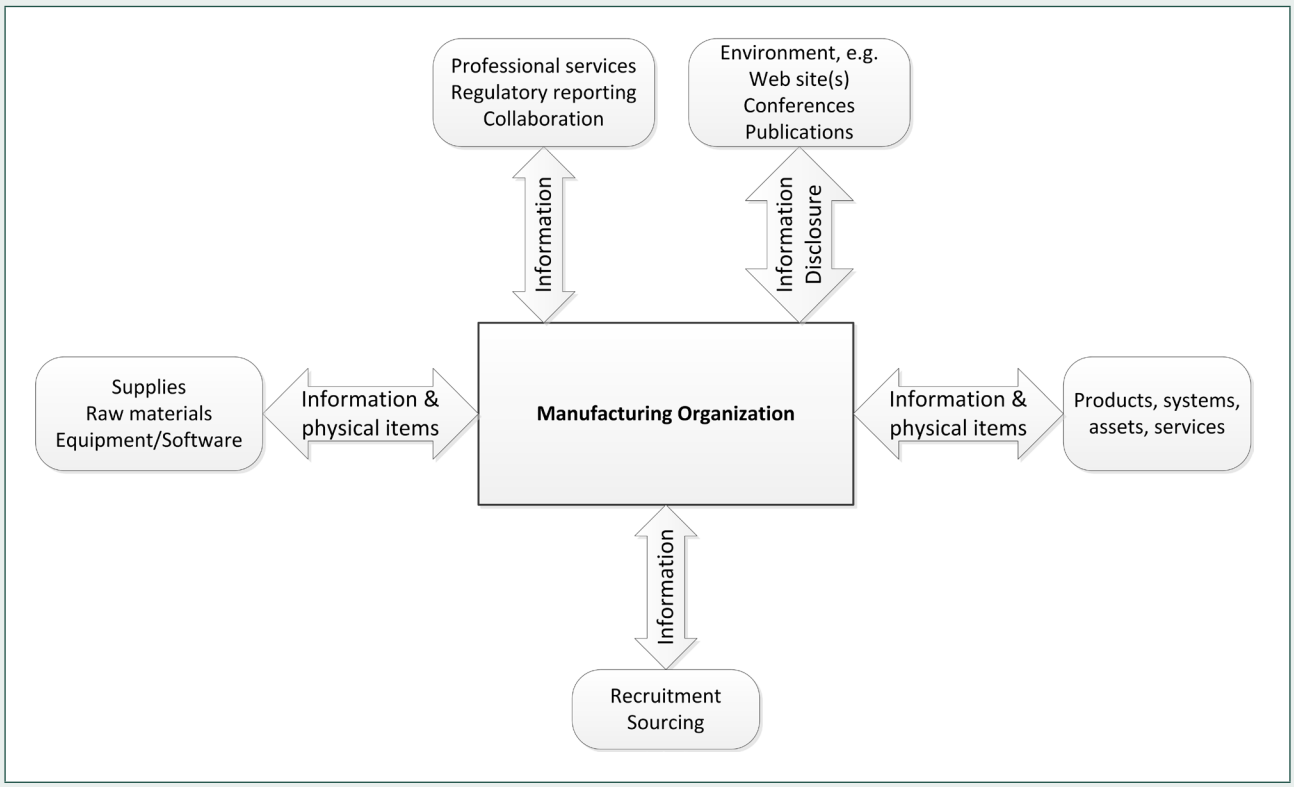
Particular attention is drawn to the following specific regulations:

- Data Protection Act 1998 [1]
- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2]
- Trade Union and Labour Relations (Consolidation) Act 1992 [3]
- Environmental Information Regulations 2004 [4]
- Freedom of Information Act 2000 [5]
- Freedom of Information (Scotland) Act 2002 [6]
- Computer Misuse Act 1990 [7]
- Control of Major Accident Hazards Regulations 2015 [8]
- Official Secrets Act 1989 [9]
- Re-use of Public Sector Information Regulations 2005 [10]

0 Introduction

An increasing use of digital technologies in the design, manufacture, delivery, operation and disposal of products, systems, assets and services has led to the use of the terms digital manufacturing and industrial digitalization. As a consequence, manufacturing organizations typically exist within a complex digital ecosystem as illustrated in Figure 1.

Figure 1 – The manufacturing organization and its digital ecosystem



The manufacturing organization exchanges information, much of it in digital form, with a diverse range of organizations in addition to handling physical items. Such exchanges can occur using a variety of technologies including email, electronic data interchange (EDI), collaboration portals, digital object libraries and direct connectivity between systems. Many of these exchanges are achieved using information and communications technologies (ICT), which can be referred to as the Internet or the Internet of Things (IoT). It is also important to consider the interactions between these ICT and operational technologies (OT), including the Industrial Internet of Things (IIoT). This increasing digital interaction introduces a number of threats and opportunities to both an organization and its stakeholders, including suppliers, customers and its personnel.

For the purposes of this PAS the term digital also encompasses processing of data and/or information using machine learning, artificial intelligence techniques and the adoption of technology that enables smarter and more autonomous manufacturing processes.

All organizations are dependent to some degree on a supply chain and unless they sell directly to their customers or end users are part of a wider supply chain as illustrated in Figure 2. For manufacturing organizations, their supply chain is likely to include organizations that provide:

- supplies or consumables, raw materials and any equipment or systems and software used in the manufacturing process;
- professional services, e.g. technical, financial and legal services; and
- resourcing services, e.g. recruitment of personnel or provision of temporary labour, sourcing of supplies, raw materials, etc.

The manufacturing organization therefore needs to be aware of and manage security risks relating to it and those that might arise through its supply chain.

Within a manufacturing organization there is a value chain, which is based on a process view of the organization's operations and comprises a set of activities that are performed to deliver its manufactured outputs. Whilst an organization might engage in hundreds of activities in the process of converting inputs and resources into the manufactured outputs, these activities can be classified generally as either primary or support. Figure 3 illustrates a generic value chain that comprises:

- primary activities, i.e. inbound logistics, manufacturing operations, outbound logistics and any product related service delivered to the organization's customers; and
- supporting activities, i.e. enterprise ICT equipment and systems, OT, sales and marketing, resource management and procurement, financial and legal activities.

Figure 2 – Illustrative manufacturing organization with a supply chain

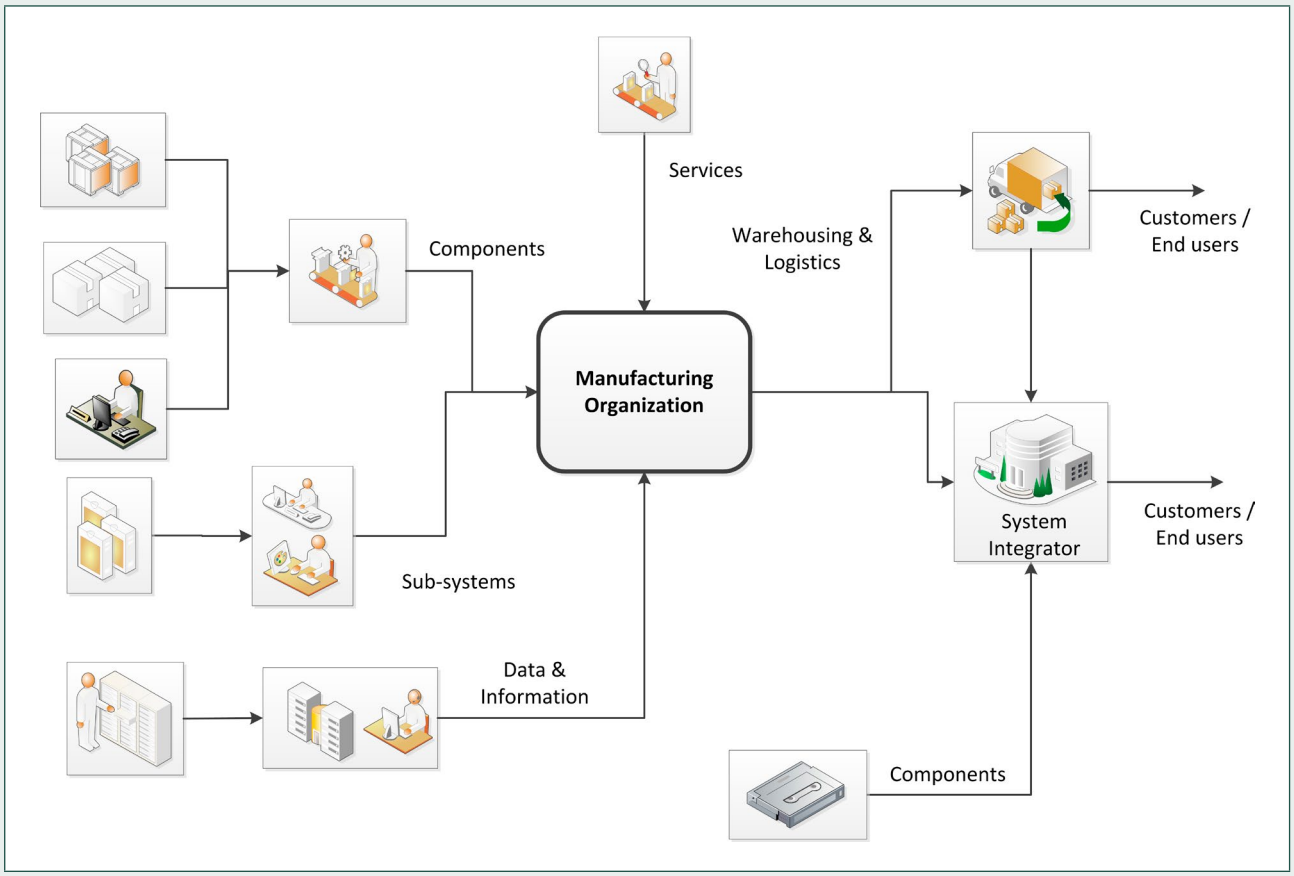
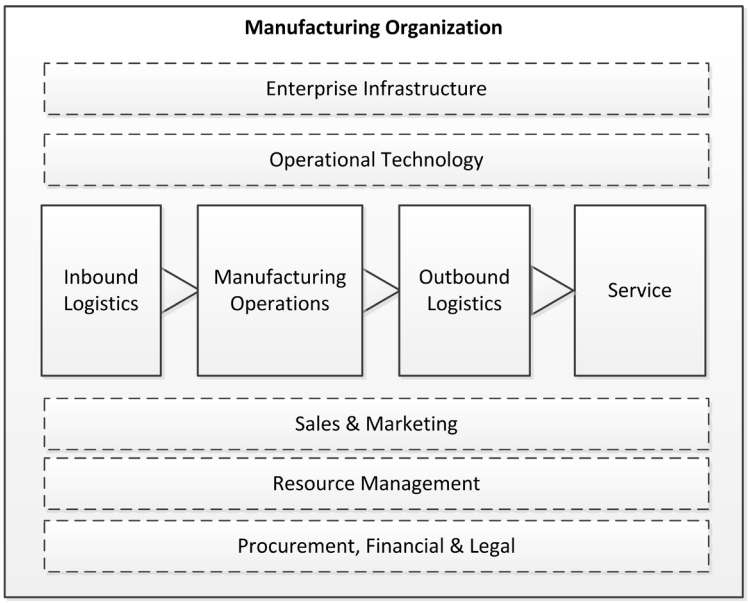


Figure 3 – The manufacturing value chain



NOTE 1 *The organization's supply chain forms part of the organization's overall value chain, e.g. through supplies delivered via its inbound logistics processes and the wider digital ecosystem.*

NOTE 2 *Organizations should consider the impact of risks both downstream and upstream of their operations and the potential need for additional testing and/or verification of automated updates to systems, software data and/or information.*

The security issues that might affect a manufacturing organization include:

- loss or theft of intellectual property (IP) and/or commercially sensitive information;
- criminal acts, for example computer misuse, fraud, sabotage, theft and vandalism;
- counterfeit supplies, including the potential effects of counterfeiting when the organization's products are deployed or operated;
- cyber security incidents affecting all aspects of the organization's operations;
- accidental or deliberate alteration or corruption of manufacturing information and/or software; and
- loss of sensitive customer or personal information.

In the past, many of these issues would have required physical access to the manufacturing process or its inputs and outputs, but with the increasing digital connectivity of both manufacturers and their systems, the threats now emanate from both local sources, and those around the globe.

The principles upon which drafting of this PAS was undertaken were that:

a) the manufacturing organization's security is owned, governed and promoted at board-level;

b) security risks to the manufacturing organization, its assets, manufacturing processes and outputs are assessed and managed appropriately and proportionately, including those specific to its supply chain;

c) the manufacturing organization appreciates the value of data and/or information it processes, whether owned by itself or a third-party, and takes steps to protect it across its lifetime;

d) where a manufactured item embodies digital technology or information the manufacturer ensures that the item is secure-by-design and provides aftercare and incident response to ensure that the item remains secure over its lifetime; and

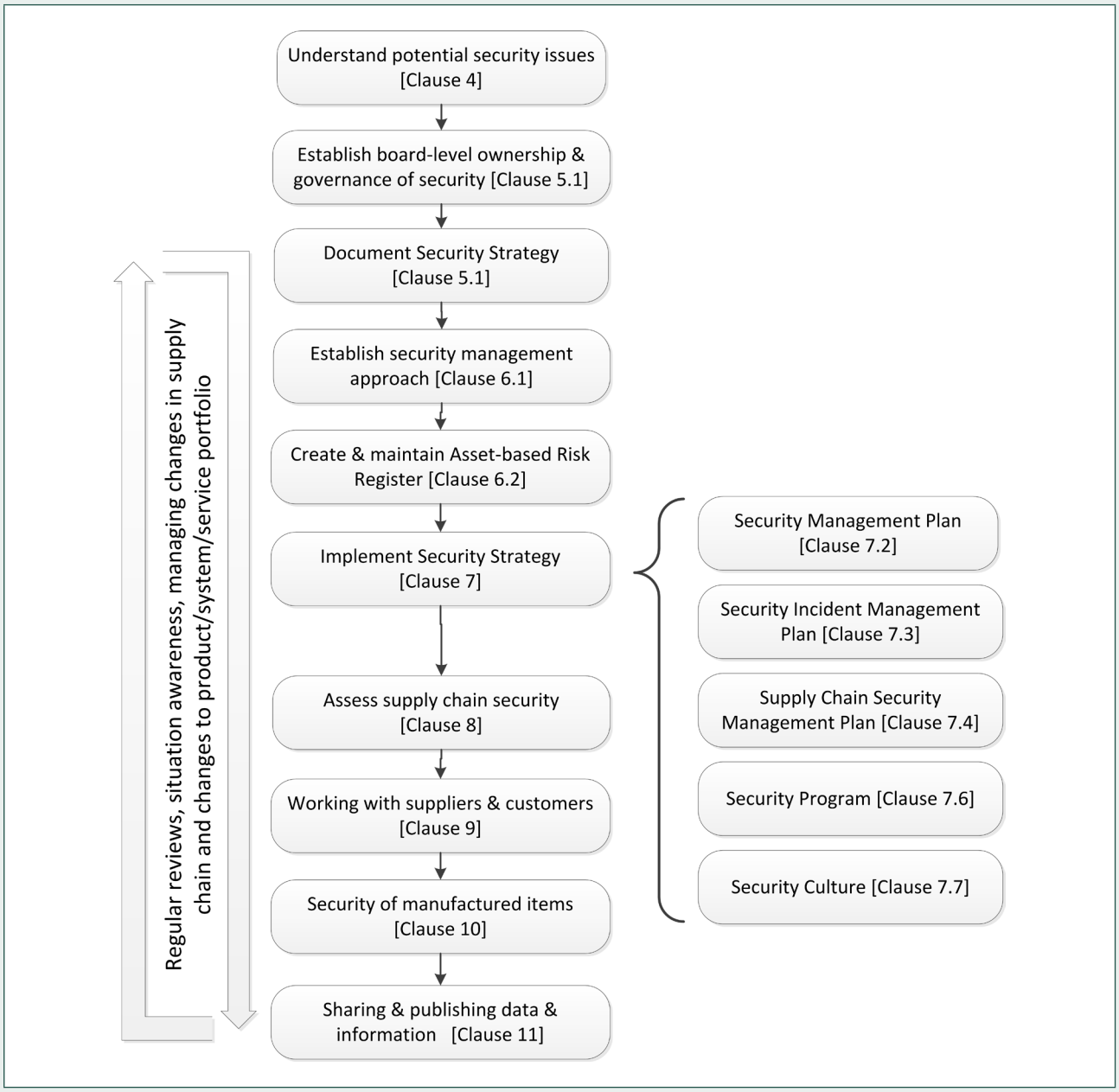
NOTE *It is the responsibility of the manufacturer to provide information and communicate to the customer and/or end user the lifetime support of the products and/or systems, and any associated services.*

e) the manufacturing organization works with its supply chain to implement an appropriate and proportionate level of security in the delivery of the digitally manufactured items and any related services and/or information.

NOTE *In determining what is appropriate and proportionate, the organization's board-level management should ensure that consideration is given to the nature, likelihood and severity of security threats and the potential impact(s) on the organization and its stakeholders in the event that the risk(s) occur.*

An overview of the PAS's security-minded approach to manufacturing is provided in Figure 4, cross-referenced to the relevant clauses.

Figure 4 – Overview of security-minded manufacturing



1 Scope

This PAS specifies requirements for the security-minded management of manufacturing organizations and the associated value chain utilizing information, digital technologies and associated control systems for the design, production, operation, maintenance and disposal of products and systems. These requirements aim to protect organizational reputation and liability, intellectual property, safety and security of manufacturing assets, and the integrity and value of the manufactured items.

It covers how to identify security threats throughout the manufacturing value chain and product lifecycle: design; manufacture (including processing and mixing); commissioning and handover; operation and maintenance; performance management; change of use/modification; and disposal. It also addresses security issues within the digital ecosystem that the organization and its supporting supply chain operate.

This PAS covers the following elements of security: people, physical, process and technological.

It explains the need for, and application of, trustworthiness and security controls throughout a manufacturing value chain to deliver a holistic approach encompassing: safety; authenticity; availability (including reliability); confidentiality; integrity; possession; resilience; and utility.

This PAS addresses the steps required to create and cultivate an appropriate security mind-set and culture within a manufacturing organization and across its supply chain, including the need to monitor, audit and evaluate effectiveness.

The approach outlined in this PAS is applicable to any manufacturing organization and its ecosystem where manufacturing information is processed and used in digital form.

NOTE *This PAS also aligns with the approach advocated by the Centre for the Protection of National Infrastructure (CPNI) for raising security-mindedness across sectors.*[1)]

The PAS is for use by senior executive managers, operational managers, engineers, and operatives in manufacturers of products and systems and their associated supply chains and its ecosystem. It might also be of use to insurers and trainers.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Standards publications

BS ISO 55000:2014, *Asset management – Overview, principles and terminology*

PAS 1192-5:2015, *Specification for security-minded building information modelling, digital built environments and smart asset management*

Other publications

[NR1] NATIONAL CYBER SECURITY CENTRE (NCSC). *Digital service security – Guidance*. October 2016. Available from: www.ncsc.gov.uk/guidance/digital-service-security [viewed April 2018]

[NR2] CABINET OFFICE. *Government Security Classifications.* Available from: www.gov.uk/government/publications/government-security-classifications [viewed April 2018]

[1)] Further information is available from CPNI's website: https://www.cpni.gov.uk.