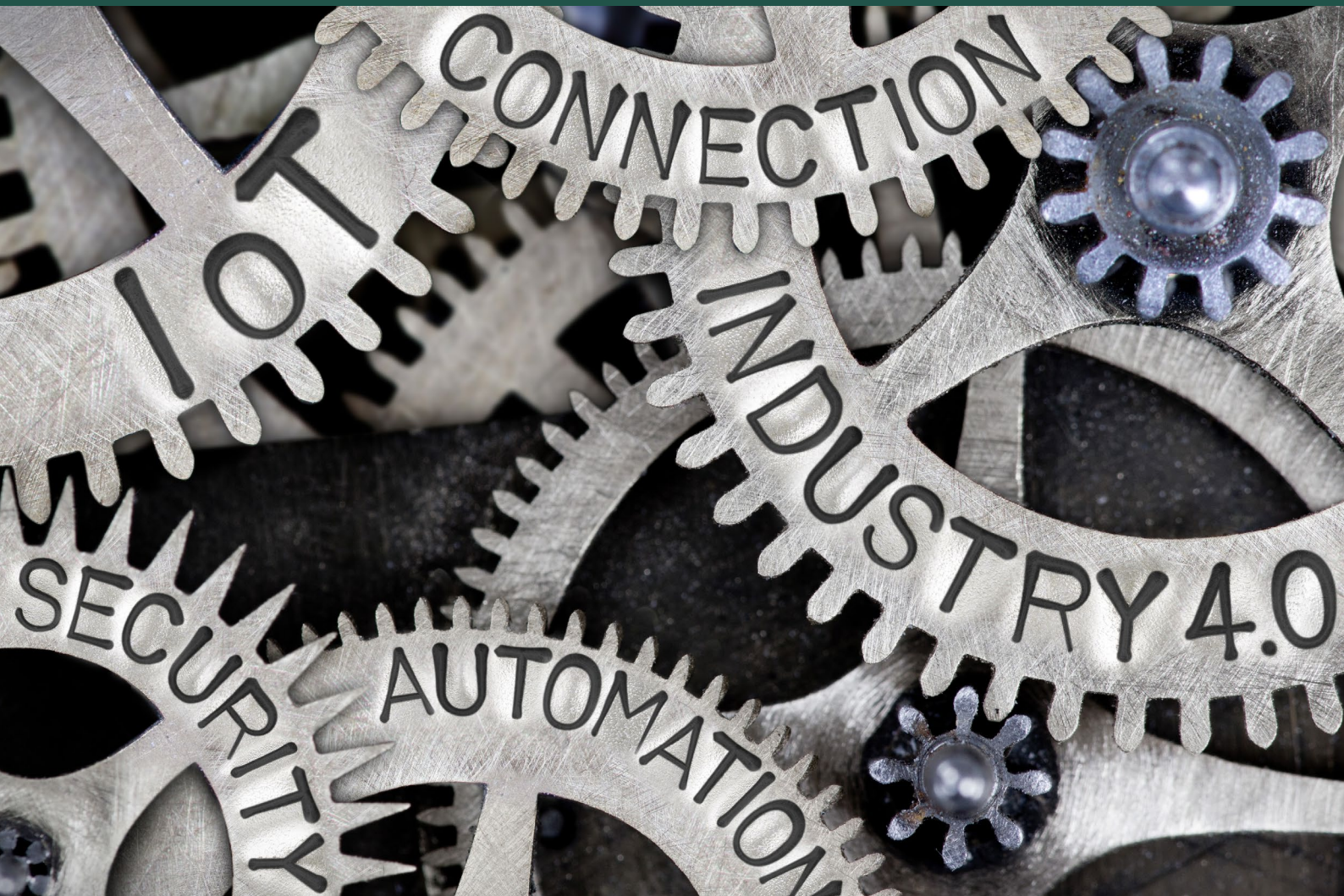


PAS 1085:2018

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



Innovate UK

bsi
Documents
Document Sharing Hub

AVA

Publishing and copyright information

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

© The British Standards Institution 2018. Published by BSI Standards Limited 2018.

ISBN 978 0 580 52421 9

ICS 03.100.50, 25.040.40, 35.030

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

Publication history

First published May 2018

Contents

Foreword	ii
0 Introduction	iv
1 Scope.....	1
2 Normative references	1
3 Terms, definitions and abbreviations	2
4 Manufacturing organization's environment.....	8
5 Security governance	13
6 Assessing and managing security risks	17
7 Implementing the organization's security strategy	22
8 Assessing security of the supply chain.....	26
9 Working with suppliers and customers	29
10 Security of a manufactured item	32
11 Data and information management.....	33
12 Security-minded approach in relation to compliance with legislation and other standards	46
Bibliography	49
List of figures	
Figure 1 – The manufacturing organization and its digital ecosystem ...	iv
Figure 2 – Illustrative manufacturing organization with a supply chain.	v
Figure 3 – The manufacturing value chain	vi
Figure 4 – Overview of security-minded manufacturing	vii
Figure 5 – Holistic approach to security.....	9
Figure 6 – Establishing the organization's context	14
Figure 7 – Security concepts and relationships.....	17
Figure 8 – Risk management approach	20
Figure 9 – Supplier security triage process	27
Figure 10 – Generic data and information lifecycle.....	34
Figure 11 – Security goals for the organization's data and information.	39
Figure 12 – Data and information security triage process.....	41
Figure 13 – Personally identifiable information test	42

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.

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 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.

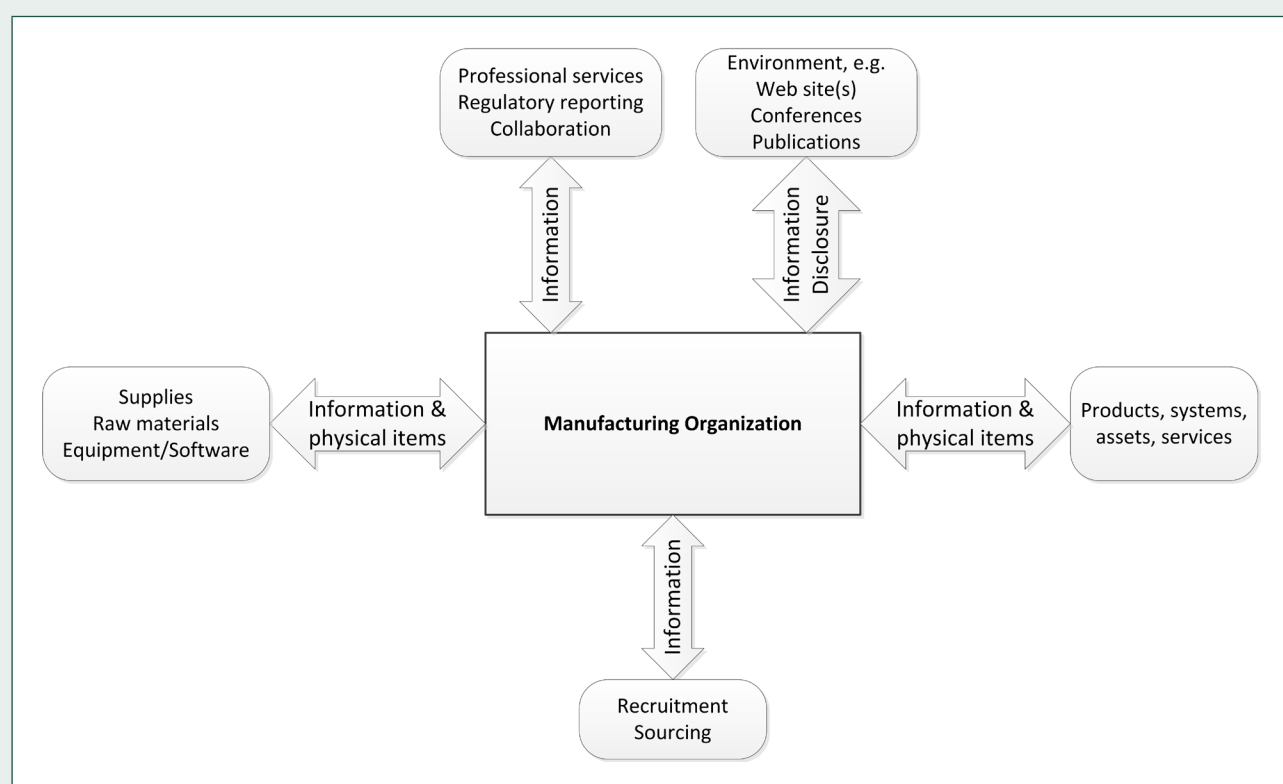
Particular attention is drawn to the following specific regulations:

- 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

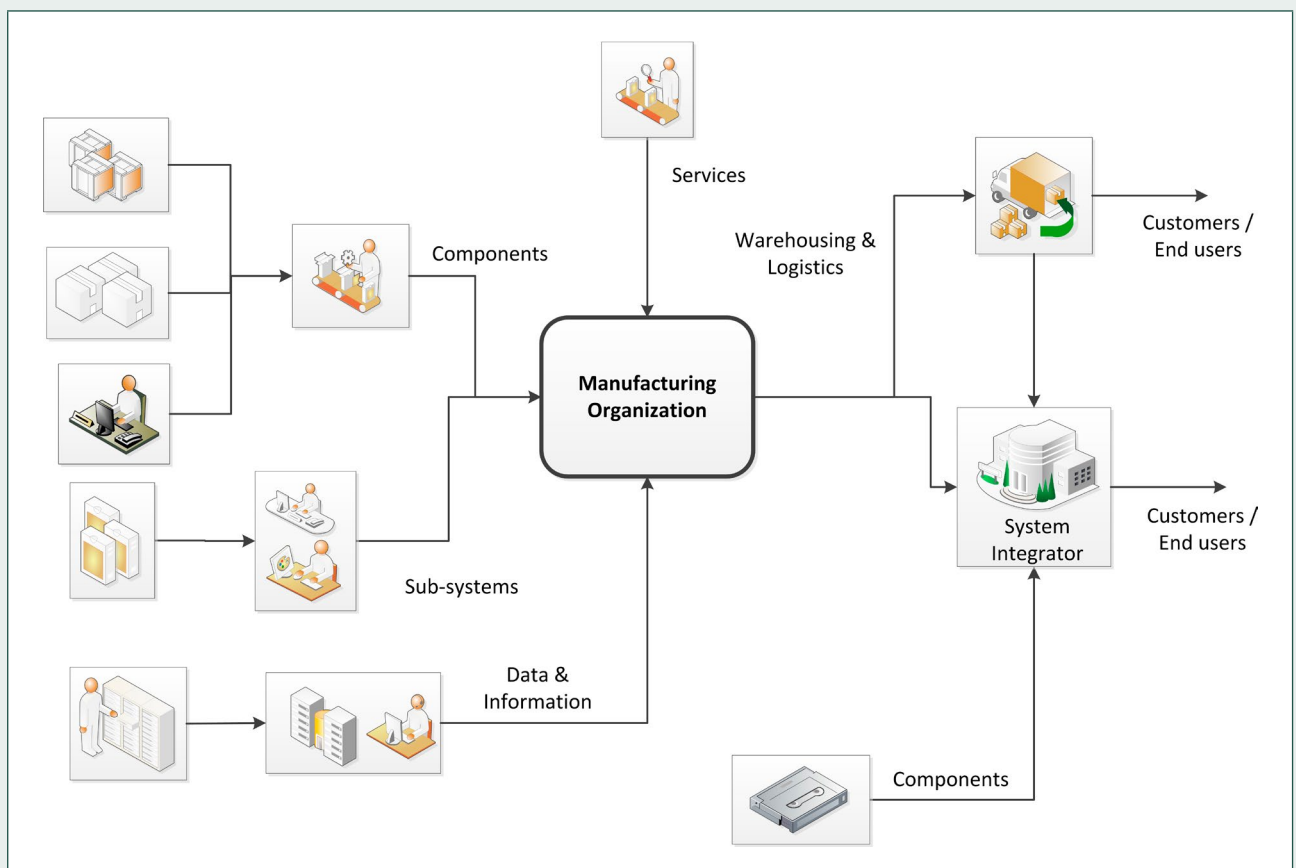
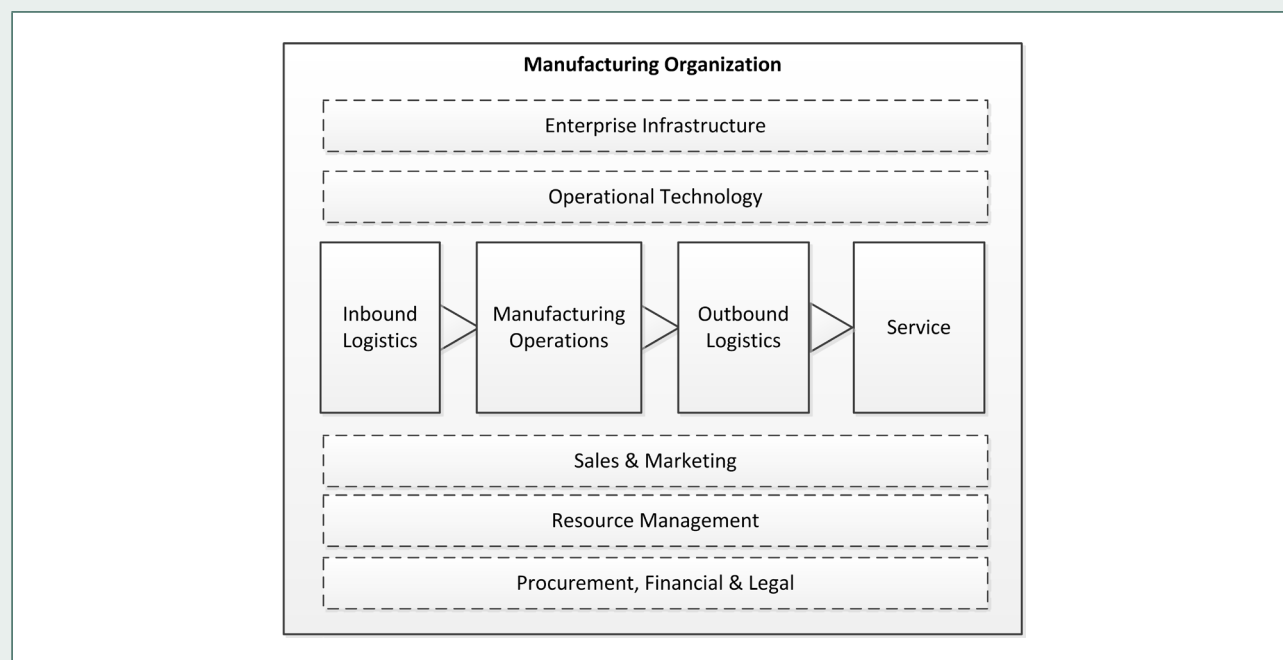


Figure 3 – The manufacturing value chain



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:

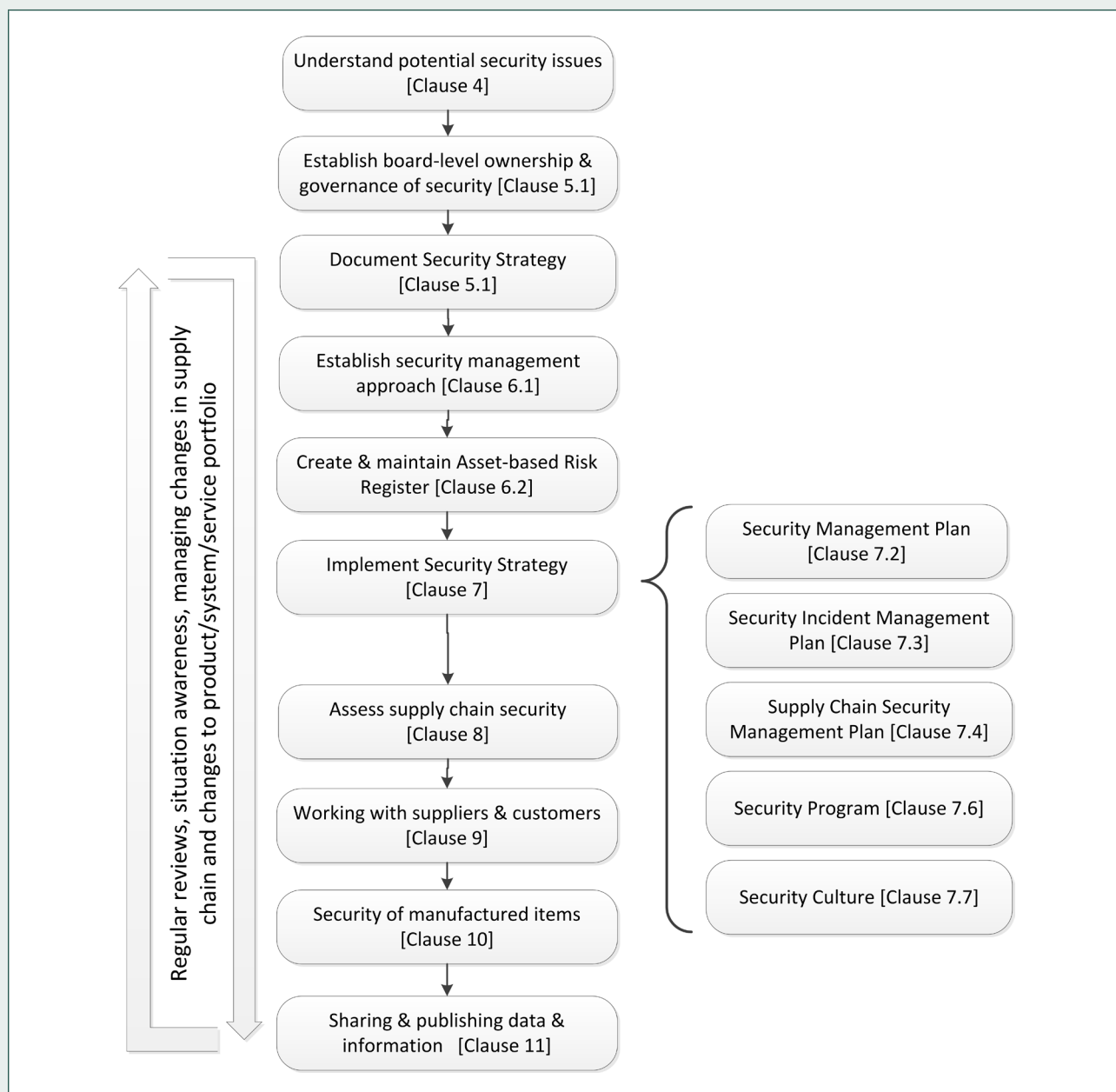
- a) the manufacturing organization's security is owned, governed and promoted at board-level;
- b) security risks to the manufacturing organization, its assets, manufacturing processes and outputs are assessed and managed appropriately and proportionately, including those specific to its supply chain;
- 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
- 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 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.

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



This page is deliberately left blank.

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>.

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this PAS, the following terms and definitions apply.

3.1.1 asset

item, thing or entity that has potential or actual value to an organization

NOTE 1 An asset can be fixed, mobile or movable. It can be an individual item, plant, a system of connected equipment, a space within a structure, a piece of land, an entire piece of infrastructure, an entire building, or a portfolio of assets.

NOTE 2 An asset might also comprise data, information in digital or in printed form, as well as an organization's internal processes.

NOTE 3 Digital information can be localized (i.e. based on a single data source) or distributed (i.e. derived from multiple data sources and/or locations).

NOTE 4 The value of an asset might vary throughout its life and an asset might still have value at the end of its life. Value can be tangible, intangible, financial and non-financial.

[SOURCE: BS ISO 55000:2014, 3.2.1]

3.1.2 asset data

data relating to the specification, design, construction or acquisition, operation and maintenance, and disposal or decommissioning of an item, thing or entity that has potential or actual value to an organization

[SOURCE: PAS 1192-5:2015, 3.1.2, modified]

3.1.3 asset information

information relating to the specification, design, construction or acquisition, operation and maintenance, and disposal or decommissioning of an item, thing or entity that has potential or actual value to an organization

NOTE Asset information can include design information and models, documents, images, software, spatial information and task or activity-related information.

[SOURCE: PAS 1192-5:2015, 3.1.2, modified]

3.1.4 context

circumstances that form the setting for an asset, event, data and/or information, which allow its significance and/or meaning to be better understood

3.1.5 cyber hygiene

conditions and practices that serve to promote or preserve cyber safety and security by individual system users

NOTE Good cyber safety and security practices are not dissimilar to good health practices related to infection and disease control, i.e. taking appropriate steps to prevent infection (e.g. malware), seeking advice in the case of a suspected infection, and when infection occurs, isolating it or taking steps to prevent further spread.

3.1.6 data

series of marks, digital or analogue signals or encoded characters stored or transmitted electronically

NOTE 1 Marks can include writing, printed characters or graphics.

NOTE 2 There are alternative definitions of data; this specific definition builds on that contained in PAS 183:2017 and is being used in the context of security-mindedness.

NOTE 3 Analogue data varies continuously and relates to natural phenomena such as sounds, natural light, river levels, waves and time. It can also include images such as sketches, drawings and text which have been produced by hand rather than using digital technologies.

NOTE 4 Digital data is represented as binary digits (bits) that have only two states, 0 and 1. These data can be a digital representation of analogue data, captured through a quantization process, or data that was created in digital form, for example as a result of a computer process or by entry using a human interface device (keyboard, touchscreen, stylus, etc.).

NOTE 5 The distinction between data and information is that data does not need to have any meaning attached to it; data becomes information via context.

3.1.7 data controller

person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed

NOTE 1 The wording of the definition given in the Data Protection Act 1998 [1] (DPA) is due to be amended by the General Data Protection Regulation (GDPR) [2] Article 4(7).

NOTE 2 Whilst few manufacturers may fall within the scope of the Security of Network and Information Systems Directive (also known as the NIS Directive) [11], data controllers should be aware of its objective regarding managing security risks, protecting against cyber attacks, detecting cyber security events and minimizing the impact of cyber security incidents.

{SOURCE: Data Protection Act 1998 [1], Section 1(1)}

3.1.8 data sharing

provision of data from one or more organizations to a third-party organization or organizations, the reciprocal exchange of data between organizations, or the sharing of data between different parts and/or systems of the same organization

NOTE 1 There are two main types of data sharing:

- a) *systematic, routine data sharing where the same data sets are shared between the same organizations, or parts of an organization, for an established purpose; and*
- b) *exceptional, one-off decisions to share data, for example, in unexpected or emergency situations, the provision of medical or social care data to emergency service first responders when they are responding to an incident.*

NOTE 2 Data sharing might take place implicitly as well as explicitly with outsourced services via the use of cloud services where appropriate security measures are not in place.

{SOURCE: ICO's Data Sharing Code of Practice [12], May 2011, modified}

3.1.9 data and information sharing agreement (DISA)

set of rules to be adopted by the various organizations involved in a data and/or information sharing operation

3.1.10 disclosure

action of making sensitive, classified or private data and/or information known

3.1.11 hostile reconnaissance

activity of acquiring information about a target with the view to planning to attack, compromise, disrupt or destroy that target

NOTE 1 The target might be an individual, organization, enterprise or built asset, in whole or in part.

NOTE 2 The planned hostile action might be physical or cyber in nature.

NOTE 3 Reputational damage might result from such physical or cyber hostile actions.

{SOURCE: PAS 1192-5:2015, 3.1.15}

3.1.12 information

one or more data items that have a context and therefore convey a message or meaning

NOTE 1 A string of characters might be referred to generally as data; but if these characters are understood by a person or a computer program (for example, as someone's name), then the characters convey information. Information always involves the presence of data in some format, on some medium, which could be, for example, a physical document, a document image on a screen, or the contents of an electronic file.

NOTE 2 There are alternative definitions of information, but from a security-mindedness perspective the information's context can increase the sensitivity of the information.

3.1.13 information management

policies, processes, procedures and tasks applied to the data and/or information across its lifecycle to ensure its accuracy, authenticity, confidentiality, integrity and utility

NOTE See also Figure 9 which illustrates the generic data and information lifecycle.

{SOURCE: PAS 1192-5:2015, 3.1.17, modified}

3.1.14 information sharing

provision of information from one or more organizations to a third-party organization or organizations, the reciprocal exchange of information between organizations, or the sharing of information between different parts and/or systems of the same organization

NOTE 1 There are two main types of information sharing:

- a) *systematic, routine information sharing where the same information sets are shared between the same organizations, or parts of an organization, for an established purpose; and*
- b) *exceptional, one-off decisions to share information, for example, in unexpected or emergency situations, the provision of medical or social care data to emergency service first responders when they are responding to an incident.*

NOTE 2 Information sharing might take place implicitly, as well as, explicitly with outsourced services via the use of cloud services where appropriate security measures are not in place.

{SOURCE: ICO's Data Sharing Code of Practice [12], May 2011, modified}

3.1.15 near-miss

incident in which a security incident is narrowly avoided, either by chance or through deliberate action

3.1.16 need-to-know

grant of access to data and/or information relating to assets for an individual or organization where such access is necessary in order for them to perform their role satisfactorily and safely

[SOURCE: PAS 1192-5:2015, 3.1.18, modified]

3.1.17 operational technology (OT)

hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the organization

3.1.18 organization

person or group of persons that has its own function with responsibilities, authorities and relationships to achieve its objectives

[SOURCE: BS ISO 55000:2014, 3.1.13]

3.1.19 pattern-of-life

identification of habits, routines and preferences of individual(s) or group(s) that enable prediction of future actions and/or behaviour

[SOURCE: PAS 185:2017, 3.1.31, modified]

3.1.20 pattern-of-use

identification of routine actions in the handling, operation and management of assets

NOTE *The pattern-of-use of assets could facilitate malicious pattern-of-life analysis by increasing the number of data and information sources that can be combined.*

[SOURCE: PAS 185:2017, 3.1.32]

3.1.21 personal data

data which relates to a living individual who can be identified:

- a) from those data; or
- b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

NOTE *Under GDPR [2], Article 4(1), personal data means “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity or that natural person”. This definition comes into force from 25 May 2018.*

{SOURCE: Data Protection Act 1998 [1], Section 1(1)}

3.1.22 personally identifiable information

also known as personal data

3.1.23 personnel

individual(s) employed by an organization, including contractors or temporary staff used to fulfil roles that are undertaken by that organization

[SOURCE: PAS 1192-5:2015, 3.1.22]

3.1.24 personnel security

system of policies, processes and procedures that seek to mitigate the risk of workers (inside an organization) exploiting their legitimate access to that organization's assets for unauthorized purposes

NOTE *These measures might be applied to all personnel that have access to, or use, the asset over its lifecycle, including personnel employed within the supply chain used to design, create, operate, decommission or dispose of the asset.*

3.1.25 physical security

multi-layering of different physical measures designed to deter, detect or delay an attack

3.1.26 processing

obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data, including:

- a) organization, adaptation or alteration of the information or data;
- b) retrieval, consultation or use of the information or data;
- c) disclosure of the information or data by transmission, dissemination or otherwise making available; or
- d) alignment, combination, blocking, erasure or destruction of the information or data

NOTE Under GDPR [2], Article 4(2), processing means “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”. This definition comes into force from 25 May 2018.

{SOURCE: Data Protection Act 1998 [1], Section 1(1)}

3.1.27 referential master data

set of permissible values to be used by other data fields in shared data and/or shared information sets

NOTE Shared data is data that is subject to formal or informal data sharing (see 3.1.8). Shared information is information that is subject to formal or informal information sharing (see 3.1.14).

3.1.28 related services

services provided in support of the specification, procurement, configuration, installation, operation and maintenance of a manufactured product and/or system

NOTE The services could be digital, physical or hybrid in nature, for example:

- a) physical service – the physical installation and maintenance of the product or system;
- b) digital – digital artefacts such as manuals or websites providing information about the product(s) and/or system(s) and/or service(s); or
- c) hybrid – remote condition monitoring and fault diagnostics for the product(s) and/or system(s).

3.1.29 risk appetite

amount of risk that an organization is willing to seek or accept in the pursuit of its long-term objectives

NOTE 1 Risk appetite might be set in relation to the organization as a whole, for different groups of risks, or at an individual risk level.

NOTE 2 In the manufacturing context, when determining the risk appetite, the needs and perspectives of all of the organizations involved should be taken into account.

{SOURCE: Chartered Institute of Internal Auditors [13]}

3.1.30 risk capacity

resource(s), including financial, intangible and human, which an organization is able to deploy in managing risk

NOTE The organization's risk capacity is generally wider in scope than the risk appetite of the organization as it represents the limits beyond which the organization could not cope in the event that the risk(s) occur(s). For example, when seeking insurance cover, the organization assesses what residual risk it is prepared to accept, i.e. its risk appetite which might be reflected in the excess payable if an insured event occurs, whilst the level of cover purchased reflects the risk capacity in respect of the insured risk(s). In assessing its risk appetite and risk capacity an organization considers both the gross risk and residual risk exposures, its reliance on controls and other mitigations, and the cost of implementing them in comparison to the consequences of the risk materializing.

{Source: Chartered Institute of Internal Auditors [13]}

3.1.31 risk universe

full range of risks which could impact, either positively or negatively, on the ability of the organization to achieve its long-term aims

{SOURCE: Chartered Institute of Internal Auditors [13]}

3.1.32 sabotage

deliberate, malicious action carried out with the aim of weakening, obstructing, disrupting, damaging or destroying an asset, activity, service, organization or other entity

NOTE Sabotage might also be conducted with the aim of enabling the targeting of a secondary event that occurs as a result of the original action for example, the evacuation of a building arising from the sabotage of a fire alarm.

3.1.33 security

state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts, including sabotage

{SOURCE: Engineering Council, 2016 [14]}

3.1.34 security incident

event or events during which the security of an asset, organization or person is, or might be, compromised, either accidentally or deliberately

NOTE 1 *Security incidents can take a number of forms including:*

- a) *unauthorized harmful modification to, damage to or destruction of a physical asset;*
- b) *supply of counterfeit raw materials, ingredients, physical and/or digital components, assemblies or sub-systems;*
- c) *loss or theft of documents, storage media, IT equipment, attractive or valuable items;*
- d) *loss, theft or unauthorized access to information or data;*
- e) *loss, compromise, unauthorized manipulation or change of project or asset information;*
- f) *unauthorized access to the built asset, or a restricted access area within the built asset;*
- g) *loss of keys, access control tokens, passes, etc.;*
- h) *planting of bugs or other surveillance devices; and*
- i) *unauthorized access to, misuse of, or fraudulent use of ICT equipment or systems.*

NOTE 2 *A near-miss is an event in which a security incident is narrowly avoided either accidentally or through deliberate action.*

3.1.35 security-minded

understanding and routine application of appropriate and proportionate security measures in any business situation so as to deter and/or disrupt hostile, malicious, fraudulent and criminal behaviours or activities and reduce the risk of security incidents

{SOURCE: PAS 1192-5:2015, 3.1.26, modified}

3.1.36 sensitive data

data, the loss, misuse or modification of which, or unauthorized access to, could adversely affect the privacy, welfare or safety of an individual or individuals; compromise intellectual property or trade secrets of an organization; cause commercial or economic harm to an organization or country; and/or jeopardize the security, internal and foreign affairs of a nation, depending on the level of sensitivity and nature of the data

{SOURCE: PAS 1192-5:2015, 3.1.28, modified}

3.1.37 sensitive information

information, the loss, misuse or modification of which, or unauthorized access to, could adversely affect the privacy, welfare or safety of an individual or individuals; compromise intellectual property or trade secrets of an organization; cause commercial or economic harm to an organization or country; and/or jeopardize the security, internal and foreign affairs of a nation, depending on the level of sensitivity and nature of the information

{SOURCE: PAS 1192-5:2015, 3.1.28, modified}

3.1.38 sensitive personal data

personal data consisting of information as to:

- a) racial or ethnic origin of the data subject;
 - b) his political opinions;
 - c) his religious beliefs or other beliefs of a similar nature;
 - d) whether he is a member of a trade union;
- NOTE** *Within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992 [3].*
- e) his physical or mental health or condition;
 - f) his sexual life;
 - g) the commission or alleged commission by him of any offence; or
 - h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

NOTE *Sensitive personal data under the DPA [1] will be defined as special categories of personal data under GDPR [2] and this will extend the range of personal data within this category. Under Article 9, the definition encompasses data which reveals “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”. This definition comes into force from 25 May 2018.*

{SOURCE: Data Protection Act 1998 [1], Section 2}

3.1.39 service

work done to meet some administrative, general, or user or customer need

NOTE *Within the manufacturing context, a system supplying a user or customer need includes logistics, communications, utilities and product or system support.*

3.1.40 stakeholder

third parties such as persons, personnel, or organizations that have a legitimate interest in the organization's manufacturing activities, and/or the products, systems and any related services it delivers

NOTE *The reference to persons encompasses people affected by the manufacturing operations, customers of the manufacturer, and any users or people affected by use of the manufacturer's products, systems and any related services.*

3.1.41 suitably qualified and experienced person

person who can demonstrate that they have:

- a) sufficient evidence, from education, training and/or experience, to demonstrate:
 - 1) knowledge and understanding of the security threats and vulnerabilities affecting the organization, its products and/or services, and any related services;
 - 2) a detailed understanding of appropriate and proportionate security controls and countermeasures; and
 - 3) practical experience of specifying and managing the implementation of security controls and countermeasures;
- b) sound knowledge of security risk identification, analysis, evaluation and treatment; and
- c) the ability to advise management on the implementation of security requirements and security practices for assets that might be subject to significant and enduring security threats, opportunities and vulnerabilities

NOTE *The organization should undertake appropriate due diligence to verify the qualifications, training and/or experience of individuals to ascertain their suitability for the role, for example, looking for evidence that the individual has relevant experience. Membership of a relevant professional body, supported by evidence of up-to-date risk and security-related continuing professional development might be appropriate indications of relevant qualifications and experience.*

3.1.42 supply chain

network of organizations, directly or indirectly interlinked and interdependent, resources, activities and technology involved in the creation and sale of products and/or systems, and any related services, from the delivery of source material(s) from the supplier(s) to the manufacturing organization, through to eventual delivery to the end user

3.1.43 system

group of interacting, interrelated, or interdependent elements forming a complex whole

NOTE *A system can include physical, digital, process and human elements.*

3.1.44 threat

potential cause of an incident which might result in harm to an asset(s), individual(s), and/or organization(s)

3.1.45 threat actor

person or organization that can adversely act on assets

3.1.46 vulnerability

weakness that can be exploited by one or more threats

3.2 Abbreviations

For the purposes of this PAS the following abbreviations apply.

DISA	data and information sharing agreement
EDI	electronic data interchange
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
ICT	information and communications technology
OT	operational technology/technologies
SaaS	software as a service
SCSMP	supply chain security management plan
SIMP	security incident management plan
SMP	security management plan
SyOpPs	security operating procedures

4 Manufacturing organization's environment

4.1 Understanding the need for security in manufacturing

The organization's board-level management shall research, document and demonstrate an understanding of the range of potential security issues that are applicable to its business, assets, personnel and the environments and ecosystems in which its manufactured products, systems and/or related services are or might be used.

NOTE 1 *Security operates on a number of levels ranging from national security issues (e.g. the protection against terrorism, tackling organized crime and detecting hostile acts by nation states), to preserving the value, longevity and ongoing use of an enterprise's assets, whether tangible (e.g. a factory or physical stock), or intangible (e.g. preventing the loss or disclosure of intellectual property and nationally or commercially sensitive information). It also includes the handling of privacy issues (e.g. the protection of personally identifiable information).*

NOTE 2 *Good security can offer competitive advantage to the manufacturing organization by protecting their key assets and engendering trust by their stakeholders and owners or users in the products, systems and related services that are provided. For those involved in the design and delivery of new or modified products or services or the systems that use them, it can also provide competitive global positioning in an international market.*

NOTE 3 *Good security requires holistic risk assessment and applying the principles of proportionality to achieve an appropriate balance of the costs and constraints associated with protecting an asset versus the impact that its loss, compromise or failure can have on the organization and the organization's stakeholders.*

NOTE 4 *It is important to recognize that once data and information has been published on the internet, or otherwise made publicly available, it is virtually impossible to delete, destroy, remove or secure all copies of the released data and information. In addition, the release of aggregated, apparently innocuous data and information can result in exposing sensitive or security information. Therefore, appropriate checks should be made before any data and/or information is made widely available.*

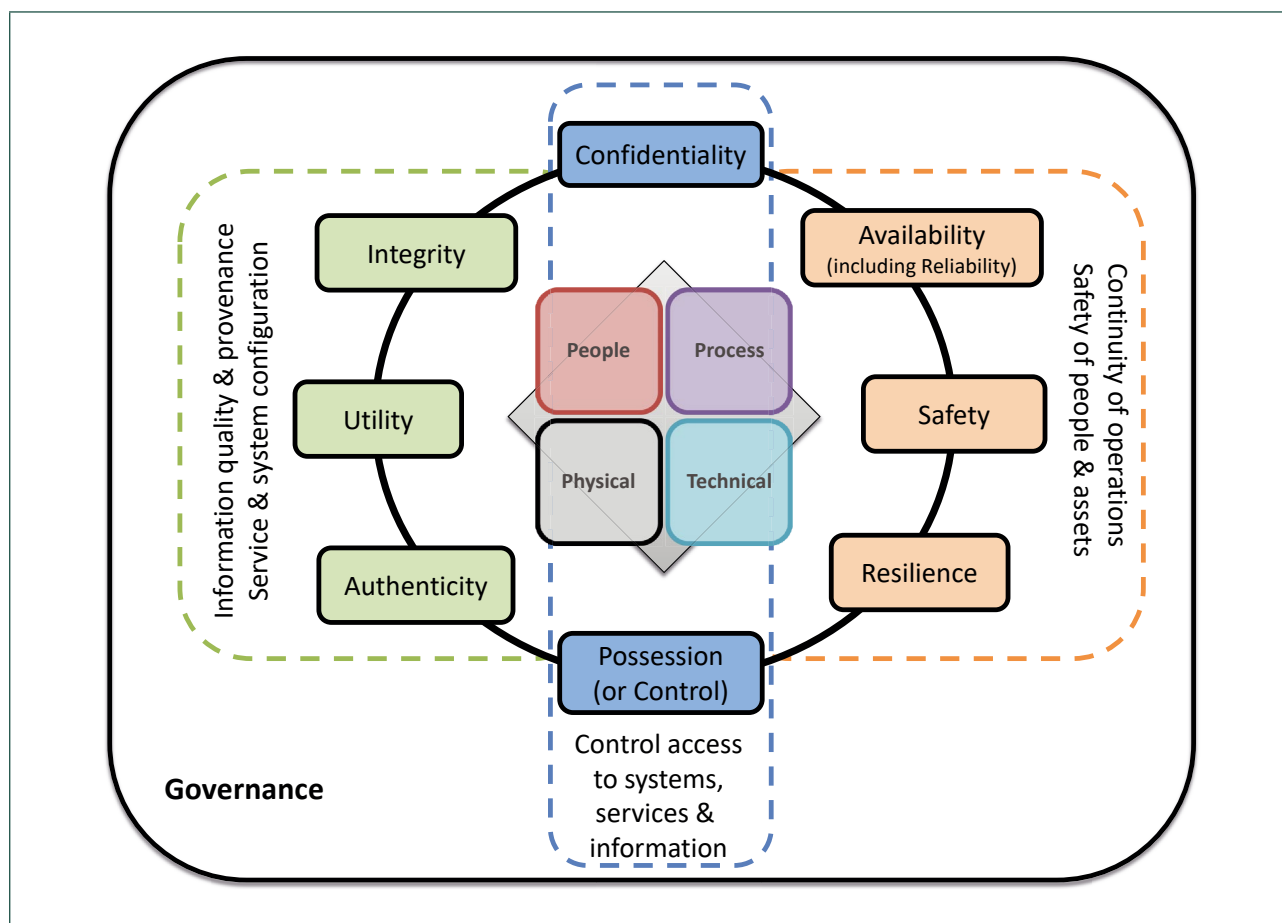
4.2 Holistic approach to digital manufacturing security

4.2.1 The organization's board-level management shall appreciate that effective security requires a holistic approach, as illustrated in Figure 5 that addresses security in respect of the following aspects as a minimum:

- a) people, i.e. the personnel that have access to the organization's assets;
- b) physical, i.e. the physical environment in which the organization's assets are designed, created, used, stored, and transported;
- c) processes, i.e. the business processes used to:
 - 1) acquire, transport, store, manage, maintain, and dispose of the organization's assets;
 - 2) design the product(s) and/or system(s) and any related service(s);
 - 3) manage the classification and sharing of data and information, both within the organization and with its supply chain, professional advisers, customers and potential customers; and
- d) technology, i.e. the design, operation, maintenance or support, decommissioning and disposal of electronic storage media, ICT equipment and systems, and the OT used by the organization.

NOTE *Effective security reduces security risks to the lowest reasonably practicable level having due regard for the severity and likelihood of risks both individually and in combination and their impact on both the organization and its stakeholders. When assessing and treating risks, organizations should focus on developing and adopting appropriate and proportionate controls or countermeasures rather than focusing primarily on adopting specific physical or technological measures.*

Figure 5 – Holistic approach to security



NOTE The eight security goals (confidentiality, availability, safety, resilience, possession, authenticity, utility and integrity) are applicable across the four security domains (people, physical, process and technical). For example, the physical composition of a digital processing system can affect the integrity of the data and/or information it processes, which can result in a loss of availability of a safety critical process leading to potential harm to the vehicle's user or to a pedestrian.

4.2.2 The organization's board-level management shall be aware of the cyber-physical security risks that arise where digital assets and processes have an impact on the physical characteristics of a manufactured asset associated with a product or service.

4.3 Digital manufacturing security issues

4.3.1 Loss or disclosure of intellectual property

The organization's board-level management shall research, document and demonstrate an understanding of the need to protect its own and others' intellectual property, which it holds, or which might be developed, and shall assess and record the potential consequences of the loss of, unauthorized access to, or improper use or re-use of that information.

NOTE 1 Intellectual property encompasses a range of material, including trade secrets, proprietary processes, technical specifications and detailed calculations or methodologies. Organizations often invest heavily in the development of intellectual property and through its use, licensing and sale can deliver significant commercial and economic benefits. The piracy, theft or unauthorized use of intellectual property can be damaging to the organization and a country's economy as a whole.

NOTE 2 Some intellectual property is sensitive information that can be used to manifest a physical result in a manufactured object, in which case it irretrievably crosses the cyber-physical boundary. This behaviour has some, but not all, of the characteristics of disclosure, and should be taken into account when considering the protection of intellectual property. The sensitive data and/or information might include or reflect:

- a) the composition or treatment of materials used in its manufacture;
- b) proprietary aspects of the manufacturing process; and
- c) where the object contains digital elements, the design and operation of those elements.

NOTE 3 Consideration should be given to the protection of intellectual property from loss, unauthorized access, or improper use or re-use. Scenarios to be considered might include:

- a) development and use of intellectual property within the organization;
- b) collaboration with third-parties, including universities and research institutes, through the lifecycle of the intellectual property;
- c) disclosure of intellectual property to third-parties, including professional advisers and the organization's supply chain;
- d) publication or presentation of data and/or information relating to the intellectual property, for example in white papers, conference or trade publications; and
- e) disclosure of intellectual property due to accessible characteristics of a product, system or service itself.

4.3.2 Criminal and malicious acts

The organization's board-level management shall research, document and demonstrate an understanding of the need to protect from criminal acts its own personnel and others':

- a) assets; and

NOTE 1 Potential threats to the organization's assets include theft, damage and sabotage. The physical security of the assets should be considered throughout their lifecycle.

NOTE 2 Where the assets are digital (for example, electronic files, designs, databases, etc.) or where the assets are systems that depend on ICT equipment and systems and/or the OT, there are increased business risks arising from malicious acts caused by a range of external and insider threats, such as damage caused by malware, hackers or disaffected personnel.

- b) operations.

NOTE 1 The increasing use of email, EDI, collaborative platforms, websites and supplier portals to share information, place and track orders and/or deliveries, submit invoices, manage enquiries, and to monitor, manage and/or maintain deployed products or systems can provide opportunities for malicious use of these channels to commit fraud, gain unauthorized access to information and/or allow the spread of malware. There is increased business risk arising from loss, misuse or incorrect allocation of user credentials (for example through failure to verify the identity of a new user).

NOTE 2 Widespread use of digital and information technologies and the outsourcing of business operations creates increased business risks which could manifest themselves as loss of availability, functionality or performance, or the loss or corruption of digital artefacts, and the physical products that directly depend on them, including those manufactured using them.

4.3.3 Counterfeit and contaminated supplies

The organization's board-level management shall research, document and demonstrate an understanding of the need to apply due diligence to reduce the risk of obtaining counterfeit, maliciously or fraudulently sub-standard, or contaminated items when purchasing assets, including raw materials, ingredients or manufactured items that are used in its own manufactured products or systems and any related services.

NOTE 1 The provenance of raw materials, ingredients, manufactured supplies and assets, and the integrity of the supply chain and logistics services used to handle them are both important if an organization is to reduce the risk of inferior, counterfeit or contaminated items entering their supply chain or facility. This might be as a result of the actions or inaction of a supplier or as a result of substitution in the sales and supply chain, for example where supplies are purchased as grey imports, i.e. outside of the authorized supply and distribution channels used by the original manufacturer or material supplier.

NOTE 2 Counterfeit and contaminated supplies are those which are deliberately and fraudulently mislabelled or described with respect to their identity, composition and/or source. Counterfeiting can apply to both branded and generic materials or products and the counterfeit might include elements:

- with the correct or incorrect ingredients/components;
- with or without insufficient key ingredients/components; or
- with fake packaging.