CPNI
Centre for the Protection of National Infrastructure

OPEN DATA: ADOPTING A SECURITY-MINDED APPROACH

November 2015

Disclaimer
Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

In June 2012, the UK Government published its Open Data White Paper: Unleashing the Potential[1] aimed at:

- making it easier to access public data;
- making it easier for publishers to release data in standardised, open formats; and
- engraining a 'presumption to publish' unless there are clear, specific reasons (such as privacy or national security) not to do so.

Such openness provides significant opportunities for reform of services, citizen engagement and innovation which in turn can each contribute to economic growth. However, it also requires that particular care is taken to identify and protect information which could impact on the safety and security of:

- individuals;
- sensitive assets and systems; and
- the benefits which the sensitive asset or system exists to deliver.

This guidance provides a framework for adopting a security-minded approach to the sharing and publication of that data which could be exploited by those with hostile or malicious intent. Its purpose is not in any way to undermine the principles of open data. Rather it encourages the adoption of appropriate and proportionate measures by data owners and data publishers to ensure that the many benefits can still be realised, while protecting both key assets and the public's right to privacy.

It draws on advice contained in PAS 1192-5[2] and should be read in conjunction with it.

What is Open Data?

The Government White Paper defines Open Data as that which meets the following criteria:

- accessible (ideally via the internet) at no more than the cost of reproduction, without limitations based on user identity or intent;
- in a digital, machine readable format for interoperation with other data; and
- free of restriction on use or redistribution in its licensing conditions.

In some cases data may be geographically tagged, enabling its geospatial visualisation (e.g. open mapping), and thereby allowing relationships, patterns and trends to be more easily analysed.

In order to deliver this open data and to realise its intended aims, including the need to protect certain information, an approach is required which delivers:

- **safety** - preventing the creation, by the use of open data, of harmful states which may lead to injury or loss of life or unintentional environmental damage;
- **authenticity** - ensuring that the open data is genuine;
- **availability** (including reliability) - ensuring accessibility and usability of the data in an appropriate and timely fashion;
- **confidentiality** - ensuring control of access and prevention of unauthorised access to sensitive information;
- **integrity** - maintaining consistency, coherence and configuration of data sets;

[1] Available from https://www.gov.uk/government/publications/open-data-white-paper-unleashing-the-potential

[2] PAS 1192-5, Specification for security-minded building information modelling, digital built environments and smart asset management. Available from http://shop.bsigroup.com/pas1192-5

- **possession** - preventing unauthorised control, manipulation or interference with systems disseminating open data;
- **resilience** - ensuring the ability of systems disseminating open data to transform, renew and recover in a timely fashion in response to adverse events; and
- **utility** - ensuring usability and usefulness of the data sets over time.

The security-minded approach

A security-minded approach should be adopted where a clear and specific reason for not publishing data exists, namely:

- to prevent an individual, or group of individuals, being identified or identifiable in the hands of a recipient of the data;
- to protect information about the location of sensitive assets or systems not otherwise generally visible directly or through other sources;
- to protect certain information pertaining to sensitive assets or systems, the location of which can be readily identified; and
- when the aggregation (through accumulation or association) of data, or an increase in the accuracy of the location of assets or systems, could compromise safety and security of an individual, an asset, a system or a related service.

Even where a data set has been anonymised or pseudonymised, care must be exercised to ensure that de-anonymisation is not possible, for example, where data aggregation allows restoration of identifiers or characteristics of a data set, leading to identification of an asset or individuals or systems, e.g. security systems. There will be an additional security risk when this process would allow pattern of life analysis of certain individuals to be undertaken using data collected over an extended period of time, thereby understanding that particular individual's habits and potentially predicting future behaviours.

The need for such an approach should therefore be assessed by the data owner prior to the release of a data set to a third party, and by the data publisher prior to:

- the publication of a new open data set;
- the update of an existing published data set;
- undertaking a review of an existing data set; or
- augmenting or linking a new or existing open data set with another data set.

The process for applying a security-minded approach is shown in Figure 1 below.

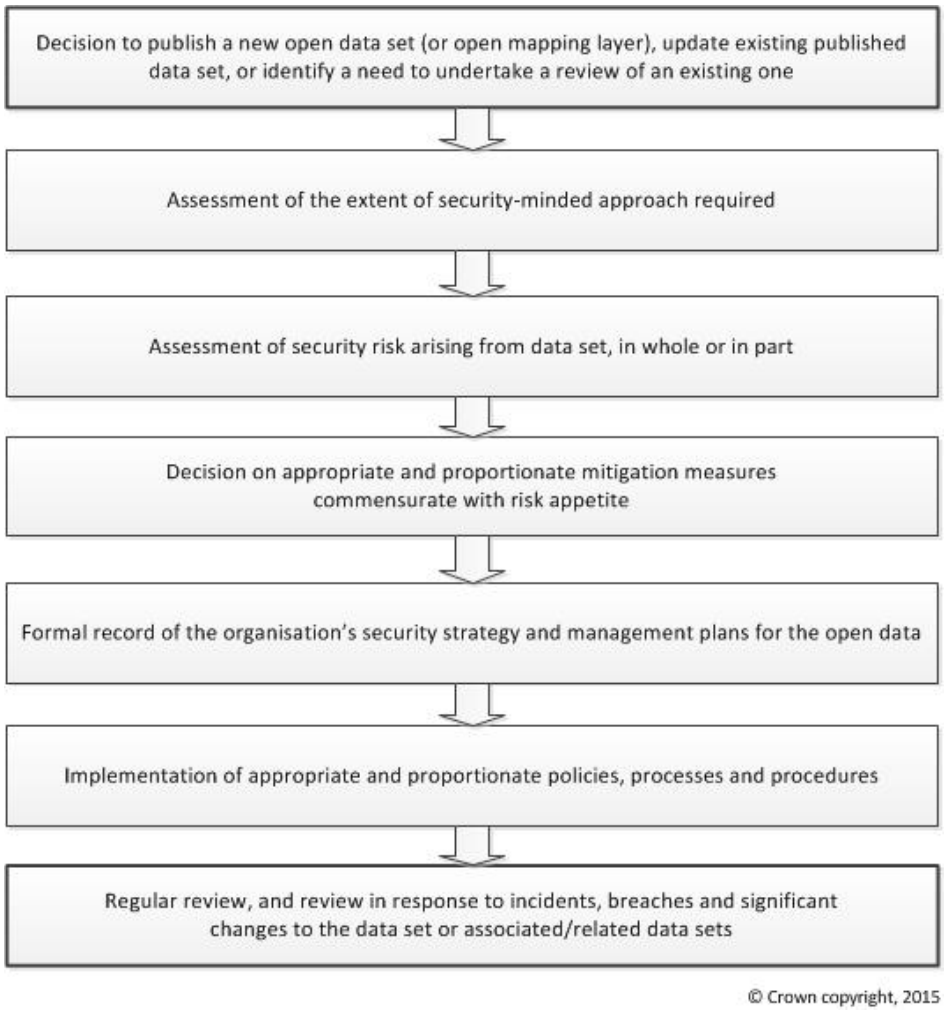


Figure 1. Summary of the security-minded process for publishing open data

Identifying the need for a security-minded approach

When a decision has been taken to publish a data set as open data, the need for, and extent of, a security-minded approach to be applied, in whole or in part, should be assessed by the publisher using the open data security triage process outlined in Figure 2 below.

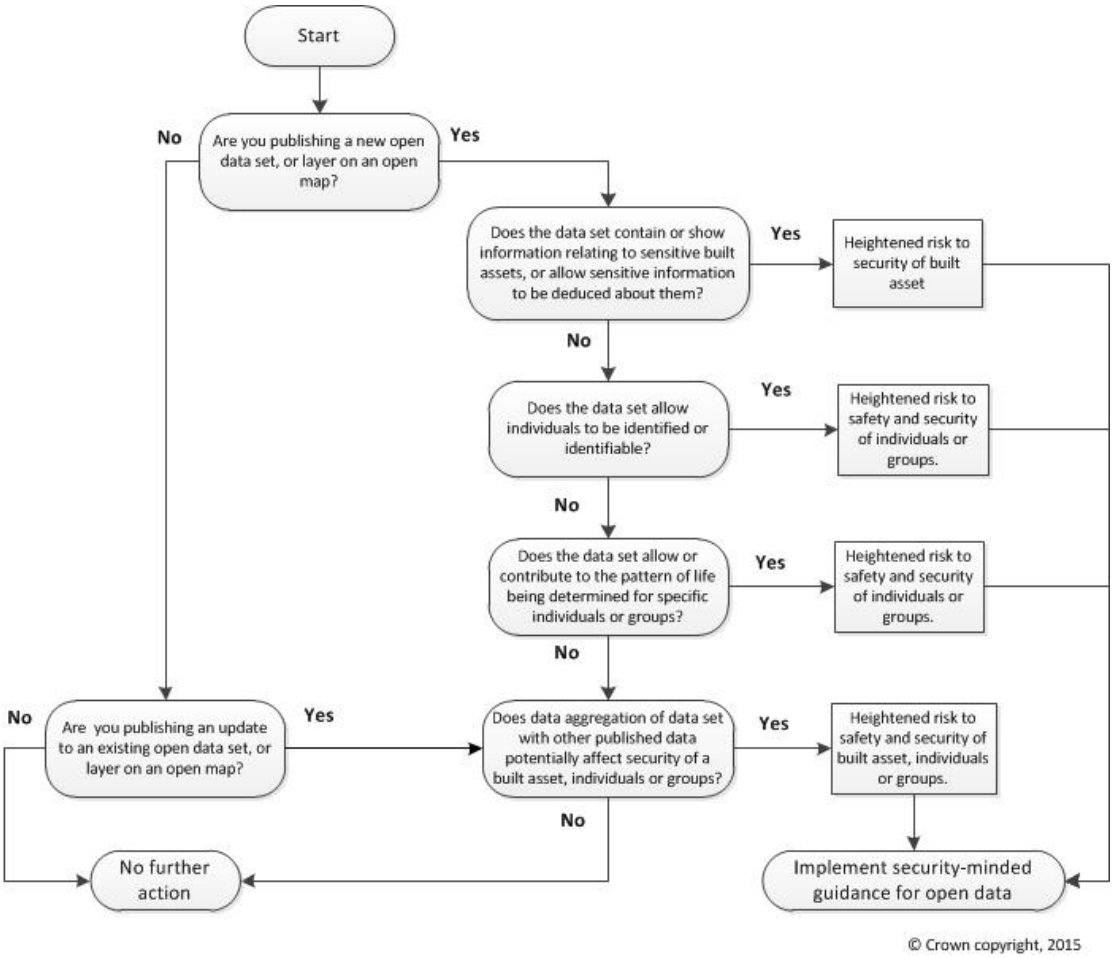


Figure 2. Open data security triage process

Further information on the concept of security and the different security issues which are relevant to open data can be found in Clause 4 of PAS 1192-5.

Where there is any uncertainty as to the sensitivity of data, appropriate advice should be sought. Information on sources of advice can be found in Clause 5.1.2 of PAS 1192-5.

Open data - managing risk

Where the open data security triage process identifies the need for a security-minded approach, it will be necessary to develop a risk management strategy comprising a risk assessment, risk mitigation, and a process of review. The risk management process is shown in Figure 3 below.

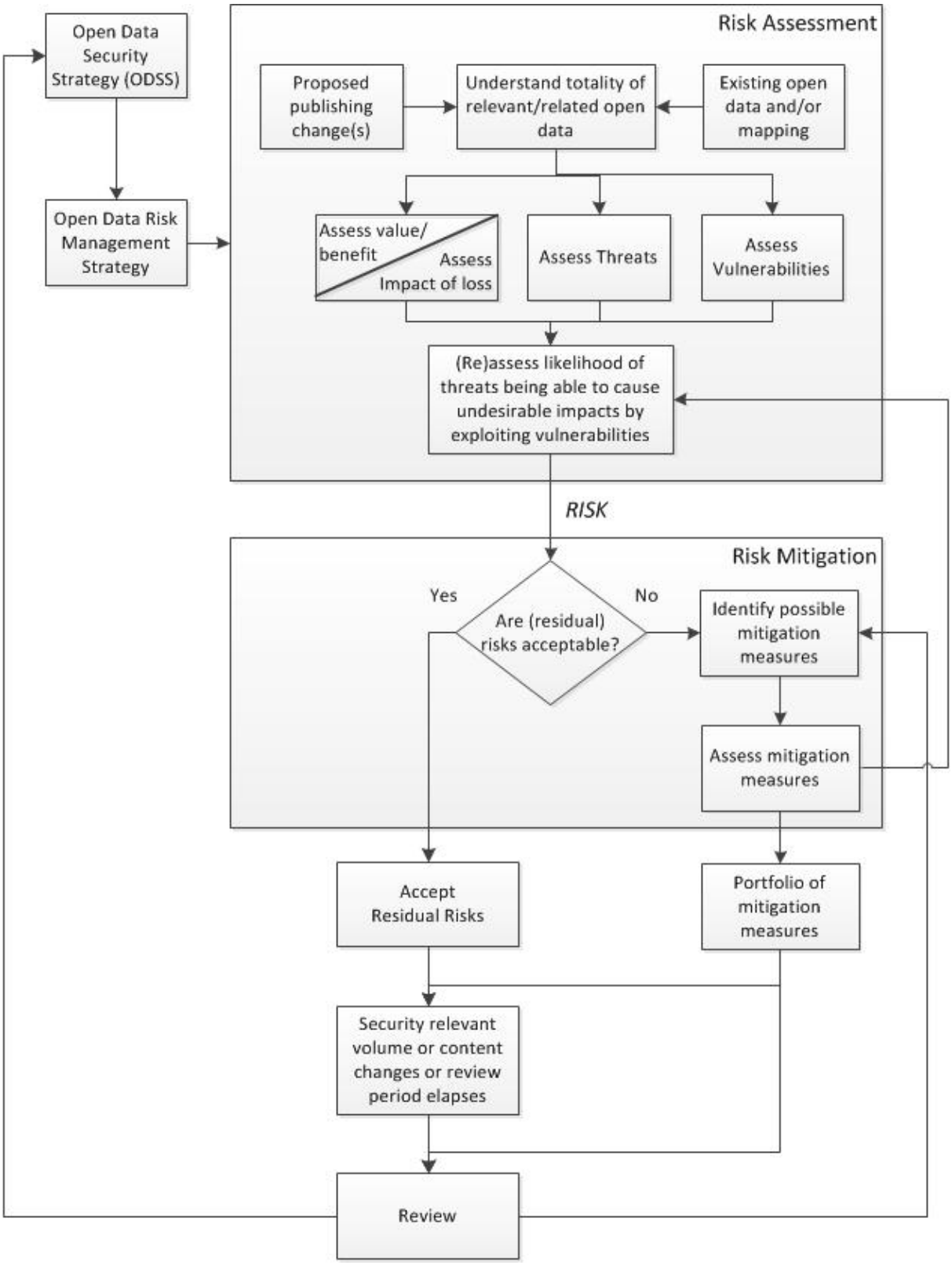


Figure 3. Open data risk management process [adapted from Fig 6 - PAS 1192-5:2015, reproduced with the kind permission of BSI]

Further information on the risk assessment, risk mitigation and review processes can be found in Clauses 7.2.2.1, 7.2.3, and 7.2.4 of PAS 1192-5.

Risk mitigation measures which it may be appropriate to adopt include:

- removing a sub-set of the data from the published data set where only that sub-set creates a risk;
- reducing the precision of the information where the precision of location or timing data increases the risk;
- providing the data in summary form to reduce the level of detail available where the granularity of the data increases the risk;
- publish the data set without the metadata, or remove the sensitive fields, where the metadata creates a risk;
- reduce the level of detail and/or remove some layers of mapped data as a user zooms in to view a locality where the granularity of the data increases the risk; and
- monitoring access by requiring user registration/login to access specific data sets.

Open Data Security Strategy (ODSS)

It is recommended that an ODSS in line with Clauses 7.1.1, 7.1.2 and 7.1.3 of PAS 1192-5 is developed.

To maintain its relevance and validity, the ODSS and its inherent risk management strategy cannot be static and it is therefore necessary to have in place a suitable mechanism for its periodic review. The review process should identify and assess any risks which have changed for political, economic, social, technological, legal or environmental reasons.

Reviews should be undertaken:

- prior to publication of an open data set;
- on a periodic basis to assess the data aggregation risks associated with material published by other data owners;
- in the event of a security breach or incident;
- in response to the development of new tools and techniques to analyse data.

Access to any part of the ODSS that details the security risks and/or potential mitigation measures, should be managed on a strict need-to-know basis, with all such information subject to security measures appropriate to the level of risk, with regard to its creation, storage, distribution and use.

Open Data Security Management Plan (ODSMP)

It is vital that the policies, processes and procedures implement a holistic approach which addresses security around the aspects of people and process, as well as physical and/or technological security.

People need to be aware of, and understand, the security policies in place. Alongside this, the security processes and measures, be they physical or technological, need to be effective and efficient. Without any one of these elements the effectiveness of the overall security regime will be reduced and there is real risk that the measures in place will be ignored or circumvented.

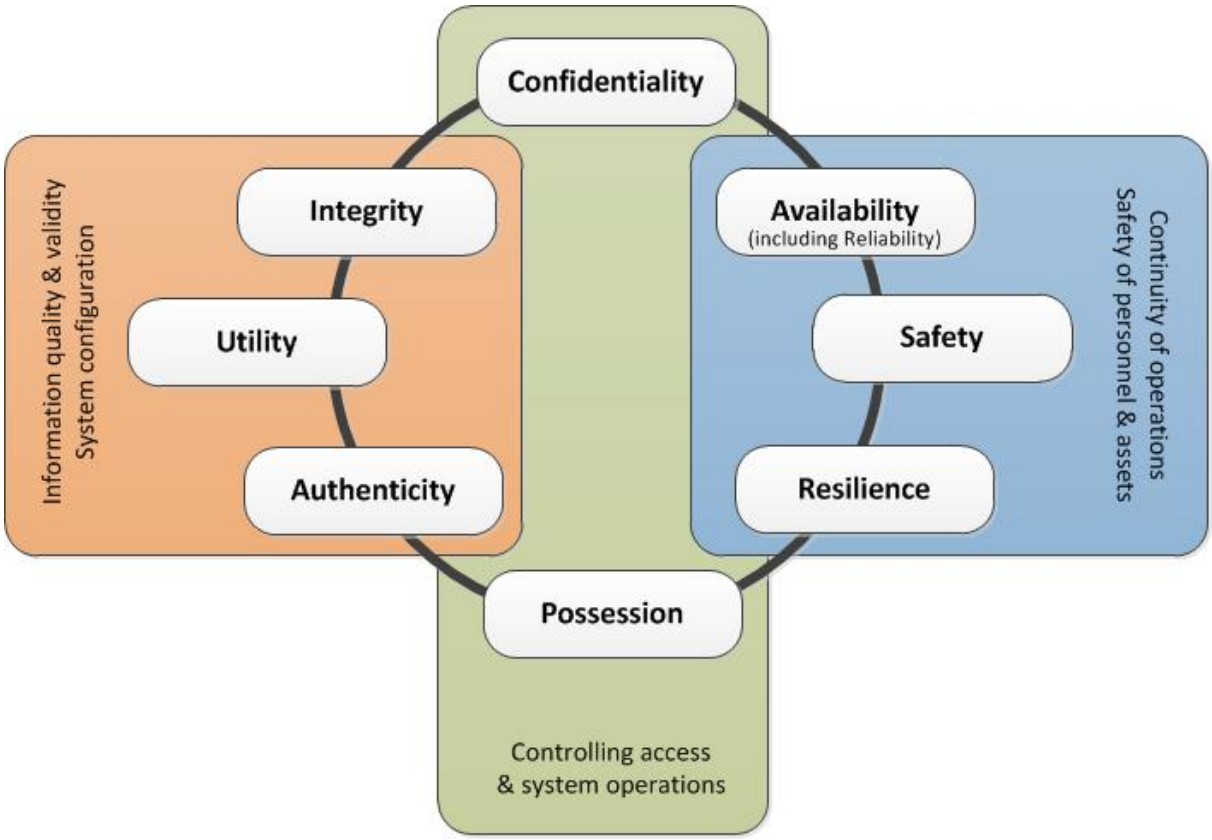
The ODSMP should include:

a) the policies, processes and procedures for the preparation, release, storage and dissemination of the open data, including the technical security requirements covering the aspects shown in Figure 4 below and described on page 2 of this guidance;
b) monitoring, auditing and review arrangements;
c) a plan for handling security breaches and incidents, in line with Clause 9 of PAS 1192-5; and

d) the process and procedures for the provision of information to third parties who intend to publish the data, including an outline of the contractual or licensing measures required.

As with the ODSS, a suitable mechanism for the periodic review of the ODSMP will need to be in place.

Access to any part of the ODSMP which details sensitive: requirements; systems; policies; processes; and/or procedures should be managed on a strict need-to-know basis, with all such information subject to appropriate security measures with regards to its creation, storage, distribution and use.



NOTE Reproduced with kind permission of CPNI and Hugh Boyes

Figure 4. Technical security requirements

Accountability and responsibility for the security-minded approach

It will be necessary for an individual to be responsible for the security-minded approach adopted. This role should:

a) consult with the data originator regarding potential security and data aggregation issues;
b) take ownership, and manage the development, of the ODSS and ODSMP;
c) be accountable for security decisions that are taken;
d) advise on the need for, and undertake, the review and auditing of documentation, policies, processes and procedures relating to the security of the open data;
e) where appropriate and necessary, seek appropriate professional security advice to provide additional guidance throughout the lifecycle of the open data.

Compliance with other legislation and standards

The ODSS and ODSMP should take into consideration relevant legislation and regulations. Further information can be found in Clause 13 of PAS 1192-5.