Department for Business, Energy & Industrial Strategy
CPNI Centre for the Protection of National Infrastructure
National Cyber Security Centre a part of GCHQ

Joint Ventures in the Construction Sector: Information Security Best Practice Guidance

August 2022

About this Guidance

This guidance is for construction industry Joint Ventures (JV) and businesses of all sizes planning to take part in Joint Ventures. It relates to the holistic security approach JVs should adopt to protect any sensitive information they manage. Guidance on personnel, physical and cyber security measures more generally is available from the Centre for the Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC).

- Section 1 of this guidance is aimed at business owners and JV Board members. It describes why information security matters to the construction industry, and particularly to JVs.
- Section 2 is aimed at Board members and JV Information Security and IT experts from each of the parent companies. It describes the key steps that should be taken to ensure a JV's information is secure.
- Section 3 provides focused advice for IS and IT operations specialists on producing detailed plans for securing information of a JV.

Section 1
Why Information Security Matters in JVs

- Business Owners
- JV Board Members

Section 2
Key Steps for Securing Joint Ventures

- JV Board Members
- Group IT Directors (CIO)*
- Head of Infosec (CISOs)*
- Security or Operational IT practitioners*

Section 3
The Security Management Plan

- Group IT Directors (CIO)*
- Head of Infosec (CISOs)*
- Security or Operational IT practitioners*

Business Owners:

Understand the importance of cybersecurity to JVs and ensure key staff are empowered to implement the guidance.

JV Board Members:

Ensure that security is appropriately represented on the JV Board.

Group IT Directors (CIO):

Ensure that the IT infrastructure needed to support the proposed JV is secure.

Head of Infosec (CISOs):

Ensure that the Information Security Management Plan is appropriate and proportionate to the JV.

Security or Operational IT practitioners:

Ensure that the Information Security Management Plan is aligned with industry best practice

*from the parent companies

Acknowledgements

This guidance was produced by members of the Civil Engineering, Architecture and Construction (CEAC) Trust Group in collaboration with the Department for Business, Energy and Industrial Strategy (BEIS), CPNI, and NCSC.

The authors are grateful for the support and input provided by the following organisations:

Balfour Beatty

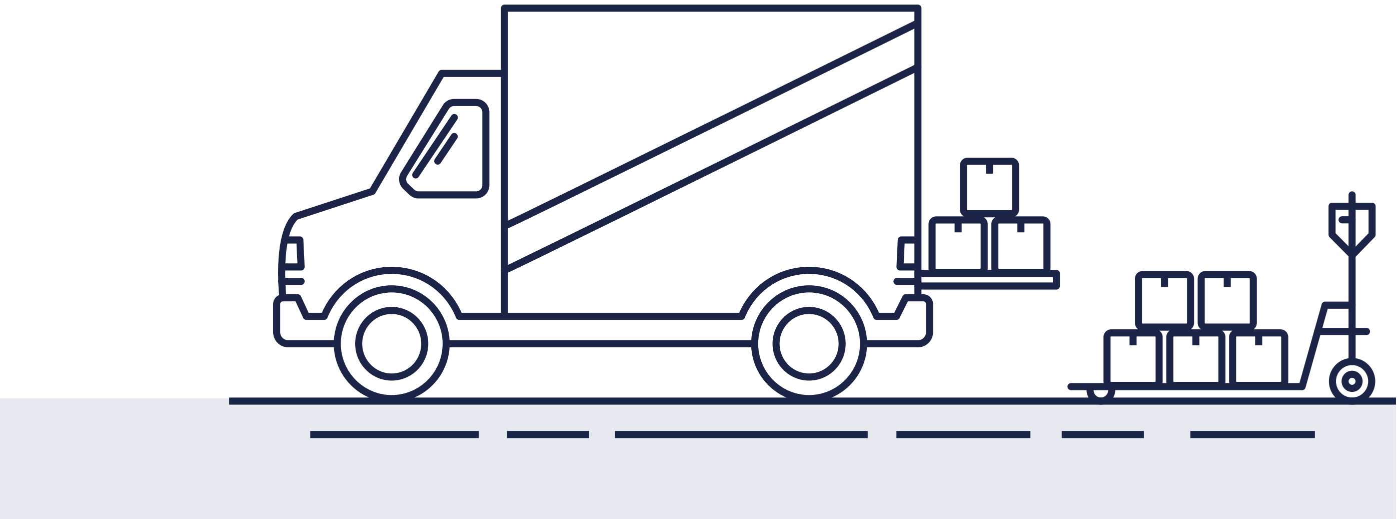
bam

GallifordTry

MORGAN SINDALL GROUP

Sir Robert McALPINE

The authors also acknowledge and appreciate the review of draft material by: Aggregate Industries, Amey plc, Arup Group, Atkins, Barratt Developments plc, BDP Ltd, The Berkeley Group Holdings plc, Bloor Homes, Costain Group, Foster + Partners, J. Murphy & Sons Ltd, Keepmoat Homes Ltd, Kier Group plc, Knights Brown Construction Ltd, Laing O'Rourke, The Mott MacDonald Group, Persimmon plc, Redrow plc, Rogers Stirk Harbour + Partners LLP, Skanska UK, United Living Group, VolkerWessels UK, Willmott Dixon, and WSP UK Ltd.



Section 1

Why Information Security Matters in JVs

Why Information Security Matters in JVs

Digitalisation in the construction sector is bringing greater efficiency, reduced costs and wider data sharing. It is also creating a paradigm in which larger and larger volumes of data are created and digitally stored for every project. **The success of a project now relies on the confidentiality, integrity and availability of its information and IT systems.**

These changes mean the industry is increasingly of interest to threat actors – including cyber criminals, foreign state actors and malicious insiders – who may seek to steal, misuse, modify, damage or deny access to key information, with the potential for significant impacts on victims. Importantly, the threat is not to large companies only: criminals can target all sizes of construction business. NCSC has recently published guidance[1] for SMEs on protecting themselves from cyber threats.

Successful attacks by malicious actors can be extremely costly and jeopardise project success:

a. **Ransomware attacks** – in which cybercriminals encrypt and/or steal data to extort ransom payments – cost UK businesses £365 million in 2020[2]. Globally, construction is one of the sectors most targeted by ransomware and multiple UK companies have been affected in recent years[3].

b. **Data breaches can incur heavy fines** under the UK Data Protection Act 2018 (up to £17.5 million or 4% of annual global turnover) – and can also **delay projects** and **impact the reputation** of affected companies.

As well as malicious attacks, accidental actions can also impact a project's information security. These might include sharing sensitive information in a presentation or published article, leaving commercial information on a memory stick on site, or even re-using software containing unsanitised data from a previous project. These accidents can constitute regulatory breaches and lead to the leaking of sensitive information into the public domain.

[1] NCSC's guidance for SMEs can be found on the NCSC website
[2] Serbus Report
[3] Nordlocker - Ransomware Attacks by Sector

Information security risks are **particularly relevant to Joint Ventures** (JV) due to:

a. Their **large monetary value;**

b. The **high volumes of potentially sensitive data** they can potentially generate, process, share and store;

c. Potential **differences in partners' approaches** to security and risk appetite;

d. The **complexity** of their IT infrastructure;

e. Their potential **physical proximity to other significant assets**; and

f. Their **large site structures,** which make them difficult to secure against physical attacks.

Adopting a standardised approach to JV information security is key to addressing these concerns, and will yield benefits including:

a. **Minimisation of delays, cost and complexity caused by retrofitting security measures**;

b. Increased compliance with regulations bringing **reduced risk of fines and prosecution**;

c. **Reduced likelihood of monetary loss or reputational damage** as a result of a physical or cyber security incident;

d. Clear roles, responsibilities and accountabilities **reducing friction between partners**; and

e. **More accurate IT cost estimates and better infrastructure provision.**

This guidance provides a set of **non-mandatory recommendations** for ensuring information security in JVs together with details of how recommendations might best be implemented. At a high level, its main requirements are that **security is represented at JV Board level** and that individuals responsible for information security from a personnel, physical and cyber security perspective understand and address the specific challenges facing JVs.

Section 2

Key Steps for Securing Joint Ventures' Information

2.1 Overview

This section outlines five steps that should be taken to keep JVs' information secure throughout the project lifecycle and is consistent with the process set out in ISO 19650-5 which relates to security-minded information management:

Step 1: Establish Information Security Governance and Accountability;

Step 2: Assign Key Roles and Responsibilities;

Step 3: Understand the JV-specific Information Security Risks and Requirements;

Step 4: Develop and Agree an Information Security Strategy; and

Step 5: Design and Implement an Information Security Management Plan.

It is mainly aimed at the CISOs and CIOs of JV partners, as well as JV Board members, who should use it as a high level guide to securing JVs' information by ensuring each step is followed in sequence.

2.2 Step 1:
Establish Information Security Governance and Accountability

In order to ensure that information security challenges are properly understood and addressed, JVs should establish a security-minded approach – **with information security considered part of the JV's objectives and risks**. To achieve this, JVs should:

1. Ensure that their JV Board includes an **Information Security Sponsor** who is ultimately accountable for the Venture's information security;
2. Appoint a team to develop the details of the security-minded approach with **clear roles and responsibilities**; and
3. **Review and, if required, update appointments** at regular intervals.

Practically, the main Information Security Sponsor will be accountable for:

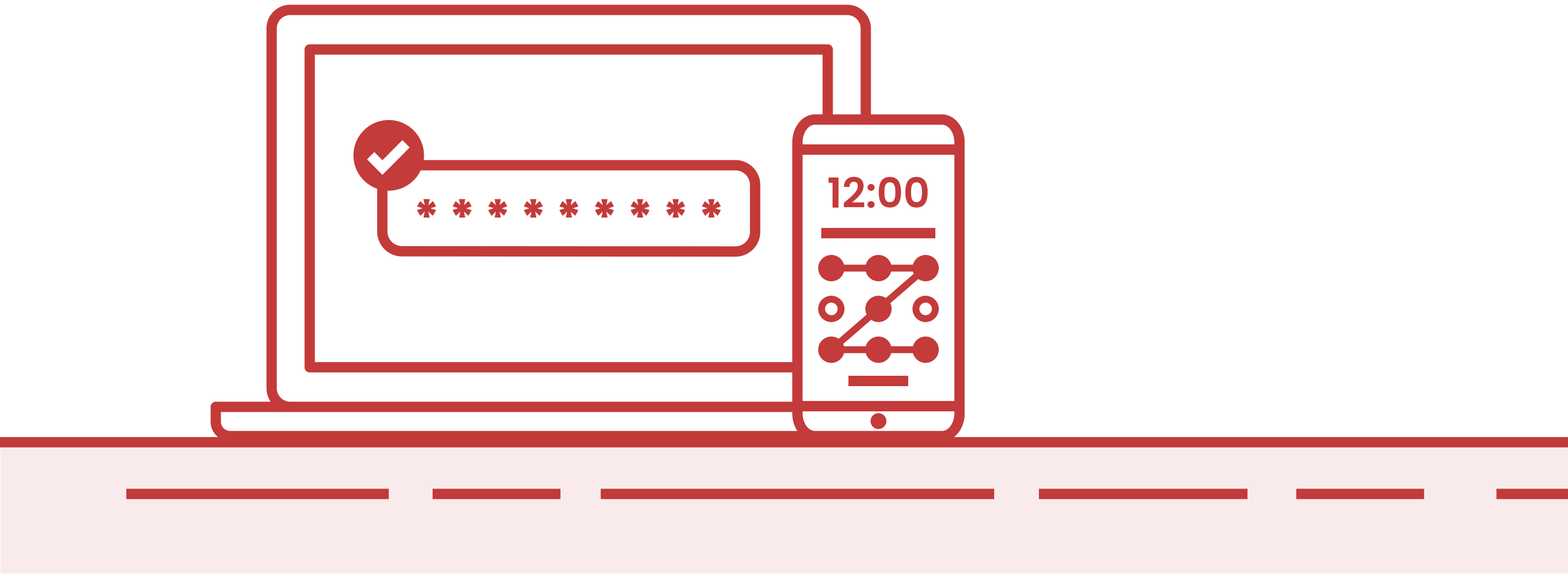
a. Overseeing the completion of key steps as outlined in this guidance; and

b. Owning any residual information security risks.

Key Steps for Securing Joint Ventures' Information

They don't need to **be a security specialist** (it is not expected that every JV Board will have a security professional on it), but should be prepared to act as an executive sponsor to ensure the successful delegation and completion of key actions and to seek specialist guidance where required. They will also play a cultural role in ensuring that the JV adopts the security-minded approach. This might include **reinforcing to other Board members (or representatives of JV Partners) the importance of information security**, or using their authority to ensure that information security concerns are given the appropriate consideration at Board level.

JV Partners should ensure that copies of this guidance are disseminated to all members of the JV Board. It should be understood by Board members that although the Information Security Sponsor is accountable for guiding information security activity, **information security is the responsibility of the entire JV Board**, as any security incident is likely to have repercussions affecting the whole JV.



2.3 Step 2:
Assign Key Roles and Responsibilities

After establishing a governance structure, JV partners should identify staff responsible for:

a. **Assessing the specific information security risks and requirements** faced by the JV (Step 3 – Section 2.4);

b. **Developing a JV-wide information security strategy** (Step 4 – Section 2.5); and

c. Overseeing the translation of the security strategy into a JV-specific information **security management plan** (Step 5 - Section 2.6 and Section 3) that implements the policies, processes and security controls to support the aims and objectives of the strategy.

Exact responsibilities will vary between JVs depending on their nature and constraints (see Section 2.4); however, at a minimum every JV should identify individuals for the following types of roles – the exact role titles may be different in different JVs:

Role	Responsibilities
	Wider JV Board
JV Information Security Lead	Manages the JV's information security strategy, security management plan, and day-to-day information security needs. This is the equivalent of a CISO.
JV IT Lead	Works with the Information Secuity Lead to provide the necessary IT infrastructure to support the JV's IT needs. This role is often supported by internal teams within the partner organisations.
JV Security Controller	A representative of each JV Partner, who oversees their own organisation's information security activity and collaborates with other Security Controllers to define JV-wide information security strategies and plans.
JV Data Controller	Ensures that the JV as a whole meets its obligations under the Data Protection Act 2018.
JV Data Processors (multiple)	Operate as 'Processors' within the Data Protection Act 2018 framework.
JV Data Protection Officer (DPO) or Privacy Officer (if required)	A single named individual, who informs and advises the Board on data protection, and monitors compliance with the Data Protection Act (and possibly other legislation, see Section 2.4).

Table 2.1 – Suggested Information Security Roles

Note that **different roles do not necessarily need to be filled by different staff.**

Responsibility for ensuring individuals are chosen to fill these roles ultimately rests with the main Information Security Sponsor; however, it is recommended that:

a. The **Information Security Lead** is an individual with **strong awareness of the importance of information security,** who will be **willing to work with CISOs of JV partners;**

b. The **IT Lead** is a representative of the organisation **responsible for providing IT infrastructure** to the JV; and

c. The **Security Controllers** are security professionals within each JV Partner with an understanding of their own organisation's information security strategies, policies and plans. Typically the JV Security Controller sits as a named member of staff within the JV. The role may or may not be a full time role depending on the size of the JV.

2.4 Step 3:
Understand the JV-specific Information Security Risks and Requirements

With a governance structure established and key roles identified, the next step is to understand at a high level the specific information security challenge faced by the JV. The Information Security Lead and Security Controllers must:

a. Assess the **high level information security risk facing the JV**;

b. Identify any relevant **regulatory requirements**; and

c. Decide on the JV's **risk appetite**.

Assessing the Risk

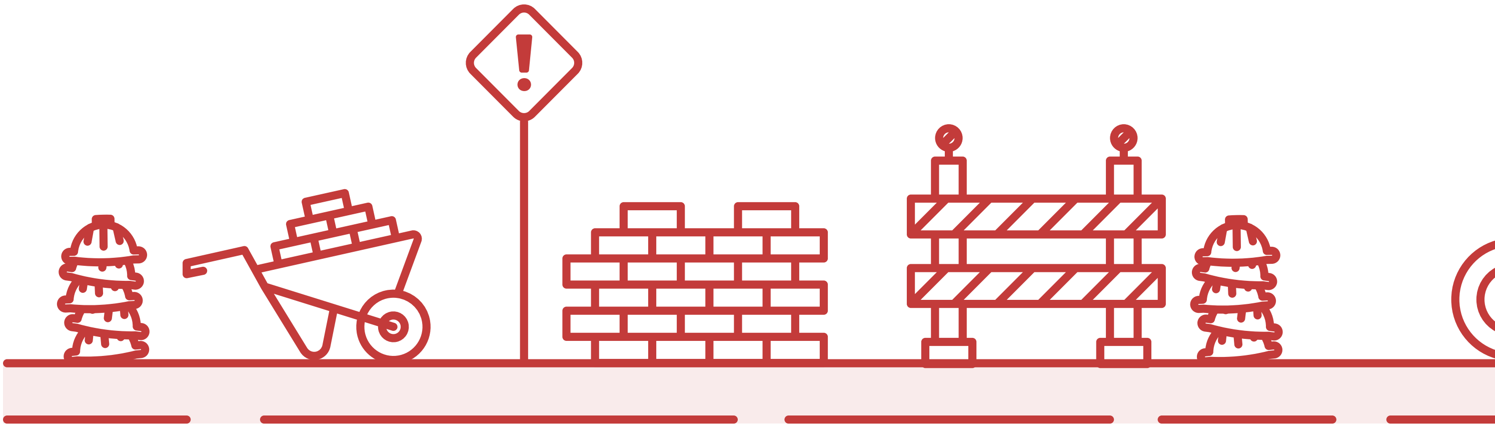
Triaging the JV-specific challenge begins with characterizing the IS risk facing the JV. This does not mean performing an in-depth risk assessment, rather identifying at a high level the scale of risk. To achieve this, the IS Lead and Security Controllers should discuss and agree on:

The JV's Information Classification Requirements – What is the highest sensitivity of information to be held by the JV? What volume of information at this sensitivity is the JV expected to hold? (If classification terminology differs between the JV and its partners then a mapping matrix should be created to reflect this);

The JV's relationship to neighbouring assets – Will the JV hold sensitive information relating to neighbouring assets. If so, what controls will the JV need to apply to protect this information?

The JV's Size and Value – Is the JV sufficiently large, both in terms of number of participants and monetary value, to represent an attractive target for attackers?:

What is important is not that the risk is ascribed a particular value, but that there is a consensus on the overall risk facing the work relative to other JVs.



Identifying Regulatory Requirements

The Information Security Lead and Security Controllers should then identify any laws and regulations that the JV must comply with. These are in addition to the Data Protection Act which applies to all JVs. Possible regulations include:

a. **The Freedom of Information Act (FoIA) 2000** – if the project involves public authority information not specifically exempt under the Act; or

b. **The Official Secrets Act (OSA) 1989** – if the project involves classified government information that could comprise national security or national interests if leaked.

If there is uncertainty over which regulations might apply, then the individuals responsible should seek clarification from the customer or the relevant legislative body. Failing to identify regulatory requirements greatly increases the risk of future failure to comply.

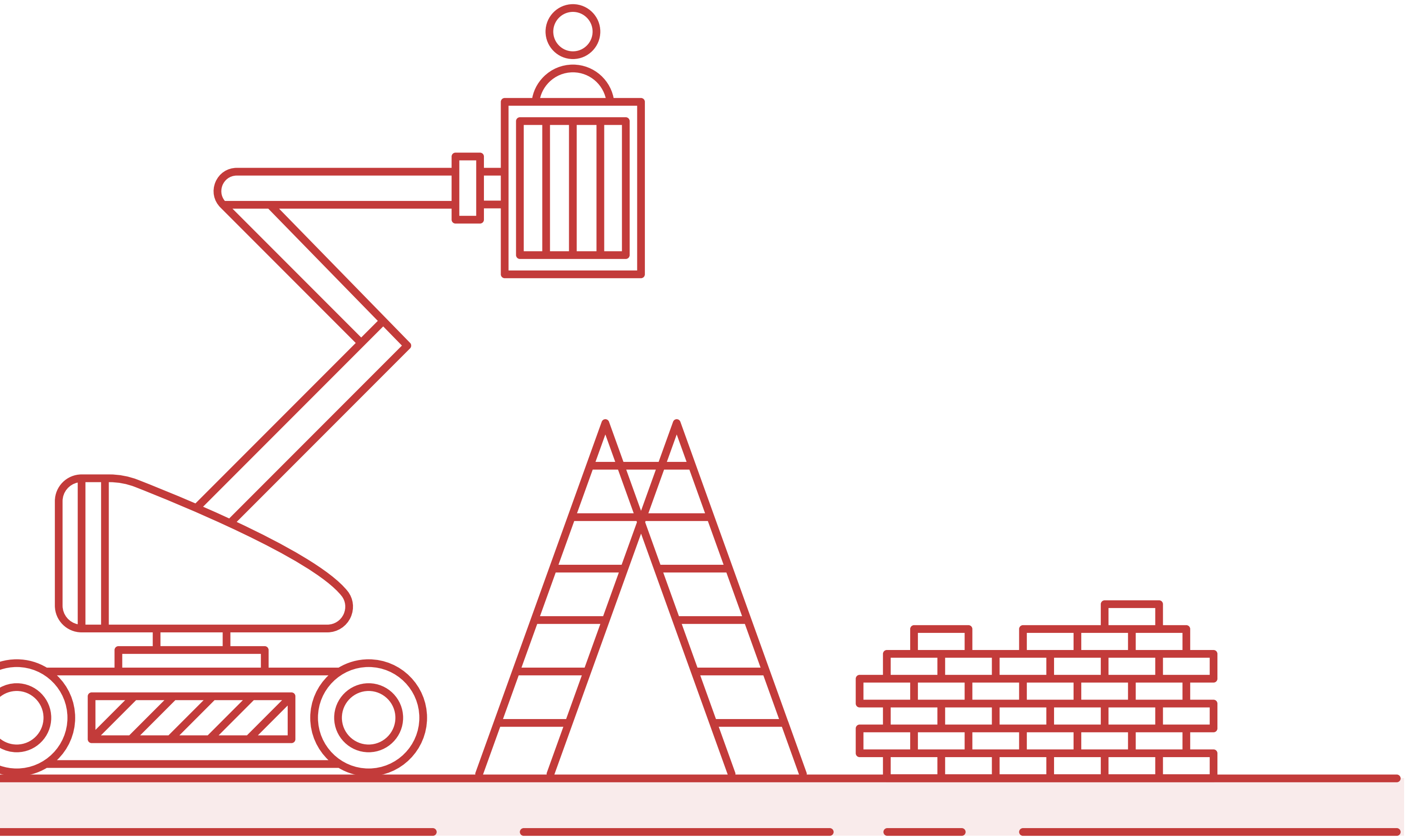
Deciding a Risk Appetite

Finally, the Information Security Lead and Security Controllers should then decide on the JV's risk appetite.

This may be challenging; 'risk appetite' is a term highly subject to interpretation, and it is likely that JV Partners will have different approaches to determining their own risk appetites.

It is recommended that the Information Security Lead and Security Controllers together first agree the risk appetite framework to be used, determine the risk appetite level, and then share material between themselves to ensure that the appetite's practical meaning is well understood.

As a starting point, the Information Security Lead and Security Controllers might consider NCSC's guidance on risk appetite.



2.5 Step 4:
Develop and Agree an Information Security Strategy

Once the high level information security challenge is understood, the Information Security Lead, IT lead, and Security Controllers should develop and agree on a JV-specific Information Security Strategy.

This Strategy may build on the existing one(s) employed by the Information Security Lead's organisation(s), but should reflect the JV's overall risk level, regulatory requirements and risk appetite decided in Step 3.

In practice, the Information Security Strategy should constitute a single document detailing:

a. The JV's **Governance and Management Framework** (Section 2.2) and Roles, Accountabilities and Responsibilities (Section 2.3);

b. The JV's **Data Classification** and **Regulatory** Requirements (Section 2.4);

c. A proposed **Information Security Risk Management** approach for determining granular JV-specific information security risks and their mitigations;

d. The proposed **approach to manage physical** (e.g., CCTV, site access, etc.) and **personnel** (e.g., clearance requirements, JML (joiners, movers & leavers) processes, etc.) and **cyber** security required to manage information security risks which exceed the agreed risk appetite of the JV;

e. The outline of a **closure process** for the JV. This should establish ownership of any information assets developed by the JV, retention periods for developed information assets, practices for archiving these assets, and responsibility for information assets post JV closure; and

f. A plan for the **regular review** and, if necessary, update of the Information Security Strategy.

The Information Security Strategy should also reflect any additional requirements identified by the JV customer. The Board should consider whether any cyber insurance covers all data relevant to the JV, and consider whether additional JV-specific cyber insurance is required. If the Board decides to purchase Cyber Security Insurance at JV level, this should also be recorded. The Strategy should be reviewed by the customer and signed off by the JV Board.

2.6 Step 5:
Design and Implement an Information Security Management Plan

The final step in securing a JV is **interpreting its overall Information Security Strategy to produce and implement a concrete and fully costed Information Security Management Plan**. This will require information security expertise and should be developed by **qualified practitioners** drawn from the JV partners and **overseen by the Security Controllers**.

Section 3 of this guidance provides recommendations for creating a secure and complete **Information Security Management Plan**.

Section 3 of this guidance provides recommendations for creating a secure and complete **Information Security Management Plan.**

Section 3

The Information Security Management Plan

3.1 Overview

This section provides recommendations and guiding principles for producing an Information Security Management Plan. It is aimed at **security and IT operations** specialists who should use it to develop a Plan aligned with the JV's **Information Security Strategy**.

The **JV Information Security and JV IT Lead** will have joint ownership of the Information Security Management Plan, and will be responsible for identifying team members for its development.

To avoid duplication and unnecessary effort, the Information Security Management Plan should **adopt and adapt existing policies, practices and procedures employed by JV partner organisations** wherever appropriate. This will ensure that existing domain expertise is utilised wherever possible.

A complete Information Security Management Plan should cover:

a. The JV's **Information Security Risk Management** approach (Section 3.2);

b. The JV's **Identity and Access Management** (IAM) solution (Section 3.3);

c. The JV's **Continuity Strategy** (Section 3.4);

d. Any needs for **JV-specific security training**, creating a security culture to ensure the correct handling of classified data, or **raising the security-awareness of staff** (Section 3.5);

e. The JV's **physical security requirements** for security of on-site data (Section 3.6)

f. The JV's **HR security policies** (Section 3.7); and

g. The JV's **approach to 3rd Party Suppliers** (Section 3.8).

Gaps or omissions in the Information Security Management Plan will reduce effectiveness of the Information Security Strategy and increase the risk of a security breach or incident.

To ensure that the Plan remains fit-for-purpose, security controls should be regularly monitored, tested and audited for their effectiveness. The Plan in its entirety should be reviewed annually, with its sections additionally reviewed after any security incident affecting them. If review suggests any changes or updates these should be communicated to the Information Security and IT leads.

3.2 Information Security Management (ISM)

The first step in developing an Information Security Management Plan is agreeing and implementing the JV's approach to identifying, assessing and controlling risks to its shared IT infrastructure.

This guidance does not prescribe a specific approach but recommends that JV partners draw on their existing expertise in widely understood methodologies including ISO 27001, NCSC CAF, or NIST CSF.

The chosen approach should include strategies for the following activities[4] but should not be considered an exhaustive list:

a. Identify

Determination of JV information security risks by:

1. Identifying the business-critical (information and non-information) assets, procedures, processes and capabilities and determining their threats, vulnerabilities and risks; and
2. Establishing operational policies for security, e.g., Acceptable Use Policy, Mobile Devices and Teleworking Policy, etc., that include roles and responsibilities and details of the consequences if broken.

b. Protect

Use of appropriate controls to ensure secure delivery of service by:

1. Managing access to assets and information using a need to know/least privilege approach (see also Section 3.3);
2. Protecting sensitive data in transit and at rest as well as performing regular on-site and off-site backups;
3. Protecting end devices using end-point security products and implementing a JV-wide patch/update solution; and
4. Establishing a JV-specific Security Education Training and Awareness (SETA) programme (see also Section 3.5) and embedding a security-minded culture.

c. Detect

Deployment of tools and processes to identify security events through:

1. Developing a business impact analysis of information security events to help identify the most critical business areas;
2. Network defence measures, for example, Host-based/Network Intrusion Detection Systems (HIDS/NIDS), are deployed strategically and working; and
3. Ensuring appropriate logging measures are in place that are monitored and secured.

c. Respond and Recover

Establishing and documenting the processes for dealing with a detected security event by:

1. Developing, testing and subsequently updating all response and recovery plans (see also Section 3.4);
2. Identifying, informing and liaising with internal and external stakeholders including regulatory bodies and fulfilling legal obligations, e.g. informing the ICO of a data breach as soon as practicable, but no later than 72 hours after it has occurred; and
3. Managing public relations to protect the JV's reputation.

Once an ISM approach is chosen, representatives of the partners **should perform a gap analysis against their own enterprise ISM approach** to identify any areas where there is a need for process change.

Where possible J**V partners should also pursue alignment with standards, particularly Cyber Essentials, for their IT systems and processes.** While not mandatory, certification can demonstrate a degree of cyber maturity, and some government contracts may require it to be in place. If certification is not achievable, JV partners should aim to document how they enforce UK Cyber Essentials controls, with exceptions recorded on the JV's risk register. This will provide assurance that, at the very least, a minimum of cyber security hygiene is in place. **JVs should also seek to comply with the requirements set out in ISO 19650-5.**

[4] The main areas of concern shown here are based on a NIST CSF approach.

3.3 Identity and Access Management

To secure the complex relationships between partners, JVs should use a **common identity governance framework** supported by a **shared Identity and Access Management (IAM) solution**.

The framework should describe and document the different types of identities, roles and access rights of the JV and how these map onto the existing staff profiles in the partner organisations.

The framework should also establish security requirements for accessing IT infrastructure. This should include password policies, as well as multifactor authentication and single-sign-on strategies implemented for privileged accounts.

The companion IAM solution **should as a minimum, enable all aspects of the proposed governance framework**. It might also:

a. Integrate with and support the appropriate HR JML processes for the JV; and

b. Support integration with the JV partners' IAM solutions to facilitate the creation of trust relationships if appropriate.

3.4 Incident Management, Disaster Recovery and Business Continuity

Like other organisations, JVs need to ensure that there are **documented processes and procedures in place** to detect, respond to and recover from information security events. In the case of a JV, this can be done by reusing and adapting existing practices.

The main processes involved in the creation of a continuity strategy are:

a. Identifying mission- or business-critical functions and the resources that support them;

b. Anticipating potential contingencies or disasters; and

c. Developing, implementing and testing appropriate continuity strategies.

JVs should produce, ratify and distribute documents including an Incident Response Plan (IRP), a Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) covering:

a. **IRP** – the immediate response of a detected information-related incident. If an incident escalates or is disastrous, the process changes to DRP or even BCP;

b. **DRP** – restoring systems after an information-related incident has occurred, e.g. after a successful breach of a web-server or water damage to several servers; and

c. **BCP** – the recovery of business processes in response to major or long term damage, e.g. fire or flooding at the primary data centre, ransomware on mission-critical servers. This will typically be used concurrently to the DRP.

In order to inform the IRP, DRP and BCP, the JV should carry out a **Business Impact Analysis** (BIA) to determine likely threat scenarios, the business units they affect, and damage they might cause. This should be used to identify priority systems and activities to be addressed in the plans.

To complement these plans, the JV should also deploy monitoring tools/solutions to detect attacks as early as possible. Potential tools/solutions include:

a. Intrusion Detection System: both host and network based;

b. Cloud Provider-based solutions;

c. Log monitoring, firewall and anti-virus software; and

d. Increased staff awareness through targeted SETA training (Section 3.5) and a security-minded culture.

3.5 Security Education, Training and Awareness (SETA)

Although each JV partner is likely to have their own SETA programme, the formation of a JV poses its own challenges as **training provisions are likely to differ between partners**. This may lead to gaps in the training provision between staff members of the different organisations. To address this, the JV should establish a **shared SETA baseline**. This should address personnel, physical and cyber security measures required to protect information.

Exact security training and awareness levels depend on staff roles and data access privileges; requirements for each staff role should be explicitly decided and agreed upon between JV partners. Partners should then perform **gap analyses** between their existing SETA provisions and level of security training and awareness expected of staff operating at the JV level. Where gaps are identified, JV partners should ensure that their staff:

a. Read and confirm they understand any new, JV-specific information security policies;

b. Are aware of the potential disciplinary actions in case of a breach; and

c. Are provided with any additional security training required for their roles.

Once the appropriate training needs have been identified and implemented, they should be embedded into the Joiners, Movers and Leavers HR processes. Any training should be refreshed on an annual basis and following a related security incident.

In the case of staff hired directly by the JV (rather than through individual partners), it will be the responsibility of the JV Information Security Lead and their organisation to ensure that the new personnel receive training to bring them up to the SETA baseline.

Information on developing a security-minded culture is available on the CPNI website.

3.6 Physical Security

As JVs often deliver major construction/infrastructure, there is a critical need for appropriate physical security to ensure information assets are protected from threats. Site security controls are already relatively mature in the sector given the need to protect expensive physical assets, but it will be important to determine what additional measures are required to threats to information assets.

It is important to recognise, however, that in a JV setting the nature of the data (i.e. high volume and sensitivity) and project size (multi-year, multi-million-pound and with potentially sensitive neighbouring assets) may necessitate additional on-site security controls than would otherwise be required.

Controls on Physical security might include:

a. **Perimeter Security** – including secure access, CCTV, ID checks, security screening of bags etc;

b. **Device Protection** – such as privacy screen protectors for laptops/monitors to prevent "shoulder-surfing"; and

c. **Disaster Protection** – including fire detection systems and uninterrupted power supplies.

The physical security controls implemented should be documented, tested and reviewed at regular intervals.

Information on physical security is available on the CPNI website.

3.6 Personnel Security

JVs may require additional personnel security controls beyond those already imposed by partners. In particular, access to certain sensitive information might require elevated security clearances for staff or additional legislative compliance from the JV partners.

These could include:

a. **Vetting requirements**: Counter Terrorist Check (CTC), Security Check (SC), or Developed Vetting (DV); and

b. **Official Secrets Act 1989**: the legal framework for handling information, documents and other articles whose unauthorised disclosure is considered damaging.

JVs need to implement appropriate HR processes to ensure that clearances can be obtained without impacting the recruitment/deployment of staff, and that staff sign declarations recognising their requirement to comply with any applicable policy and legislation.

Information on personnel security is available on the CPNI website

3.8 Supply Chain Security

To ensure a strong security baseline, supply chain security should be addressed in line with NCSC's guidance, which outlines 12 principles grouped into four key themes:

a. Understanding the risks posed by the supply chain:

   1. When engaging a supplier, understand what assets need to be protected and why;
   2. Do due diligence on the supplier and understand their security provision; and
   3. Determine and analyse the security risk posed by the supply chain.

d. Establish control to mitigate the identified risks:

   1. Communicate the JV's view of security needs to the suppliers;
   2. Set and communicate minimum security requirements for suppliers;
   3. Build security considerations into the contracting processes and require that the suppliers do the same;
   4. Meet the JV's own security responsibilities as a supplier and consumer;
   5. Raise awareness of security within the supply chain; and
   6. Provide support for security incidents.

g. Verify the effectiveness of the arrangements:

   1. Build assurance activities into the JV's supply chain management.

b. Continuous improvement by reviewing and updating the approach:

   1. Encourage the continuous improvement of security within the JV's supply chain; and
   2. Build trust with suppliers.

Additional guidance is available from CPNI.

The JV should identify standard minimum security requirements to insert into subcontractor and supplier contracts, and undertake activities to provide assurance that they are being complied with. These could be adapted from established processes at individual JV partners as appropriate.

To achieve a further level of information security, JV partners might consider enrolling third party contractors in the JV's defined information security structure. Practically, this would involve identifying an individual as the Security Controller for the contractor (in a role paralleling the Security Controller at each of the JV Partners). This individual would then be responsible for performing a gap analysis of their systems and processes against the Information Security Management Plan; identifying any shortcomings; and maturing policies or educating staff to address them.

Given that subcontractors will typically be smaller companies with less developed information security policies, there may be a significant number of gaps – making full alignment a challenge. In this case, security practitioners from the JV partners could offer support and education to mitigate any particularly large gaps, athough responsibility for their compliance would still rest with the subcontractor representative.

Information Security Checklists

For Boards and Practitioners

A.1 Security Checklist for JV Boards

Step 1

Item:	Responsibility of:	Ref.	Check
Has a Main Information Security Sponsor for the JV been appointed to the Board?	Board Members	2.2	□
Does the JV Board understand the need for a security-minded approach to information management?	Main Information Security Sponsor, Board Members	2.2	□
Are channels in place to make sure information security issues are heard by the Board?	Main Information Security Sponsor, Board Members	2.2	□

Step 2

Item:	Responsibility of:	Ref.	Check
Have an Information Security and IT Lead been identified?	Main Information Security Sponsor	2.3	□
Has a Security Controller been identified for each of the JV partners?	Main Information Security Sponsor	2.3	□
Have Data Controllers, Processors, and Owners been identified to ensure DPA compliance?	Main Information Security Sponsor	2.3	□
Have individuals been identified as responsible for any other data legislation compliance identified as applicable in Step 3	Main Information Security Sponsor	2.3	□

Step 3

Item:	Responsibility of:	Ref.	Check
Have the Information Security Lead and Security Controllers been tasked with completing Step 3?	Main Information Security Sponsor	2.4	□
Has the high level relative information security risk been discussed and agreed?	Information Security Lead, Security Controllers	2.4	□
Have any additional legislative requirements been identified?	Information Security Lead, Security Controllers	2.4	□
Has a risk appetite been decided?	Information Security Lead, Security Controllers	2.4	□

Step 4

Item:	Responsibility of:	Ref.	Check
Have the Information Security Lead and Security Controllers been tasked with preparing an Information Security Strategy?	Main Information Security Sponsor	2.5	□
Has a JV-specific Information Security Strategy been drawn up covering all of the key elements identified in Section 2.5?	Information Security Lead, IT Lead, Security Controllers	2.5	□
Is existing cyber insurance adequate, or is JV-specific cyber insurance required?	Main Information Security Sponsor	2.5	□

Step 5

Item:	Responsibility of:	Ref.	Check
Have security practitioners representing the JV Partners been identified as responsible for the Information Security Management Plan?	Main Information Security Sponsor	2.6	□
Has an Information Security Management Plan been completed?	Security Controllers, Security Practitioners	2.6	□

A.2 Security Checklist for Practitioners

Step 5.1

Item:	Prompts:	Ref.	Check
Has a Main IS Sponsor for the JV been appointed to the Board?	How does the JV's ISM approach integrate with those of the JV partners? How are JV-specific risks going to be determined?	3.2	□
Does the agreed approach reflect the requirements outlined in Section 3.2?	Will certification/accreditation to any standard (Cyber Essentials, ISO 27001, etc) be pursued? Is there a need for JV-specific Cyber Insurance? Are physical and personnel security covered?	3.2	□

Step 5.2

Item:	Prompts:	Ref.	Check
Has the JV's IAM framework and solution been agreed?	What are the JV-specific roles and access rights? How do these roles map to the existing roles within the JV partners and how are any differences/gaps addressed?	3.3	□
Does the agreed approach reflect the requirements outlined in Section 3.3?	How are the "least privilege" and "separation of duties" principles implemented and enforced? What is the agreed MFA solution? How is the IAM solution integrated into the HR JML process?	3.3	□

Step 5.3

Item:	Prompts:	Ref.	Check
Has the JV's IAM framework and solution been agreed?	What are the JV-specific roles and access rights? How do these roles map to the existing roles within the JV partners and how are any differences/gaps addressed?	3.3	□

Step 5.3

Item:	Prompts:	Ref.	Check
Has a Business Impact Assessment been performed?	What are the JV's specific mission- and business-critical functions, especially those over and above the ones of the JV partners? What is the business impact if these functions are breached/attacked?	3.4	□
Has an Incident Management Plan been developed?	Have potential contingency and disasters been determined, documented and implemented, e.g., incident playbooks?	3.4	□
Has a Disaster Recovery Plan been developed?	How do these align with the JV's existing plans? Do these plans cover physical and personnel events?	3.4	□
Has a Business Continuity Plan been developed?	Are roles, responsibilities and routes of escalation clearly defined and documented? Have the plans been tested?	3.4	□
Has a monitoring strategy been implemented?	What are the intrusion detection and prevention solutions, e.g. firewalls; honeypots HIDS and NIDS, cloud-based supplier-provided? What is the Anti-Virus, Malware protection and alerting approach for servers and staff devices (laptops/PCs)? How are staff trained and sensitised to detect suspicious behaviour, e.g. gate-tailing, shoulder-surfing; social engineering?	3.4	□

Continued overleaf.

A.2 Security Checklist for Practitioners

Step 5.4

Item:	Prompts:	Ref.	Check
Has a SETA plan for the JV been established?	Have the JV-specific security awareness and training needs been identified and documented, especially those over and above the ones provided by the JV partners? Does the programme touch on physical and personnel security? How does the JV's SETA programme align with those of the JV partners, in particular how are any gaps going to be addressed? Has the JV's SETA programme been integrated into the JV's HR JML process? Are staff aware of the disciplinary consequences of failing to comply with the security requirements of their roles as a result of the SETA programme? Have the measures been put in place to develop a security-minded culture?	3.5	□

Step 5.5

Item:	Prompts:	Ref.	Check
Has a Physical Security Plan for the JV been drawn up?	Have all JV-specific physical security risks pertaining to information security been identified and documented, especially those over and above the ones normally associated with a construction project? What physical security measure will be used to ensure site security? Are staff trained and aware of the roles they play to ensure the physical security of staff as well as the construction sites?	3.6	□

Step 5.6

Item:	Prompts:	Ref.	Check
Have any additional Personnel Security requirements been identified, documented, and actioned?	What are the staff clearance requirements depending on their roles' access to potential sensitive data? Do existing staff have sufficient clearance to handle the JV's data to which they require access? Has the HR recruitment process accounted for the delay to obtain security clearance? Have staff been trained and made aware of their responsibilities in relation to the handling of sensitive data in accordance with their security clearance?	3.7	□

Step 5.7

Item:	Prompts:	Ref.	Check
Does the JV have a supply chain information security plan?	What are the JV-specific concerns regarding its supply chain, especially over and above the requirements already imposed by the JV partners? Are there procedures in place to flow requirements down to suppliers?	3.8	□

JV Information Security Roles and Responsibilities

B JV Information Security Roles and Responsibilities

B.1 Overview:

The table below summarises the proposed structure of the information security. Note that different roles do not necessarily need to be filled by different staff.

Information Security Role	Information Security Accountabilities and Responsibilities	Rationale
	JV Board	
JV Main Information Security Sponsor	• Owns the overall information security risk • Accepts the residual risk • Agrees and signs off ISM budget.	The equivalent of a CEO who is ultimately responsible for the information security and agrees the JV's risk appetite.
	JV Information Security Lead Team members	
JV Information Security Lead	• Owns the ISM strategy & its implementation • Advises the Board on ISM risk specific to the JV • Collaborates with the CISOs of the JV partners on a cohesive ISM approach • Works with the JV IT Lead on identifying, evaluating & implementing technical and policy ISM controls for the JV IT infrastructure.	The equivalent of a CISO who manages the JV's day-to-day ISM needs and develops its ISM strategy.
JV IT Lead	• Owns the JV's IT infrastructure • Advises the Board on IT requirements for the JV • Collaborates with the CIOs of the JV partners to determine the most effective & efficient IT infrastructure for the JV • Works with the JV IS Lead on identifying, evaluating & implementing technical and policy ISM controls for the JV IT infrastructure.	The equivalent of a CIO who works with the CISO to provide the necessary IT infrastructure to support JV's IT needs and implements the JV's ISM strategy.
JV Security Controller	• Oversees staff screening (BPSS, SC, etc) • Owns physical security of JV construction sites • Responsible for running of SETA of JV staff • Works with HR on Joiners, Movers, Leavers for JV • Collaborates with the security controllers of the JV partners to develop JV-wide approach.	Each JV partner will have a security controller with similar responsibilities. The JV needs to determine best practice amongst its partners and any gaps that exist as a result of forming a JV.

Information Security Role	Information Security Accountabilities and Responsibilities	Rationale
	JV Information Security Lead Team members	
JV Data Controller	• Ensures JV's compliance with data protection principles • Enables individuals to exercise their rights regarding their personal data • Oversees deployment of appropriate technical and organisational controls to secure personal data • Chooses and contracts suitable data processors • Fulfils the JV's accountability obligations, e.g. carrying out Data Protection Impact Assessments (DPIA), maintaining a record of processing activities (RPA), appointing a Data Protection Officer or Privacy Officer, etc. • Ensures correct handling of any data breaches including notification to the supervisory authority, i.e. Information Commissioner's Office (ICO) in the UK • Collaborates with the Data Controllers of the JV partners to develop JV-wide approach.	The JV is subject to the DPA 2018 and thus needs to have an identified person controlling the JV's data.
JV Data Processors (multiple)	• Ensures correct processing of data according to the instructions of the JV Data Controller • Oversees deployment of appropriate technical and organisational controls to secure personal data • Notifies the data controller of any data breaches without undue delay • Advises the JV's Data Controller when any of their instructions would lead to a breach of the local data protection laws • Fulfils the JV's accountability obligations, e.g. DPIA, RPA, appointing a DPO, etc • Collaborates with the Data Processors of the JV partners to develop JV-wide approach.	The JV is subject to the DPA 2018 and thus needs to have an identified person ensuring the processing of the data is carried out as instructed by the data controller.
JV Data Protection Officer or Privacy Officer	• Assists with monitoring internal compliance • Informs and advises on the JV's data protection obligations • Provides advice regarding DPIAs & RPAs and acts as a contact point for data subjects and the ICO • Collaborates with the DPO or Privacy Officers of the JV partners to develop JV-wide approach.	The JV is subject to the DPA 2018 and thus needs a dedicated resource to inform, advise on data protection as well as monitor compliance. This role may expand to address other legislation with which a JV must comply.

Minimum Requirements for JV Participation

C Minimum Requirements for JV Participation

C.1 Overview:

This appendix lists the minimum requirements to participate in a JV aligned with this guidance.

C.2 Up-to-date Information Security Policies

To ensure that a JV has a solid foundation on which to build its information security posture, all JV members are expected to have up-to-date policies in place covering:

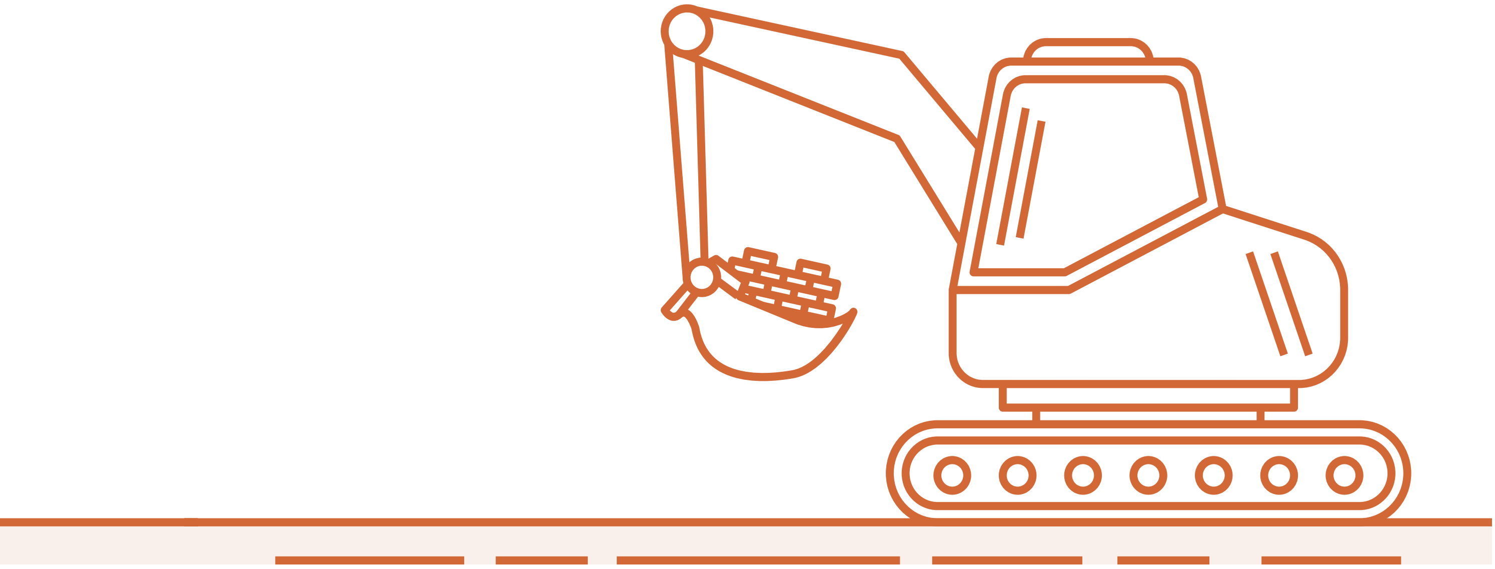
- **Mobile Devices and teleworking** (e.g. remote working, personal devices, etc.);
- **Human resource security** (e.g. clearance requirements, personnel security, joiners, movers, leavers, etc.);
- **Asset management** (e.g. acceptable use, data handling and sharing, removable media, etc.);
- **Access control** (e.g. authentication, multi-factor authentication, authorisation, etc.);
- **Physical & Environmental security** (e.g. CCTV, entry and exit search, clear screen and desk, etc.);
- **Operations security** (e.g. anti-virus, backup, logging, etc.);
- **Communications security** (e.g. network security, email, web browsing, etc.);
- **Incident Management** (e.g. Incident Response, Disaster Recovery, Business Continuity);
- **Legal and Regulatory Compliance** (e.g. DPA, FoIA, etc.);
- **3rd party/supplier management** (e.g. assessing suppliers, data sharing agreements); and
- **Information Risk Management approach** (ISO 19650-5, ISO 27001, NIST CSF, NCSC CAF, etc.).

C.3
Alignment with NCSC – UK Cyber Essentials (not Plus)

Where appropriate, JV partners should aim to achieve Cyber Essentials certification. It should be recognised there may be good reasons why elements of the certification cannot be met; if this is the case the reasons and any equivalent mitigations implemented should be documented. JV partners are not expected to achieve Cyber Essentials Plus.

C.4
Security Education, Training and Awareness

JV partners should have programmes in place to ensure that their staff/contractors have a minimum information security awareness appropriate to their roles and responsibilities. Where appropriate, they must be willing to supplement this training to reflect any JV-specific requirements identified during the development of the JV security plan.



Department for
Business, Energy
& Industrial Strategy

CPNI
Centre for the Protection
of National Infrastructure

National Cyber
Security Centre
a part of GCHQ

Disclaimer: This guide has been prepared in collaboration with BEIS, CPNI and NCSC and is intended to provide information security guidance for Joint Ventures in the contruction sector. This document is provided on an information basis only, and whilst BEIS, CPNI and NCSC have used all reasonable care in producing it, BEIS, CPNI and NCSC provide no warranty as to its accuracy or completeness.

To the fullest extent permitted by law, BEIS, CPNI and NCSC accept no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the guidance or arising from any person acting, refraining from acting, relying upon or otherwise using the guidance. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.