Advice on Information Risk Management for Remotely Piloted Aircraft Systems (RPAS)

June 2015

Disclaimer

This guidance has been jointly produced by CESG and CPNI. CESG are the UK's national technical authority for information assurance. CESG provides advice to the UK Government on security of communications and electronic data. CPNI is the Centre for the Protection of National Infrastructure and provides protective security advice to organisations that make up the national infrastructure.

This guidance is for general information purposes only and for use by the audiences stated above. It is intended to help these audiences make information risk management decisions on the use of remotely piloted aircraft systems. In particular, it is meant to be a resource that assists their thinking when developing and implementing remotely piloted aircraft systems. It is not a substitute for tailored advice. It is not intended to be exhaustive and is subject to some important limitations described in the text. It is provided with no warranty of any form whatsoever whether express or implied. Readers of the guidance must make their own judgement as regards its application to their organisation and seek independent professional advice on their particular circumstances.

To the fullest extent permitted by law, CESG, CPNI and each and every author or contributor to this document excludes all liability for loss or damage caused by an error or omission in this guidance or caused by any person relying on or otherwise using the information contained in the guidance or its references. This exclusion applies however the loss or damage is caused including where it is a result of negligence.

References to any specific commercial product or technology do not indicate that the product or technology is endorsed or recommended by CPNI or CESG.

Executive Summary

The aim of this document is to provide advice on managing the risks to Remotely Piloted Aircraft Systems (RPAS) for civilian use. It does not address the risk from the use of RPAS for either legitimate or illegitimate purposes, by either authorised or unauthorised persons. It only addresses risks to the RPAS platform and the information it collects.

This document has been produced for those who are responsible for managing the risks to an RPAS, including Risk Managers, Security Authorities and Information Assurance (IA) Professionals. It provides specific advice on the operational factors that could shape the technical risks to the RPAS in a range of business scenarios.

The guidance is particularly designed for those developing and implementing RPAS, and those operating large and complex RPAS. It is not designed for casual operators of small, simple, off-the-shelf systems, because although they face some information security risks these should not require complex analysis.

This document does not present actual technical risks, as these will be different for each technical implementation and the role of the RPAS. The risks will need to be assessed for each particular implementation, focusing on the value of the business assets, the threat to those assets and the potential means of compromise.

Different information owners may also have different acceptances of risk, often referred to as their risk appetite, based upon the utilisation of an RPAS or the importance of the information product gained from an RPAS.

This document does not address any airspace provider requirements, such as safety regulations, operating permissions, airworthiness requirements, weight regulations and the crossing of territorial borders.

Version 1.0
Released 03/07/15

Contents

1 Introduction

1. This document aims to provide advice on managing the risks to a Remotely Piloted Aircraft System (RPAS) (sometimes known as an Unmanned Aircraft System, UAS). These systems are often popularly referred to as "drones" but RPAS is the accepted term, determined by the International Civil Aviation Organisation (ICAO).

2. The advice is particularly designed for those developing and implementing RPAS, and those operating large and complex RPAS. It is not designed for casual operators of small, simple, off-the-shelf systems. However, all those developing, implementing or using RPAS should be aware of the guidance issued by ICAO and the UK Civil Aviation Authority[1].

3. This document has been produced for Risk Managers, Information Security Specialists and IA Professionals who are responsible for ensuring that the risks to the RPAS are being managed appropriately. The content provides a top level view of the type of information that should be provided to them and an insight into the operational factors that could shape the technical risks.

4. This document cannot set out the physical security requirements or specify what risks will need to be managed as these will be different for each business scenario and RPAS implementation.

5. This document does not address any airspace provider requirements, such as safety regulations, operating permissions, airworthiness requirements, weight regulations and the crossing of territorial borders. It also does not address the risk from the use of RPAS for either legitimate or illegitimate purposes, by either authorised or unauthorised persons. It only addresses risks to the RPAS platform and the information it collects.

6. Legal requirements for flight, radio frequency allocation, surveillance[2], data protection and privacy requirements, is not covered by this document. References to further guidance about data protection and privacy are provided in Appendix E. Operators of RPAS must be aware of their obligations to the Data Protection Act if personal data is being processed when the RPAS is in use.

7. The key risks to an RPAS are dependent upon the business requirement and the implementation used to meet that requirement. Different information owners may also have different acceptances of risk, often referred to as their risk appetite, based upon the utilisation of an RPAS or the importance of the information product gained from an RPAS.

8. Security is a 'whole life' activity and as RPAS are developed and deployed, further analysis will be required. Those involved should ensure that:

    - A specific risk assessment is conducted for each proposed RPAS solution
    - The risks identified are treated effectively by the proposed design solutions, including operating procedures

[1] As of April 2015, they are the ICAO Manual on Remotely Piloted Aircraft Systems and CAA CAP 722 (6th edition March 2015)

[2] Covered by the Regulation of Investigatory Powers Act 2000

- The risks of specific vulnerabilities introduced by current and future developments are adequately assessed and treated.

9. A critical aspect in the context of managing the risks associated with operating an RPAS is the consideration of airworthiness and how safety and security requirements might conflict if they are not considered in conjunction with each other from an early stage within the design process. Therefore, undertaking a Risk Management exercise early on in the design of a system can be beneficial to a programme from a time, cost and performance perspective.

10. Generic advice will be provided here on the basic requirements of a Risk Management Plan, which will document specific requirements within a programme. These will include clear milestones for security assurance deliverables, acceptance plans, continued review and acceptance into service plans. There is also advice on incident management, maintenance, inspection and audit, decommissioning and disposal.

1.1 Overview of RPAS

11. An RPAS generally comprises several components that make up the system in order to meet the business requirement. The components that an RPAS could comprise include, but are not limited to: the Remotely Piloted Aircraft (RPA), Ground Control Station(s) (GCS), Launch and Recovery facilities, Remote Viewing Facilities (both mobile and fixed), Repair Facilities and a Communications Infrastructure.

12. An RPAS can be a simple aircraft with a camera that is operated in a direct line of sight of a ground controller as currently used by several UK Police Forces and Fire and Rescue Services, through to complex multi-sensor systems that can operate autonomously and provide distributed product. The aircraft can be fixed wing, rotary wing or lighter-than-air platforms. Lighter-than-air platforms often stay around a particular location, as endurance and heavy lift is often the requirement, such as acting as an observation point for a sporting event, and where speed is not the primary goal.

13. The aircraft element of the RPAS can have an endurance ranging from circa 20 minutes through to 48 hours or more.

1.2 Typical Architectures

14. This section provides an overview of typical RPAS architectures, each architecture often building complexity upon the previous one. The architectures do not take into account the particular aircraft family: fixed wing, rotary wing or lighter-than-air, as they can generally be interchanged. Examples are given within each section as to the potential uses of the architecture.

15. It should be noted that the architecture categories defined are not recognised by other agencies, which tend to categorise by weight or endurance. Rather, they have been chosen to assist the reader in understanding the various security risks.

16. The architecture information does not provide implementation details, as these vary between business requirements and manufacturers.

1.2.1 Immediate Vicinity

17. The remote pilot both controls the aircraft and views the received image. The remote pilot uses a handheld remote control to command the aircraft and receives real-time operational images to assist with the tasking. The images are generally presented either on a computer screen or a set of video glasses worn by the remote pilot, for a "pilot's-eye-view". Information gathered by the local remote pilot is forwarded to other users, generally via voice communication links. An overview of the architecture can be seen in Figure 1-1.

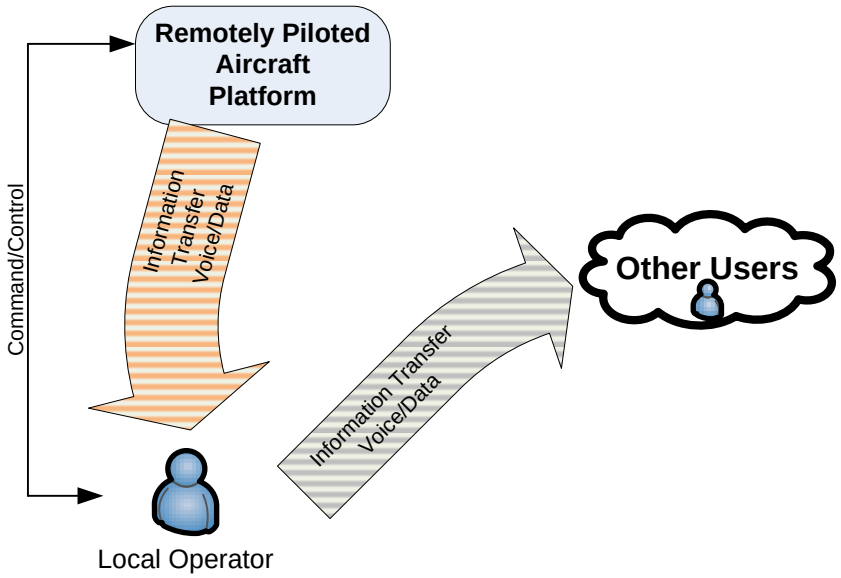

Figure 1-1 Immediate Vicinity of Operator

18. UK Police Forces and Fire and Rescue Services are currently using this system, which is usually fitted with either Electro-Optic and/or Infra-Red sensors. The Police Forces typically use this system to assist in law enforcement, such as locating people at night with the infra-red system; Fire and Rescue Services typically use these systems to check the structural integrity of buildings after incidents and to check for heat sources, such as in roof voids. In both cases, the remote pilot controls the aircraft, observes the received imagery and then directs other personnel based on the received information.

19. The aircraft used are often rotary wing although they can be hand thrown. They are generally low weight; the civil aircraft category is Small Unmanned Aircraft (0-20Kgs). The flight times are circa 20 minutes.

1.2.2 Local Control

20. These aircraft take off either via an airstrip, are launched by a rail mechanism or are rotary wing, which is useful for maritime operations where Vertical Take-off and Landing (VTOL) for launch and recovery on-board ship is advantageous.

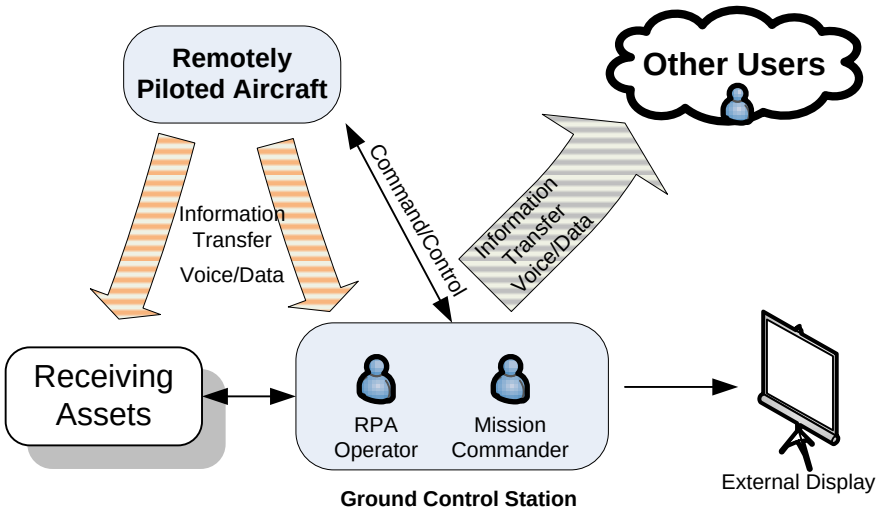

Figure 1-2: Locally Controlled RPA

21. The aircraft is launched, recovered and operated from a single Ground Control Station (GCS). As can be seen in Figure 1-2, the GCS generally has at least one remote pilot and one GCS commander, although there can be other personnel present such as a payload operator and image analyst. Command and Control information is passed between the GCS and the aircraft. The aircraft transmits imagery data to both the GCS and any other assets capable of receiving the data, such as a Remote Viewing Terminal (RVT). The RVT operator cannot directly control the aircraft but will generally communicate with the GCS via other means. Certain configurations of GCS can forward received imagery, in the form of video feeds, for display on external equipment. The GCS also has communications to other resources, such as other users, tasking authorities and Air Traffic Control (ATC).

22. Proposed uses for this include policing strategies, where an aircraft could fly over areas that would otherwise be expensive or difficult to police, looking for suspicious behaviour. For example, border agencies have trialled RPAS for border patrol, such as the Austrian/Slovakian border, the USA/Canadian border and patrolling the sea off Gran Canarias. During the Euro 2008 football tournament, an RPAS was used by Zurich Police to mount surveillance operations around the stadiums and to monitor restricted areas and tunnels.

23. Within the UK, RPAS tend to be used by the military community and are generally considered to be tactical in nature, having a weight between 20Kg and 150Kg; the civil aircraft category is Light aircraft (20-150Kgs). Flight times vary from manufacturer to manufacturer; the role of the aircraft and payload weights can allow an endurance of over 20 hours.

1.2.3 Distributed Operation

24. The aircraft used within a distributed operation can be the same aircraft as those used under Local Control, the only difference being that the Launch and Recovery location can be separate from the operational environment and the controlling GCSs can hand control over between each other, see Figure 1-3. Typical use would be where the RPA is launched from an airstrip, by the Launch and Recovery (L&R) GCS, and is then flown to the operational area, where the aircraft control is handed over to a Control GCS. This allows the L&R GCS to concentrate on the launch and recovery activity, whilst the Control GCS can concentrate on the business objective.

25. This also allows for the use of the RPA Beyond Radio Line Of Sight (BRLOS) from the L&R site and other GCS elements.

26. Well defined processes and procedures need to be in place to allow for a safe and successful handover of the aircraft between the various GCSs. This will generally require a form of communications between the GCSs elements, as well as general communications to other users.

27. Typical uses for distributed operations would again include operations such as patrolling borders, where there is a requirement to maintain an extended capability, beyond the range of a single GCS.

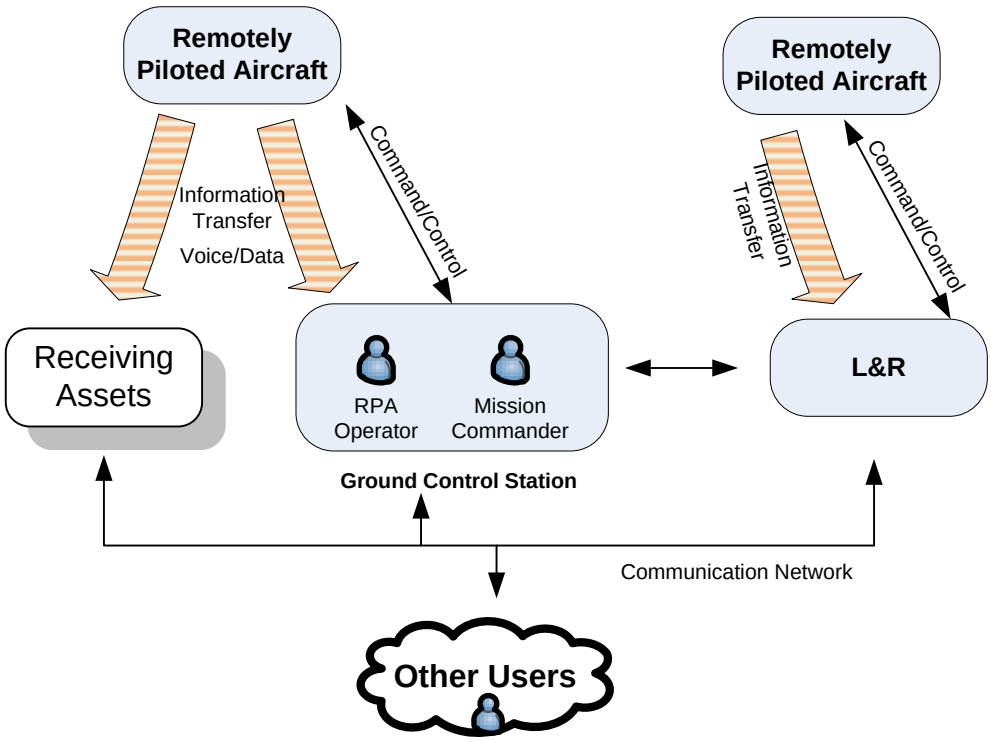

Figure 1-3: Distributed RPAS

1.2.4 Wide Area Distribution Operation

28. Wide Area Distributed Operation is essentially an extension of a Distributed RPAS, with the additional business requirement to extend the viewing capability to external observers; this can be seen in Figure 1-4.

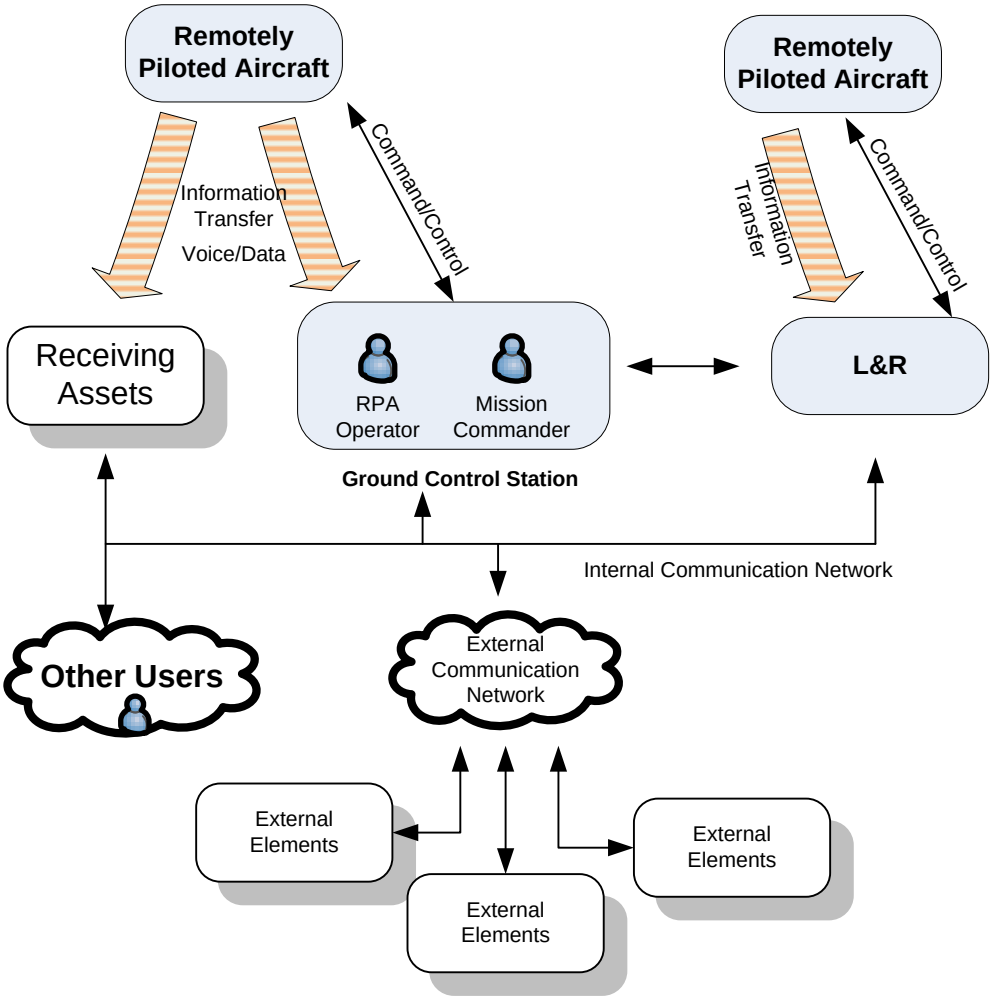

Figure 1-4: Wide Area Distributed RPAS

29. The wide area distributed system essentially allows access to the RPAS product for other customers, in order to meet their requirements. This method of product dissemination has been successfully demonstrated by various border agencies and has provided situational awareness during critical infrastructure assessments and emergency response situations, such as US Coast Guard maritime search and rescue operations streaming infrared imagery to multiple customers.

1.3 Communications and Data Transfer

30. There are potentially many different forms of communications between the components that make up an RPAS configuration. Typical communications between the RPAS elements include, but are not limited to the following:

31. GCS to aircraft – This can be both Line Of Sight (LOS) and Beyond Radio Line Of Sight (BRLOS) and relates to Command and Control, both to and from the aircraft, and the sensor data generated by the aircraft. BRLOS communications can be provided by either satellite communications link or by rebroadcast between RPAs. That is, a GCS communicates with an aircraft which is in its line of sight, which in turn relays information on to another RPA, which is out of the line of sight of the GCS but within the line of sight of the transmitting aircraft. When using BRLOS communications, latency might become an issue and should be considered.

32. RPAS Operators to Air Traffic Control (ATC) – There will be a requirement to communicate to ATC, possibly via the aircraft. Future Airspace Structure may bring in an alternative Data Link direct between remote pilot and ATC, but this concept is in its infancy.

33. RPAS Users to Other Users – These external communications are dependent upon the business information exchange requirements to directly allow the RPAS to perform its tasking. Typical examples will be:

    - voice, via existing radio communications infrastructures, to direct other assets

    - data, via existing data networks, to pass tasking to the RPAS assets and distribute intelligence information gathered by RPAS assets

34. External Communications – These communications are distinct from the communications that are required to allow the RPAS to perform its business function. The object of the external communications is to allow external elements to have access to the RPAS product. A typical example of this would be the distribution of the product to external organisations via the internet.

35. Removable Memory (RPA) – Some of the aircraft will carry storage to allow a user to capture information during flight for downloading after landing. A typical example of this is the immediate vicinity RPAS architecture, where the bandwidth between the aircraft and the ground station may be limited. Therefore, lower quality images are presented to the user for immediate situational awareness and the remote flight crew has the ability to capture and store higher definition images direct to the aircraft, for later analysis. Another example could be Flight Data Recorders.

36. Removable Memory (Ground Assets) – Ground assets will often store the aircraft sensor data and exploited information, due to its ability to store larger amounts of data. This can include the raw sensor data, often called primary imagery, and the processed data, often called secondary imagery.

37. It is worth noting that the information required by an end user is not necessarily Full Motion Video (FMV). What might be required is the correct information extracted from the FMV, in the correct place at the required time, thus allowing for timely action and decision making.

1.4 Other Considerations

38. Other considerations for the implementations of RPAS architectures that are worth noting to assist with the overall understanding of the security requirements are:

39. Contingency Actions – Consideration will be required from a system perspective on what actions should be taken upon: loss of the control link, loss of voice links, loss of data links (i.e. imagery), mechanical failure, emergency landing, aborted landing and adverse weather conditions.

40. Whether there is a requirement to operate with other agencies, where there are standards that should be observed to allow interoperability.

41. Education and training – All aspects of the RPAS operation will require training; this should include all relevant aspects of security and be cognisant of potential skill fade.

42. Maintenance Activities – Maintenance and logistic support are important in maintaining the capability of the RPAS and may include a redundancy scheme with either immediate (hot) or timely spares. It is worth noting that RPAS can be procured as a managed service, as opposed to owning the system outright.

2 Risk Management Approach

43. This section provides guidance on the type of information that should be produced for risk managers to support the business decision to use an RPAS. This information should be gathered together into a Risk Management Plan.

2.1 Business Context of the RPAS

44. The business context of the RPAS needs to be fully defined by the business owner as this will set the context for the risk management approach. It is recommended that information on the following should be available (although this list is not exhaustive and not all suggestions will be appropriate to every RPAS requirement).

45. The RPAS owner and the data owner of information provided and analysed by the RPAS.

46. RPAS capability such as: timely intelligence, surveillance and reconnaissance, all weather requirements, day and/or night operations, system endurance (aircraft and Ground Services), transit times, on-task times, situational awareness and survivability.

47. Basic technical information might also be included, if considered appropriate. Examples of this could be whether Full Motion Video is “lossless”, or has any pre-processing or post-processing been applied, such as compression. This might need to be considered if a stored RPAS video feed needed to be of evidential quality, to allow it to be used within a court of law. This would need to be considered from the perspective of the aircraft (the sensor and any pre-processing prior to transmission), to include analysis that might be carried out on an image and how the images are stored.

48. A brief description of any third parties and their roles, their interactions and any dependencies and requirements on either party. Examples of these could be training, maintenance and digital storage providers.

49. Archive, backup, disaster recovery and business continuity requirements might also be mentioned and how these will be achieved. For example where products will be archived, how often and where the system will be backed up and the maximum time an RPAS can be out of service.

50. Dates: In service, out of service, provisional or known upgrade dates of the RPAS.

51. If the requirement is for an upgrade, what is the reason for the upgrade? Typical examples could be improved performance or efficiency.

52. The tasking and implementation of an RPAS depends upon the system’s requirement. This can range from intelligence and information gathering from the RPA sensors to freight transportation and acting as communication relays. Multiple tasks could be undertaken, such as acting as a communications relay whilst undertaking a transport task. The requirements and processes will often require timely and accurate tolerances, such as the business requirement for the time taken to disseminate information or, from a safety perspective, the position of an aircraft.

53. This generic approach will concentrate on information gathering and onward communication, as this will encompass the majority of potential scenarios that an RPAS may encounter. Scenario elements will include:

54. Organisational and shared ownership of the RPAS and the information produced.

55. High-level business objectives of the RPAS, such as: provide sensor data from an area of interest in a timely manner to a ground station in a secure manner.

56. Business functions within the RPAS, such as: capture sensor data and carry out initial pre-processing on-board the aircraft and then securely transmit the data to a ground element, for further analysis. This highlights how processing sensor data can be local within the aircraft and remote to the GCS, such as enhanced non-real time processing. All scenarios need to be captured and addressed.

57. Information processes within the RPAS, such as the tasking of the RPAS, command and control of the aircraft and communications to remote users. This highlights that it is not only the sensor data and processed information that needs to be managed, but also includes other communications, such as mission tasking, communications to remote users and onward connections to either other users or other systems.

2.2 RPAS Users

58. The users within an RPAS and the recipients of RPAS information can have different requirements. The remote flight crew, for example, the controllers of the aircraft, sensor payload and initial image analysts might have higher security clearance requirements than the end users. An example of this could be during disaster recovery whereby the end user requirement may be to advise on or predict the boundaries of a flooded area and relay this information to emergency services on the ground. The information might also be supplied to provide timely media coverage and there may therefore be a requirement to “sanitise” the information, prior to its release to the media.

2.3 Interconnections and Interfaces

59. High level examples provided in Section 1.3 show how the various elements of an RPAS could communicate with each other and with external parties. This not only includes the end recipients of the information but also the communications bearers, which would have access to the RPAS information and how the various interconnections and interfaces would need to be managed. For example, an RPAS might have the requirement to be able to concurrently communicate secure voice to other air assets or users, whilst also communicating in clear voice to air traffic services.

60. The various information exchange requirements and their security requirements should, where possible, be determined prior to deployment. This will help to facilitate the business requirements for communications in an efficient manner and should describe each external connection. Tables and/or diagrams are recommended to assist in this and the information may include: ownership, business need, data flows, technical details, sensitivities and the status of the connecting systems.

2.4 Risk Ownership

61. This will generally depend on the leading operating authority, the data owners and the operating environment. The operating authority could range from a commercial organisation, to a fire and rescue authority, a local law enforcement authority or a border agency.

62. However, because the RPAS is a collection of information in various forms and possibly locations, such as real time primary sensor data, processed secondary data, forwarded data, third party data and stored data, then the data owners might belong to different business organisations.

63. Therefore, the data, in its entirety, might not belong exclusively to one organisation. Examples of this could be if the data analysis in the RPAS could also undertake analysis of third party data during aircraft down time, or other parties might use the aircraft of the RPAS as a communications bearer to extend the range of communications coverage.

64. Establishing and maintaining a framework to share services securely is critical and there are a number of potential routes to achieving this:

    - By the Lead Organisation
    - Shared across all using organisations
    - Shared within a subset of subscribing organisations

65. It should be noted that the final responsibility for the proper safeguarding of the information and risk acceptance has to remain with the organisations whose information is being processed. As such, none of the subscribing organisations can be totally isolated from the governance procedures.

66. If an RPAS is deployed in support of other operations, such as a border agency RPAS being utilised for search and rescue, then the risk ownership could pass from the border agency to the search and rescue agency.

2.5 Shared Service Assessment (if applicable)

67. If the RPAS is using a shared service, there should be an assessment of the security status of the system that is hosting the service. Also a description of the service needs to be documented and some form of shared service agreement drawn up and formally signed up to. It should include the service offering, service relationships and information risk management statements. Examples of shared services within an RPAS context are:

    - Utilising the same communications bearer as other assets, such as police voice communications networks
    - Utilising shared data storage facilities with other organisations
    - Utilising third party data communications to transfer information between locations, such as Full Motion Video (FMV) or intelligence reports

2.6 Roles, Responsibilities and Functions

68. Establishing an effective governance process is critical to good risk management. The governance framework should encompass the full lifecycle of the RPAS with brief descriptions of key responsibilities and posts to which these functions are assigned, detailing references to corporate policy as applicable. These should include ownership, policy, compliance and asset management and should be linked to the appropriate Security Operating Procedures.

69. These functions may change, particularly on transfer from a project development environment to an in-service system, so it is critical to ensure a transition to operation plan is produced to ensure that the transfer of security responsibilities is carried over.

2.7 Risk Appetite and Tolerance

70. The organisation's risk appetite determines its approach to business activities and the type of risk it is happy to manage and accept for its various business operations. Where an organisation is looking to operate an RPAS it should determine how this aligns with its risk appetite to help determine the type and nature of the security controls that need to be put into place and the overall level of assurance that is required.

71. Risk tolerance for the RPAS business activity needs to be documented and agreed by all parties, but this will largely be determined by the RPAS utilisation. For example, a risk owner might be willing to accept higher risks for a civilian RPAS used for Search and Rescue operations and possibly local law enforcement. However, risk owners (and their Security Authority) might only be willing to accept lower risks for serious crime and National Policing, such as border patrols.

72. Risk tolerance is closely related to risk appetite[3] and allows for variations in the amount of risk an organisation is prepared to tolerate for a particular activity. The initial risk tolerance can be reconsidered when there is an improved understanding of RPAS deployment, or when the circumstances of deployment change.

[3] Appetite applies to an organisation overall

3 Risk Management Activities

3.1 Security Risks Consideration

73. This will be dependent upon the business activity of the RPAS and should include a clear statement on the potential impact to the business in terms of financial, legal, reputation, integrity, etc. should the risks that have been identified be realised. If the RPAS is the primary source of real-time imagery for a sports event, with no redundancy, then there might be financial penalties, as well as a loss to the reputation of the RPAS supplier. If the RPAS were to be used to provide real-time imagery to a border agency and the imagery were to be compromised, then there might be legal implications.

74. The corporate value should consider Confidentiality, Integrity and Availability. Typical examples for an RPAS would be:

    - Confidentiality: The sensor data being transmitted from the aircraft to the ground components and stored data within the RPAS

    - Integrity: The accuracy of the commands and information sent and stored within the RPAS

    - Availability: The loss of the command and control link between ground control elements and an aircraft or the reception of imagery.

3.2 Privacy Impact Assessment (PIA)

75. The Information Commissioner's Office recommends that data controllers conduct a Privacy Impact Assessment (PIA) in order to check compliance with the principles of the Data Protection Act. More broadly, PIAs enable privacy intrusion and compliance with Article 8 of the European Convention on Human Rights (a right to respect for one's private and family life, his home and his correspondence) to be addressed. PIAs should establish the justification for using RPAS to process personal data and then review how the data is processed. This should include security and retention of personal data and methods for informing individuals that recording is taking place. . For example, if an RPAS was being used to monitor crowd behaviour at a stadium, the likelihood and justification for recording images of individuals in nearby gardens should be assessed and appropriate safeguards should be applied. Ideally, a PIA should be conducted at the start of a project and then be updated when there are changes or new insights. If a PIA has been conducted for an RPAS, reference the resulting report, related documentation and top-level summary within the RPAS Risk Management Plan.

76. The outcome of the PIA could for example affect the clearance requirements for the remote flight crew, or the method of onward transmission of the RPAS product, such as real time Full Motion Video. The outcome may also affect requirements for any media that stores information, including the handling requirements, and subsequently the requirements for appropriate sanitisation for disposal or reuse.

3.3 Threat Assessment

77. A threat assessment that is specific to the RPAS, its business requirement and its area of operation should be provided.

3.4 Risk Assessment

78. Risk assessment is the overall process of risk analysis and evaluation. The organisation should determine the most appropriate risk assessment methodology for the business.

79. The top-level outcomes of the risk assessment should be presented to the risk owners in a form which is easily understood and include the risks to any personal or sensitive information. The components of the risk assessment can change over time and the role or implementation of the RPAS may also change so the assessment will need to be periodically reviewed to ensure it is accurate. The full RPAS risk assessment should be retained for future reference.

3.5 Risk Register

80. A risk register is used to capture the outcome of the risk assessment process as a prioritised list of risks, including any privacy risks. When a risk treatment plan is agreed, the risk register should also include the residual risks.

81. The risk register is also used to track, support and justify risk management decisions that are made during the lifecycle of the RPAS.

82. If the RPAS shares or subscribes to a shared service, it may be useful to produce a joint risk register. For example, if an RPAS was being utilised to provide a new capability to a border patrol agency, then there might be a joint risk regarding joint communications bearers. That is, if the communications were prone to compromise or jamming, then this would be a risk to both parties, until the risk was mitigated, such as by a technical solution being implemented, or the risk is managed by some other non-technical means, such as the use of call signs and code words.

3.6 Risk Treatment Plan

83. Once decisions have been taken on which risks need to be treated, a Risk Treatment Plan will be needed to document and track the delivery of risk treatment controls. The reduction of a risk may involve a combination of processes and the risk assessment may need to be reviewed or repeated before the level of residual risk is acceptable to the business. A combination of Physical, Procedural, Personnel and Technical protective controls will often be required.

84. Some example security controls have been provided in Appendix C. They are broadly aligned with the ISO/IEC 27001 control headings. Differing RPAS implementations will need to tailor security controls differently.

85. The content of the risk register will provide much of the input into the risk treatment plan. For new RPAS systems and services the activities and requirements in the risk treatment plan should

be aligned with the main project plan, as the delivery of protective controls may need to be integrated into different project work streams and assurance gained on their security functionality at different stages of the project.

86. When the system is in service, the Risk Treatment Plan will need to come under management change control procedures.

87. There may come a point in the risk treatment cycle where there are no protective controls for a risk or those that are available cannot reduce the risk to a manageable level. If this occurs then this should be documented (in a Residual Risk Statement), escalation procedures should be instigated and advice sought from the senior manager responsible for risk.

4 RPAS Lifecycle Risk Management

4.1 Development and In-Service Activities

88. During the development and acceptance stage of an RPAS the Risk Management Plan should set out clear milestones for the security assurance deliverables, linked to the main project or development milestones. On entry of the RPAS into service, the development and acceptance plan should be archived.

89. Before acceptance, a new plan should be developed to meet the requirements for information risk management in-service. This could include different business requirements for the RPAS that could lead to a change to the RPAS risks, such as moving from a search and rescue role to a police enforcement role, or a change in supplier support. For example, a contractor might change a sub-contractor that provides them with support; this might have a bearing on the confidentiality requirements of information or the timeliness of support, affecting business continuity and RPAS availability.

90. In the case of complex assets, a separate schedule for verification, inspection and/or testing may be undertaken, as a sub-set of the Risk Management Plan.

91. Plans should always include: configuration control of assets, configuration control, requirements reviews, verification, validation requirements, provision of training and awareness, indication of personnel responsible for actions.

4.2 Results of Security Assurance Activities

92. This section of the Risk Management Plan should summarise the outcomes of security assurance verification, testing and physical inspections, referring to individual reports for details as appropriate. Highlighting any major issues and where these relate to non-compliance against the Corporate or National policies or the security assurance requirement, then an exception report must be raised, the risk register updated and an owner appointed to manage these security issues.

4.3 Security Operating Procedures

93. Security Operating Procedures (SyOPs) should be produced for all users of the RPAS system or service. SyOPs will support the procedural measures identified as protective controls in the RPAS Risk Management Plan.

94. All users should formally acknowledge their security responsibilities through an accountable corporate process, such as by signing a copy of the SyOPs or an Acceptable Use Policy. The relevant SyOPs should be made available in all work areas for staff to refer to and brought to the attention of staff as part of their annual refresher training.

95. SyOPs must be reviewed regularly to ensure they remain applicable and relevant.

96. The SyOPs documents are generally individual documents. However, SyOPs may be embedded within documents covering the management, operation, and use of the RPAS and its ICT systems

and services. These may include detailed technical documents, corporate standards documents and User Guides for various groups of end-users. For example, for a simple RPAS, such as a single user for law enforcement in the immediate vicinity of the aircraft, then the SyOPs might be located within the RPAS Risk Management Plan. Otherwise, it will probably be easier to produce and maintain the SyOPs as a separate set of documents.

97. As a minimum confirm that the required SyOPs:

    - exist for all roles that enable the live running of the RPAS systems or services
    - have been issued to the appropriate audiences
    - have been read and understood and where appropriate, asset management staff and users have signed to confirm acceptance of the conditions
    - are monitored in operation and subject to regular review
    - are maintained under formal change control arrangements which include the requirement to consult the Security Authority about significant change proposals

98. If SyOPs are located in several areas, a list of all documents that contain SyOPs should be produced and, for each, provide:

    - document title, reference, version and date
    - ownership and responsibility for management of the document
    - distribution of the document
    - an outline of the SyOPs content of the document

99. The RPAS Risk Management Plan should highlight key security issues and summarise how these are addressed by relevant SyOPs.

100. It should be noted that some SyOPs documents will include information about security arrangements that could be of help to a would-be attacker. Therefore SyOPs should be appropriately protectively marked, distribution limited and should have appropriate storage and destruction controls in place.

4.4 Incident Response Plan

101. An Incident Management policy and coherent incident management procedures must form part of the Risk Management Plan and be supported by standards and procedures. All users must be made aware of the procedures and their role in the event of an incident.

102. The arrangements for incident management, reporting procedures and response requirements should be articulated. These may be available in a corporate policy, in which case refer out to the relevant document and section.

103. Specific instructions should be provided for foreseeable problems to an RPAS (such as power outage, malicious software infection, loss of media items, hardware or link failure) with details of individuals/posts/functions in the organisation who should be contacted for help.

104. These procedures might link into other emergency response planning, such as the loss of an aircraft over a populated area.

105. References should be provided to locations for Business Continuity Plan, Disaster Recovery Plan and Forensic Readiness plans.

106. The Business Continuity Plan will aim to keep the most essential business processes running, as far as possible, throughout the incident. The Disaster Recovery Plan will aim to recover the RPAS business by replacing assets, which have been damaged or lost as a result of an incident. This could be achieved by having spare RPAS assets available at remote locations. A Forensic Readiness policy and supporting standards, guidelines and procedures must be in place to maximise the ability to preserve and analyse data generated by the RPAS ICT systems or services that may be required for legal and management purposes.

107. All plans must be regularly reviewed and tested to ensure they are fit for purpose.

4.5 Assurance Maintenance Plan

108. The assurance maintenance plan should detail how assurance gained in any aspect of the RPAS system or service will be retained throughout the system lifecycle.

109. The plan should address how product updates will be assessed, providing advice on categorising likely changes into security risk categories and how the various categories will be tested, for example changing RPAS component suppliers or changing the RPAS architecture where security assurance functionality is present. Typical aspects that should be covered:

- Security documentation management and maintenance
- Maintenance schedule and review procedures for assured components and (as appropriate) the information system. This includes both hardware and software reviews
- Vulnerability awareness and patch management
- Change procedures
- Test and validation strategy
- Possibly TEMPEST[4] reviews, specifically for systems operating at a threat level assessed to be Medium, or above, and after system changes that could alter the TEMPEST performance and profile of the RPAS.

[4] Spying on information systems through leaking emanations, which include unintentional radio or electrical signals, sounds, and vibrations.

4.6 Inspection and Audit Records

110. The date, assurance activities and outcomes of ad-hoc and scheduled RPAS security audits and security inspections of the RPAS should be documented.

111. Any formal reports that are produced should also be referenced.

4.7 Decommissioning and Disposal

112. As with many systems, there are a number of aspects to consider when dealing with the secure decommissioning and disposal of an RPAS and connected ICT systems. These typically include:

- Asset recovery
- Contract closure
- The secure disposal of storage media and solid state components used during the lifecycle of the RPAS, including where RPAS information was stored by a third party
- The decommissioning and disposal of the RPAS at the end of the lifecycle
- Security staff and user debriefing

113. When new systems and services are being delivered to replace legacy ones, it is imperative that the requirement to decommission the legacy RPAS securely is not forgotten.

114. Availability and integrity requirements in respect of information stored on an RPAS or an ICT system could persist for legal, regulatory or corporate reasons. Assurance that the data can continue to be accessed when required (availability) and will remain unchanged (integrity) may be necessary. In addition to considering the longevity of the media, availability of suitable hardware and software to read that media and the information thereon has to be considered.

115. Where an RPAS system is processing information that is required for maintaining accounting and audit records, these should be retained for a period specified in the SyOPs.

116. Confidentiality requirements must be considered, if an associated RPAS system has been processing classified, personal or sensitive information which attract special handling requirements. The system components will require sanitisation or certified destruction by approved products or processes.

117. If the RPAS contains sensitive security components, such as cryptographic items, then these components will need to be dealt with in an appropriate manner. This might include returning them to an equipment originator, storing appropriately for future use or destroying when applicable and by appropriate and approved products and processes.

118. Even if there are no apparent sensitivities, organisations should consider purging RPAS systems before disposal or transfer to prevent the accidental release of classified, personal or sensitive information into the public domain.

119. In the case of an ICT system with interconnections, notice of decommissioning should be issued to all data exchange partners and formal assurances obtained that data has been purged where appropriate and that all access rights between remote systems have been removed.

120. Once all security relevant activities associated with decommissioning and disposal have been completed and verified, the Security Authority may issue a Decommissioning Certificate.

5 Typical RPAS Risk Model

5.1 Risk Management Process

121. Figure 5-1 shows a typical model that could have been produced for use in a risk assessment. The model tries to capture the majority of potential business objects/assets and connections/interfaces and as such is generic and should be used for guidance only.

122. RPAS systems might be developed and deployed in isolation but they often interact with other systems outside of the scope of the project. The interaction may be to deliver information or data to an outside system, or it may be that the RPAS relies on an outside system in some part of its overall operation. A risk assessment may therefore involve consideration of facilities and services that have been, or need to be, assured by another organisation.

123. Critically, if the RPAS is handling personal or sensitive information the risks to that information must be considered as part of the overall assessment, so risks are appropriately identified and controls put in place that satisfy any legal or regulatory requirements.

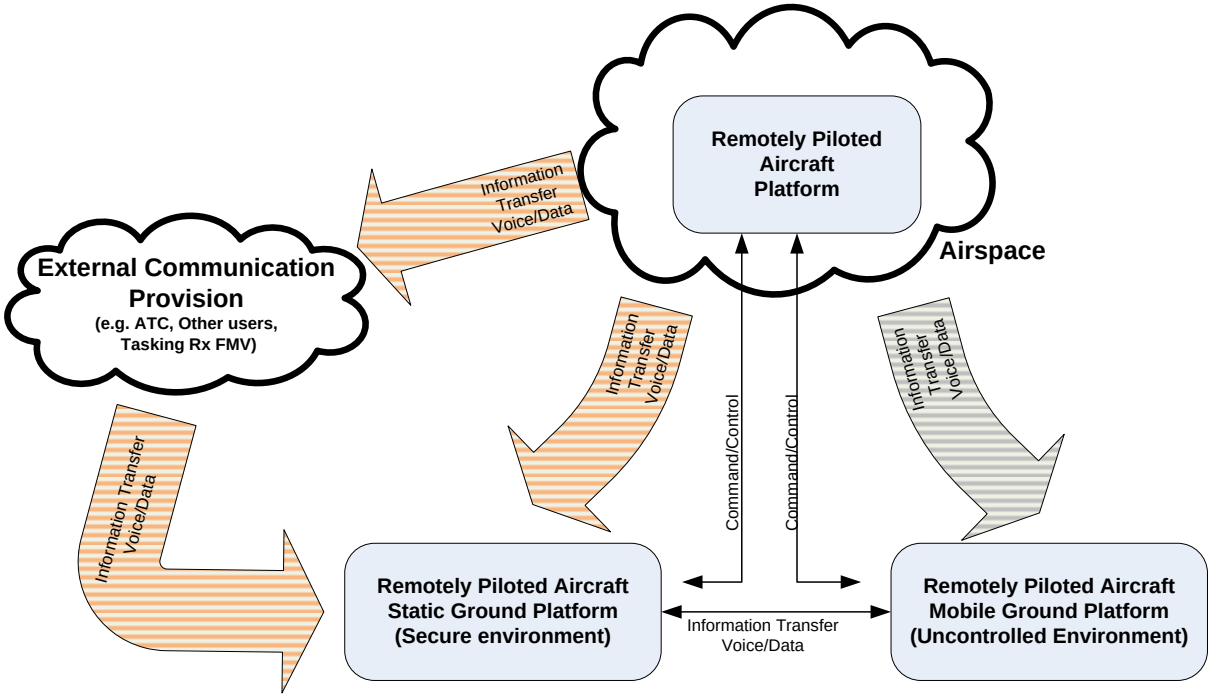

Figure 5-1: Simplified Generic RPAS Model

124. The business components depicted in Figure 5-1 should be considered during the assurance activities. The “Internal RPAS Command/Control facilities” are within the assurance process, as these communications are specific to the RPAS. The “External Communications Provision” forms an important component, as the RPAS will need to make use of these facilities to allow the RPAS to conduct business with external third parties, but is outside the assurance process. The external systems are outside the assurance process as the systems either already exist or are being provisioned under a separate project.

125. External communications could possibly be subject to their own assurance processes and there may be subsequent requirements for external systems to connect. These connections should be fully documented as Information Exchange Requirements (IER) and Code of Connection (CoCo) agreements should be in place where appropriate.

126. The business objects that are not included in the assurance activities are essentially entities that the RPAS needs to communicate with to enable it to conduct its business but which are not controlled by the RPAS operator. However, there might be dependencies or assumptions placed on these objects. An example of which might be that a business object will handle the RPAS data appropriate to the data's classification. When required, these objects can be placed in the assurance activities.

127. The RPAS system is shown as three elements:

- RPAS Static Ground Element

This encompasses all static ground objects, such as: Ground Control Stations, Launch and Recovery vehicles, maintenance facilities and communications facilities. In this example, this also includes the aircraft element of the RPAS, when it is not flying.

The physical location for this object is assumed to be in a controlled environment. That is, the RPAS operating authority has confidence that access to the ground elements is controlled; such as on an aerodrome, a military airfield or in a disaster support Headquarters.

An example of potential attack:

In order to ascertain the flight plan of an aircraft, an attacker might attempt to intercept tasking requests from an external agency via an Internet link. An alternative could be attempting to intercept, and possibly decrypt, the command and control link to an aircraft.

- RPAS Airborne Element

This is the aircraft element of an RPAS, when it is flying.

The physical location for this object is airspace. This could be either the area of interest for the mission, the airspace used to transit between the Launch and Recovery and the Area of Interest or an area of airspace that the aircraft is loitering in whilst waiting for an instruction. The airspace will also include the airspace that the RPAS will utilise in the event of a failure, such as a lost link procedure used in a communications failure or where the aircraft will head in the event of a catastrophic event, such as engine failure.

Examples of aspects that might need to be considered within the risk modelling would be:

What would be the outcome of an aircraft crash, such as a potential loss of life?

Would people be interested in the content of the sensor data link?

An example of potential attack:

In order to carry out a Denial of Service attack on an RPAS, an attacker might attempt to jam the Command and Control signals to an aircraft from an RPAS Ground element.

- RPAS Mobile Ground Element

  This encompasses any mobile ground elements of the RPAS. In the corporate model shown in Figure 5-1 this includes elements such as Remote Viewing Terminals, as there are communications from the aircraft and with the Static Ground Element. However, depending on the perceived threats to the RPAS, the risk model could also include other mobile elements, such as supply vehicles.

  The physical location of this object is assumed to be in an uncontrolled environment. That is, the RPAS operating authority generally needs to provide the physical protection for the RPAS. Examples could be a Remote Viewing Terminal, mobile platforms with receive capabilities, such as in convoy operations or mobile command vehicles, or other emergency services, such as relayed imagery to emergency rescue services.

  An example of potential attack:

  In order to gain access to real time sensor data, and compromise the confidentiality of the RPAS, an attacker might attempt to steal or capture a Remote Viewing Terminal.

128. The model shows that the various elements can communicate with each other. The communications that the RPAS utilises can be either part of the RPAS or externally provided. For example, the RPAS Ground (Static) object can communicate to the RPAS Ground (Mobile) object by either “Internal RPAS Command/Control Facilities” or via “External Communications Provision”. The “Internal RPAS Command/control Facilities” would be specific communications bearers as part of the RPAS architecture, such as dedicated radios that are provided as part of the RPAS or its own Local Area Networks (LAN). The “External Communications Provision”, would be third party bearers, such as other emergency services’ radios, mobile telephony services, satellites or external LAN.

129. One-way communications for the imagery generated from the aircraft are also shown on the model. This does not necessarily need to be a separate communications bearer from the other communications, but is shown to highlight the fact that not all receiving elements might need access to the RPA data. For example, Air Traffic Control would only need voice communications relayed by the aircraft. However, other airspace users might need other information such as sensor data, as well as the voice communications relayed from the RPA.

130. The model also shows how recipients of the communications can receive data from either the internal or external communications, an example of this is shown by the Air Traffic Control (ATC) object. ATC can receive voice and data communications from either the RPA (Airborne), via Internal RPAS Communications Facilities, or from RPAS Ground (Static), via either Internal RPAS Command/Control Facilities or External Communications Provision. The voice could be immediate air tasking and the data could be pre-flight planning information.

5.1.1 Example RPAS Objects

131. The asset list for the operational RPAS example is in Table 5-1: Catalogue of Generic RPAS Objects and Descriptions below.

Business Object	Description
RPAS Static Ground Element	Encompasses all RPAS elements, such as: Ground Control Stations, Launch and Recovery sites, Remote Viewing Terminals, provision within other static locations (such as Headquarters), maintenance facilities and the aircraft when on the ground.
RPAS Mobile Ground Element	The mobile RPAS components that are not within the RPAS Ground (Static) environment, such as: Remote Viewing Terminals
RPAS Airborne Element	The aircraft element of the RPAS. This could be immediately post launch from a Launch and Recovery site, the aircraft transiting to or from a Launch and Recovery site and the tasking site or airborne on task over an area of interest.
C^2 Connection	Command and Control (C^2) between RPAS Ground elements that can control an aircraft (such as a Launch and Recovery facility or a Ground Control Station) and the aircraft. This can include the command and control of: the flight path of an aircraft, the sensor payload, on-board radio communications settings, Identification Friend or Foe (IFF), GPS and other navigation equipment. Emergency commands, such as dump gas on a lighter-than-air aircraft, would also be communicated between the ground objects and the aircraft. However, emergency commands might be conducted on a separate or redundant communications path.
Sensor Data	This is either the raw sensor data from the RPAS or processed data that is being relayed by the RPAS. This could also include sensor data that has had pre-processing on the aircraft, prior to being transmitted to the ground elements.
Voice/Data	Represents the voice and data communications that could be possible within the RPAS between its connected objects.
Internal RPAS Communications Facilities	Represents all communication facilities that are provided by the RPAS. This could include: The Command and Control links between the RPAS ground objects capable of controlling an aircraft and the aircraft itself, dedicated LAN within the RPAS architecture, RPAS provisioned radios (such as V/UHF radios for communications to ATC providers) and any internal intercommunications systems within the RPAS.
External Communications Provision	Represents communications external to the RPAS that the RPAS relies upon to conduct its business, such as to receive tasking orders from external agencies and relaying FMV to third parties via an external LAN or the internet.
Controlled Area	Represents the locations where various RPAS ground elements may operate. When required by the RPAS role, access to these elements will be in a controlled manner, appropriate to the RPAS application and employment. Examples range from access control within an aerodrome through to armed guards within a military compound.

Uncontrolled Area	Represents the locations where various RPAS ground elements may operate. These RPAS ground elements will operate in areas where control cannot always be guaranteed, such as access control, oversight by third parties of imagery and in prone to loss or capture areas.
Operating environment	Represents the locations where the RPA will operate. From a security perspective, this can be either a controlled environment or an uncontrolled environment. Within a controlled environment it is assumed that there is a realistic assumption that the RPAS operating authority could secure the aircraft if it landed, either intentionally or otherwise. In an uncontrolled environment, it is assumed that the aircraft could be difficult to secure if it were to land, or it is within a threat environment. An example of a threat environment would be where a hostile actor would have access to the communications channels.

Table 5-1: Catalogue of Generic RPAS Objects and Descriptions

132. The risk to each business asset needs to be assessed in terms of a compromise to its Confidentiality, Integrity and Availability. The outcome of the assessment should be a prioritised list of risks. It should include any privacy risks, regardless of the risk value. The risk register must also include any untreatable risks.

133. In the RPAS example, three objects are out of scope, these are:

134. External Authorities: This is to show that an RPAS would need to communicate voice and data to external entities. The voice or data traffic can be provided by either internal RPAS Communications Facilities, such as a VHF Radio to Air Traffic Control from either a ground element or an aircraft, or External Communications Provision, such as telephone or fax between the RPAS and Air Traffic Control.

135. Other Airspace Users: This is to show that an RPAS might need to coordinate its activity with other airspace users, such as voice communications to allow the remote pilot to be able to communicate their intentions to other airspace users, operate the transponder and possibly pass sensor data to other airspace users that are capable of receiving the data. An example could be the provision of timely situational awareness information to border patrol teams prior to arrival on location.

136. External Agencies: This is to show that the RPAS could be tasked by external agencies that need real time access to the sensor data and communication to the remote flight crew, but could be in a remote location. An example of this could be an RPAS being tasked to assist in search and rescue operation. In the event of a major disaster that covered a significant area, a coordination and control Headquarters could be located some distance from the RPAS ground infrastructure but need to be able to task the RPAS based on the situation, which could include FMV from an aircraft sensor and reports from the RPAS ground elements.

5.2 Typical Risks to an RPAS

137. The outcome of a risk assessment should identify the specific risks to the RPAS in the context of meeting a particular business requirement, taking into account architectures and implementations. Some of the typical risks that might be identified are discussed below. (**It should be noted that this is not exhaustive and should not be used as a definitive list**.)

5.2.1 Command and Control Links

138. This refers to the communications between a GCS and an aircraft, and between multiple RPAs if information is being relayed between aircraft. Many risks to command and control links will be mitigated as part of the airworthiness certification process.

139. This link is prone to interception and can therefore be observed by an attacker. If the link contained information that was mission critical data, such as way-points, target areas and aircraft health information (such as remaining fuel) then the confidentiality of this information could be compromised and therefore hinder the successful completion of a task.

140. The communications link would also be susceptible to an active attack, where attackers either try to alter the information or replay previously sent information, affecting the integrity of the information and the availability of the RPAS.

141. The command and control links are also susceptible to jamming and the RPAS, specifically the aircraft, must be able to deal with these attacks and enter a known lost link procedure, in order to maintain the operational availability of the asset.

142. Possible mitigations include encrypting the traffic and employing a protocol to prevent the replay attack, such as sequentially labelling or time stamping the on-air traffic.

5.2.2 Imagery Data Links

143. This refers to the sensor data that is transmitted from the aircraft. The data can be received by GCSs and other receiving assets.

144. This link is prone to interception and can therefore be observed by an attacker. An attacker could therefore observe the same information as an RPAS user, thus affecting the confidentiality of the sensor data.

145. This risk could be mitigated by the use of appropriate encryption techniques. However, the methods of Key Variable distribution for the cryptographic devices would also need to be addressed, as would the associated management overhead.

146. The actual risk to the data needs to be assessed by the data owner, as the imagery from immediate vicinity RPASs might not be that critical, as the perceived technical capability or

opportunity of an assailant might not warrant the use of encryption. However, other observers could still access the information.

5.2.3 Other Communication Bearers

147. Overall business needs will rely upon the distribution of information from the use of RPAS implementations. This will often rely on the use of existing communications networks, such as radio systems for voice and networks for data. The bearers chosen must be capable of providing the appropriate level of protection to the information in transit, in terms of confidentiality, integrity and availability, and the appropriate information exchange requirements should be agreed.

148. Another bearer that needs consideration is the received GPS signal, which is susceptible to jamming. This will need to be taken into account, as an aircraft might need to enter a lost link or GPS denied mode of operation.

5.2.4 System Users

149. There will be a need for system users to authenticate to the system, prior to its use, thus allowing for all actions to be recorded and preventing repudiation of commands. This not only refers to the operation of an RPAS but also the downloading of information from the RPAS.

150. System users should be divided into appropriate roles and responsibilities. This is both from an operational point of view, such as a remote pilot or an RPAS commander, and a technical point of view, such a normal users and users with enhanced privileges, such as administrators.

151. Related risks could be mitigated by the appropriate use of strong Identification and Authentication protocols and procedures, to ensure that only authorised individuals can gain access to the information, an Accounting and Audit policy and an appropriate Protective Monitoring policy.

5.2.5 Data at Rest

152. As all RPAS architectures have the potential to store data at rest, and they might have a requirement to archive data for retrieval at a later date, then the data should be protected appropriately. Any data aggregation or association issues should also be considered.

153. For example, an evidential chain for the data or the privacy of a person’s action, which was observed by an aircraft, could be protected by an appropriate encryption.

154. This is also important in the case of through life support and maintenance tasking on the system, where the maintainers might be from an external, possibly less trusted, source.

155. If the RPAS is to be used by different agencies, there may be a requirement to ensure that the system has an appropriate reuse policy, to ensure that any media is appropriately sanitised, prior to reuse.

5.2.6 Other Areas of Possible Concern

156. There may be a requirement to provide aircraft flight plans to civil authorities, prior to the flight of an aircraft, which might be available to a potential attacker.

157. If an aircraft routinely flew the same route at the same time, then an attacker could take advantage of this.

158. An aircraft might have a separate emergency command and control link, where upon receipt of the appropriate command the aircraft will perform an emergency action. An example of this is lighter-than-air aircraft often have the ability to “dump” the gas that is assisting with the lift, in order to provide an emergency controlled descent. These emergency links should be protected to prevent a potentially simple Denial of Service attack from taking place.

159. There are moves towards making RPAS autonomous and semi-autonomous, which will only increase the need for RPAS architectures to be secured appropriately.

160. Certain RPAS perform data manipulation and processing on-board the aircraft, as the amount of information gathered by the aircraft would be too great to send to the GCS, due to bandwidth constraints. The aircraft might therefore need to protect the capability from hostile attack. This would need procedural handling and support regimes, as well as data at rest policies, for storage purposes and in case of a crash.

Appendix A - RPAS Maintenance and Repair

161. An RPAS maintenance and repair model has been provided for completeness.

162. Figure A- shows a high-level model for RPAS maintenance and repair arrangement, from first to fourth line repair. The aim is to show typical connections and business objects that an RPAS maintenance and repair arrangement might use. The model should be adjusted according to the actual RPAS maintenance and repair implementation.

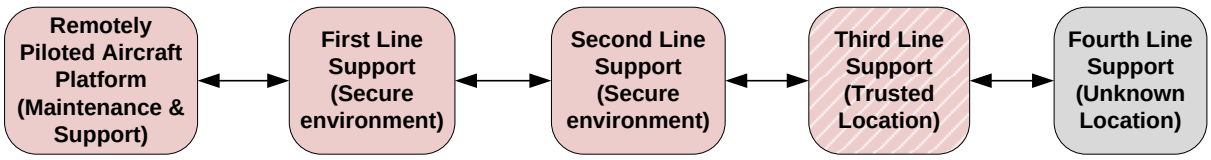

Figure A-1: Potential RPAS Maintenance and Repair Arrangement

163. The support objects for the various levels of repair for this system are defined as:

164. First Line: Minor maintenance, repairs and regular servicing. This is the maintenance and preparation of complete systems or equipment to keep them in a state of readiness for normal daily use.

165. Second Line: Minor maintenance, repairs and regular servicing, where the item concerned is in an unacceptable condition or requires preventative maintenance.

166. Third Line: This is sometimes referred to as deep support or maintenance. This incorporates more significant damage repair, scheduled major servicing and all maintenance. This could be provided by the user or a trusted third party, such as a repair agency or a trusted subject matter expert. The third line support can call on the knowledge of developers and system architects but generally does not directly interface with the end user.

167. Fourth Line: The maintenance activities that require aircraft design authority knowledge. This often involves the complete overhaul and/or modification of the RPAS and is generally carried out by the RPAS manufacturer or an equivalent.

168. The proposed model can be changed as required. For example, the implementation might not have a second line support facility or the equipment manufacturer provides all support to the RPAS.

169. The model in Figure A- shows that the first and second line support is being implemented as part of the RPAS programme and is therefore subject to its assurance. The support would take place at trusted and controlled locations, for example changing Line Replaceable Units (LRUs) at a Launch and Recovery site within a secured section of an aerodrome. Maintenance and repair would also take place in trusted locations. This is important, as the RPAS equipment might contain sensitive or classified information, such as commercial or government information, respectively, and therefore would need to be subject to agreed handling requirements.

170. In this example, the third line support is shown to be part of the assurance activities, as the assumption is that the RPAS requires the third line support to be able to continue with its role and business requirement within a timely fashion. That is, there might be a reliance on third line support as part of the business continuity plan or there might be requirements to provide rapid prototyping for particular missions.

171. The provider of the third line support might also have requirements placed upon them, such as its own certification status and handling requirements. If the third line support provider is providing the support specifically for the RPAS programme, then the provider might fall under the assurance activities of the RPAS.

172. In this example, the fourth line support is out of the assurance activities, as it is assumed that there will be minimal interaction with the original equipment provider, from a security perspective. That is, the fourth line support could provide structural components and hardware, but there would be a reliance on the third line provider to ensure that no sensitive or classified data was sent to the fourth line support provider. There might also be a requirement to ensure the integrity of any hardware, firmware or software sent to third line support from the fourth line support provider. An example of this might be the checking of software from fourth line for viruses or ensuring that hard drives provided do not contain erroneous software that had been used for development but could jeopardise the security of operations.

Appendix B - RPAS Training Provision

173. RPAS training provision has been included for completeness.

174. Figure B-1 shows a proposal for a high-level generic corporate model for RPAS training provision. The aim of this model is to show typical connections and business objects that an RPAS training arrangement might use. The model should be adjusted according to the actual RPAS training arrangement.

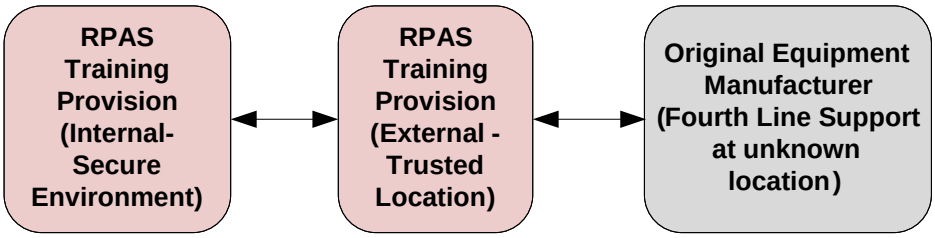

Figure B-1: Potential Corporate Model for RPAS Training Provision

175. The training provision, shown in Figure B-1, shows both internal and external training provision for the RPAS. The actual arrangement will be dependent upon the individual program implementations and requirements.

176. Figure B-1 is showing that there might be a requirement to provide internal training. This could be the case where the training provided requires access to previous sensor imagery, which might be of a sensitive nature or have a classified marking. Other possible reasons could be that the training might be specific to an operation about to be undertaken or might provide information on the RPAS performance and capability as a whole, rather than just using publically available sensor performance.

177. Due to these potential requirements, the internal training would fall under the assurance process for the RPAS.

178. The external training provision would allow for external trainers to train the end user to the full capability of the RPAS as a whole, including any sensitive aspects of the RPAS, without needing access to previous RPAS generated information. An advantage to this approach is that an external body that specialises in such training can be used.

179. The external training can be tailored in such a way that the maximum classification of the training provided is limited. That is, the RPAS when operational might have a classification of SECRET but the training provided to allow remote flight crew to use the RPAS might only be as high as OFFICIAL - SENSITIVE.

180. Figure B-1 shows the external training provision within the assurance process, as without current, suitable and approved training, the remote flight crew might not meet all the requirements to operate the RPAS.

181. It should be noted that if the external training provider did not have a suitable certification status, then the external training might also come within the assurance activities of the RPAS, or the RPAS programme would provide a separate certification for the external training.

182. The RPAS programme might also use a combination of internal and external training. Examples of this are external trainers are used to train remote flight crew, who in turn train other remote flight crew.

183. The Original Equipment Manufacturer, fourth line support, is also included within the model, as this is the source of the majority of the information that will be used to generate training material. As the original equipment supplier might not have any requirement to have access to any of the RPAS generated information, or even know what the purpose of the RPAS is, then the Original Equipment Manufacturer is not in the assurance process, but does have connections to the training providers.

184. A business connection between the internal training provider and the original equipment manufacturer, as shown in Figure , could be present within the RPAS. This example is shown for two reasons:

- There might not be an external training provider and the original equipment manufacturer might be the only source of training information.

185. The RPAS trainers might want to know about some specific or specialist advice. This might include enquiring about training techniques for future developments, of which the external training provider is unaware.

186. In a similar fashion, there could be a direct connection from the RPAS to either the external training provider, if the RPAS programme did not wish to have a potential training burden, or to the original equipment manufacturer, where appropriate. An example of this could be when the RPAS implementation is simplistic with no storage of the RPAS sensor information, such as local law enforcement with a single aircraft, providing real time video to a visor mounted display and nowhere else.

187. Connections from internal training provision to the external training provision and the internal training provision to the original equipment manufacturers are within the assurance process. This is because the RPAS is responsible for the policy of their data exchange with the other parties and the policies and processes would need to be agreed, prior to any data exchange.

188. As with all training, it is recommended that a Training Needs Analysis should be considered, as should the validation of any training provision.

Appendix C - Overview of High Level Security Measures for an RPAS

High Level Security Control/measure	Guidance
Security Policy	
Information Security Policy	The RPAS will need to operate under an applicable information security policy. The security policy should be available internally with the RPAS and the supporting business. The information security policy should be referenced within any overall business plans. The information security policies should be regularly maintained and reviewed annually.
Organisation of Information Security	
Internal Organisation	There should be senior ownership of the RPAS and the supporting governance. There should be representation from all relevant areas of the organisation. This could include: technical areas (to assist with RPAS requirements for such things as technical support, maintenance, training, procurement and through life upgrades), current and developing security teams (to assist with RPAS physical protection and advising on implementation considerations, such as key variable delivery requirements), HR and legal teams (to assist with who can operate the RPAS, where it can be operated, training requirements and contractual requirements, such as repair contracts). There might be requirements for confidentiality agreements, such as when providing coverage for a third party or using a third party to store information. Due to the nature of RPAS, there is a possibility that there will be contact with authorities, outside the normal use of an RPAS. For example, the incident management team might need to communicate with Police or Fire, if an RPAS no longer responded to command and control. All information security incidents related to UK HMG classified/sensitive systems must be reported to GovCertUK and in the event of cryptographic incidents, to CINRAS. Incidents related to commercial systems should be reported to CERT UK. The RPAS internal organisation should keep abreast of and maintain an awareness of security issues; this is

High Level Security Control/measure	Guidance
	often achieved by maintaining contact with special interest groups and professional associations. An independent review of security should be undertaken periodically, gaining an understanding of any changes that have occurred since the RPAS was first certified and ensure any new risks have been identified and acted on.
External Parties	The RPAS risk management process must identify any risks that are presented by external parties. This could include third parties that you have a business requirement to communicate with, such as airspace providers, other agencies that the RPAS is supporting (such as search and rescue or police teams) or a third party that the RPAS is utilising to support remote data storage. The third parties must be made aware of any of the RPAS requirements and must agree to these requirements. The RPAS should control and monitor all access, unauthorised access attempts, and access by third parties. The identification and authorisation standards for third parties will need to be established and documented in the appropriate security plans. Security monitoring and incident management will need to be implemented in such a way that it does not unreasonably adversely affect the business requirements for operating an RPAS. For example, what actions would be undertaken if a security event was detected by an external 3rd party supplier as certain actions could prevent the business function of the RPAS from being carried out?
Asset Management	
Responsibility for Assets and Asset Registers	Assets should be assigned to owners and RPAS assets should only be used in an acceptable manner. For instance, if the RPAS had a laptop as one of its component parts, it might not be acceptable to allow RPAS users access to this laptop for non-business purposes. All assets within an RPAS must be auditable. This might take the form of an asset register or inventory of assets and should contain information, system and software assets. This should include any build standards or modifications. Component parts of an RPAS might be modified for a specific tasking and thus alter the build standard of

High Level Security Control/measure	Guidance
	the individual component parts, whilst the remainder of the RPAS inventory remains unaltered. Within an RPAS, this might be linked to other registers, such as maintenance registers, to assisting in maintaining airworthiness.
Information Classification	The RPAS assets must be valued by the business with regards to their confidentiality, integrity and availability. Where appropriate, assets should carry some form classification, to help guide their secure handling.
Human Resources Security	
Prior to Employment	The RPAS authority should clearly define the required roles, and associated responsibilities, for the posts within the RPAS. The RPAS authority should ensure that any information security responsibilities, for a particular role, are included within the terms and conditions or employment or contract.
During Employment	Information security education, training and awareness must be provided, where required. This should include the dissemination of Security Operating Procedures (SyOPs). Staff handling sensitive or classified information must understand their personal responsibilities for securely handing the information relating to the RPAS.
Termination of Change of Employment	As part of the standard procedures for terminating the employment of a member of staff, or if a member of staff leaves a particular role, it is important to remove their access rights and permissions to the RPAS. This is especially important if the user had the capability to remotely access the RPAS, such as via an RVT system configuration or remote tasking facility. All assets in the users charge must be returned to the RPAS authority, this includes hardware, software and potentially other items, such as documentation. It is imperative that equipment SyOPs detail the requirements to return assets to the RPAS authority. Staff leaving employment or an area should be debriefed and made aware of any ongoing responsibilities, such as the Official Secrets Act or Intellectual Property Rights.

High Level Security Control/measure	Guidance
Physical and Environmental Security	
Secure Areas	Appropriate physical protection must be ensured. This will be dependent upon the implementation of the RPAS. If the RPAS operates from a permanent location, then perimeter security around an airfield might be requires. If the RPAS is mobile in nature, then secure facilities, such as a secured area around a GCS, might be required. Entry controls to locations will have to be to a required, and agreed, standard. Secure areas might have to be identified and secured appropriately. This need not only be at an RPAS operational location but also at secondary locations, such as remote storage facilities and areas for post collection analysis. The risk presented by the operating location should be taken into account, this should include environmental threats. Certain locations, such as those providing support to Search and Rescue in a disaster location, might have a multitude of other people in the area. This might have to be controlled in some way and facilities provided to ensure separation from RPAS equipment. Examples of this might be the general public, external fuel providers and delivery of supplies.
Equipment Security	The location of equipment needs to be considered. Risks from overlooking, especially if using an RVT should be considered by the risk assessment. Unauthorised access to equipment should be prevented, which includes equipment that is in storage, as well as in operation. If the RPAS requires supporting utilities to operate, such as power, then risks to an interruption of the utilities needs to be considered. If the cabling between entities is accessible, there is potential for accidental damage, tampering, interference or interception. This risk might be reassessed as a matter of routine, such as at predetermined intervals or when there is new activity local to the RPAS, as this might have an effect on the RPAS equipment and its associated location and routing.

High Level Security Control/measure	Guidance
	Maintenance activities will need consideration, such as where maintenance activities are conducted, any security requirements that are placed on maintenance facilities and any specific requirements that are placed on the maintenance staff, such as training or vetting requirements. Equipment disposal and re-use need to be addressed, to take into account any sanitisation requirements of hardware and media.
Communications and Operations Management	
Operational Procedures and Responsibilities	All users should be provided with the required training and documented security operating procedures. This provision not only assists the operation of the RPAS but also minimises the likelihood of an accidental compromise of information. Where appropriate, there should be a segregation of duties within roles. All actions should be attributable to an individual user and this might be achieved through the use of non-technical methods. For example, if an RPAS pilot logs on to a system and there is then a shift change, it might be unacceptable for the user to log off and a new user log on. Therefore, a user, or a user role, might log on and the actual user operating the equipment may be recorded in a separate log, to identify the responsible individual without interrupting flight operations. There should be a separation between development, test and live systems and a change management process in place to undertake the implementation of change management. Personal, classified or operational data should not be used on development equipment.
Third Party Service Delivery Management	Delivery partners must comply with the security requirements set out in contractual agreements and specified by the RPAS owner. The contracts should include audit rights for the RPAS owner to ensure ongoing compliance to security requirements. Any services supplied by a third party should be controlled in accordance with a change control management process.
Service Planning and Acceptance	The capability requirements of a new RPAS system should be developed to ensure it meets the performance levels required. These levels should attempt to account for future service requirements and

High Level Security Control/measure	Guidance
	system performance should be monitored in an attempt to assist with this process. The system acceptance process should ensure that all security requirements have been achieved. System upgrades should not affect any of the certified security functionality.
Protection Against Malicious and Mobile Code	There need to be controls in place to minimise the risk from malicious code. Typical examples for an RPAS could be minimum privilege access for normal users, standalone antivirus machines (sheep dip machines) and run antivirus on the operational system. The issue with running antivirus on the operational system is that this might have to be undertaken in non-operational times, so as not to potentially affect a flight, and might have to be performed by a component that is not deemed to be within an airworthiness boundary.
Back-up	A RPAS implementation should ensure that appropriate back-up and restore policies are implemented. These should take into account: • What information should be backed up; • The required restore period. This is for both the RPAS system and RPAS derived information; • Testing the restore process; • Testing, and importantly checking, the backups; • Appropriate offline storage and protection of backup information and media.
Network Security Management	Network security controls should be applied to networks and network services in accordance with the outcome of a technical risk assessment. Typical examples might the differentiation between normal users and privileged users or administrators in access control requirements. Security requirements need to be included within any network service contracts and service level agreements.
Media Handling	The management of removable media is of paramount importance. Users will need to be made aware of this in SyOPs and provided with the appropriate training. Where appropriate, removable media should be encrypted, to provide a level of protection.

High Level Security Control/measure	Guidance
	Where media has contained classified, personal or sensitive information, it should be sanitised, destroyed or re-used appropriately. System documentation should also be handled in an appropriate manner, as this would give a potential attacker an immediate advantage.
Exchange of Information	If the RPAS is to exchange information with other parties, such as to receive tasking or meteorological information or provide sensor and analysis information then information exchange policies, procedures and agreements should be in place. Exchange agreements should, as a minimum, contain: • What information is to be exchanged? • How will information be exchanged? • How should each party involved handle the information exchanged? • Who can exchange information? • How will the exchange be secured and monitored? • Who is responsible for authorising the information exchange? • Who is responsible for managing the security of the interconnection or shared service? Physical and removable media must be protected in a manner appropriate to its sensitivity and classification. The exchange of information, such as messaging, must take into account the confidentiality, integrity and availability of the information. The availability of an information exchange could be overriding in the event of a search and rescue tasking, where as the dominant attributes for criminal investigation might be confidentiality and integrity of the information.
Monitoring	The RPAS must be capable of producing reports of user activities, including administrative activities, to support monitoring, incident response and investigations. Procedures should be in place to actively monitor systems and system users and policies should be in place in the event of an incident, or suspected

High Level Security Control/measure	Guidance
	incident, occurring. This might include referencing a forensic readiness plan. The audit logs should be handled in accordance with their sensitivity or classification. The logs that are reviewed might well include fault logs, as well as security logs, to allow for potential failures to be observed and appropriate action to be taken to ensure that the RPAS remains in service. Due to the distributed nature of certain RPAS, there might be a requirement to ensure that all clocks are synchronised across the RPAS.
Access Control	
Business Requirement for Access Control	To allow an individual access to an RPAS, there has to be a valid business reason and access should be controlled on a "least privilege" basis. Access control refers to both logical access, such as a payload operator logging onto a system, and physical access to the RPAS hardware itself.
User Access Management	It is important that the RPAS has a formal procedure to register a user, grant access to particular systems and revoke access rights. Access rights might be revoked and then returned during a user's absence period. User access rights need to be reviewed periodically and revoked when no longer required. If a user leaves the RPAS role or their employment is terminated, the access rights should be revoked immediately.
User Responsibilities	Corporate policies (and the SyOps) should set out the minimum requirements for user passwords and associated processes, including: password generation, selection and protection and reset. If users are able to generate their own passwords, complexity rules should be adhered to and inbuilt password checking enabled, where available. Password policy should be available to the user to reference, containing such requirements as: never divulge their password and if it requires writing down, then the storage and physical protection of the written password should be commensurate with the classification of the data being protected. If an RPAS user is not able to screen-lock a system when they leave the system unattended, such as during

High Level Security Control/measure	Guidance
	a rest period when the RPAS is still operating, then the user will need to ensure that actions are still attributable to another person. In this instance, the RPAS data owner might need to consider implementing other physical, procedural or technical controls to address the risks posed to unattended equipment. If a user needs to leave an RPAS element, then the user should ensure that, when appropriate, information should be secured. This includes documentation, as well as the IT systems.
Network Access Control	Access to internal and external networks must be controlled and documented in procedures and policy. Remote access must be appropriately authenticated, this could be from other RPAS elements or from entities utilising the RPAS services. As an RPAS network could be physically dispersed, the RPAS should prevent any unauthorised connections to both internal and external networks. The network should automatically identify equipment that is connected, enforce access control policies and should authenticate connections from remote locations or organisations.
Operating System Access Control	The system should be locked down to ensure that the RPAS only uses the services that it requires. This could assist in maintaining any air safety and safety of flight requirements by ensuring that the system configuration is maintained and can only be accessed and/or altered by authorised personnel, such as system administrators. The system should have secure log-on processes, procedures and policies that clearly identifies and authenticates users. This will enable audit to be undertaken and accountability of actions to be established. It could also be used to ensure that remote flight crew are qualified to undertake the appropriate role. That is, a user logs on based on a role that they have been trained for, such as a payload operator or a pilot. On larger RPAS, this could be linked in to a training system, which might assist in maintaining the currency of the users' training. If the RPAS will only operate within certain timeframes, such as night operations only, consideration should be given to limiting user access times. That is, a pilot would not need access to certain system

High Level Security Control/measure	Guidance
	elements when the RPAS cannot fly. However, the pilot might need access to other areas of the system in these timeframes, such as online training provision and other duties.
Application and Information Access Control	The RPAS owners and data owners should give consideration to “need to know” and “least privileges” when it concerns user access to RPAS information. For example, a pilot might not need access to the same information as an image analyst. The methods of importing information from other systems will need to be considered. For example, an RPAS high-risk or mission critical system might need a level of isolation from other systems. This might warrant a physical separation with “sheep-dip” machines utilised between, to lower the risk of malicious code being transferred by removable media.
Information Systems Acquisition, Development and Maintenance	
Security Requirements of Information Systems	The RPAS owners should identify the security assurance requirements for the RPAS. This should follow a formal risk assessment approach which is also acceptable to any other systems or organisations that the RPAS will need to connect to when appropriate. This collective approach should ease the system assurance process, if different systems have different security authorities but they all agree on a common methodology and understanding of risk.
Correct Processing in Applications	Due to the safety requirements of an RPAS, it is important to ensure that data integrity is maintained. For example, if a new software build was delivered, the integrity of the software should be examined; this is to ensure that the information had not been corrupted in transit. A level of assurance of data being consumed by the system from other sources, both internal and external, might be of importance. So to prevent the corruption of the RPAS data from other systems, check the validity of the message source. An example of this could be the positional information provided by the RPAS to external Search and Rescue services.
Cryptographic Controls	If the RPAS employs cryptographic components, a policy must be produced regarding the deployment and management of the key variable devices. This policy should include the generation and protection of key variables and should include the actions to be undertaken in the event of loss, modification or disclosure.

High Level Security Control/measure	Guidance
	If the RPAS employs cryptographic components/elements as specified by CESG then this should conform to the HMG IA Standard (IS4).
Security of System Files	RPAS Systems should establish a configuration control process for the system software. This process will include a patching regime, noting when a system cannot be patched, such as where a software alteration, such as a patch, would invalidate flight critical software evaluations. If a software vulnerability cannot be patched, a risk assessment should be undertaken to assess the risk to the RPAS. When known vulnerabilities cannot be patched, other mitigations might be acceptable, such as physical and procedural methods or removal of certain network connections. Access might need to be limited to system design files, with access only being available to those that require access to support the RPAS business function.
Security in Development and Support Processes	To ensure that the software and hardware build standards are correct and that there have not been any unauthorised changes, the RPAS should have the ability to audit the systems for compliance. This audit links in to a requirement for a formal change control process and procedures. It will also enable the RPAS to be able to provide safety of flight information on build standards. Following any system update, the RPAS may need to undergo performance and regression testing to ensure that any updates do not undermine any existing security controls and mitigations to the RPAS. Where the RPAS developer has outsourced elements or components, these may need additional supervision followed by additional test and acceptance requirements.
Technical Vulnerability Management	The RPAS authority should ensure that, where possible, system and applications are updated and patched to fix known security vulnerabilities. Where systems cannot be patched, such as due to configuration control and associated testing and evaluation of safety critical software, a risk assessment of the system should be conducted. Where possible, vulnerability patching should be in as short a time as possible to reduce the window of opportunity for threat actors to exploit these known vulnerabilities. Based on the utilisation of the RPAS, it might be appropriate to undertake periodic IT health checks and vulnerability assessments.
Information Security Incident Management	
Reporting Incident Security Events and	The RPAS authority should develop and implement an incident reporting mechanism and the users of the

High Level Security Control/measure	Guidance
Weaknesses	RPAS should be made aware of this.
Management of Information Security Incidents and Improvements	The RPAS might require a forensic readiness plan to be place. This plan might assist in legal requirements in the event of the RPAS being misused or information being obtained from the system by an unauthorised third party. The RPAS authority should have a review process in place to review security incidents and, if appropriate, modify policy or relevant controls. This process might also have an impact on the RPAS user training requirements.
Business Continuity Management	
Information Security Aspects of Business Continuity Management	Due to the nature of an RPAS, it is imperative that business continuity is addressed. The RPAS authority should put in place and regularly check business continuity arrangements. As an RPAS could be subject to malicious, accidental and natural events, all should be taken into consideration during a risk assessment and should be considered in a business continuity plan. The RPAS should ensure that it can be restored and be available in an appropriate timeframe. This is both from an RPAS operational viewpoint, such as the flying of an aircraft, and from an "offline" perspective, such as the generation of RPAS product that can be carried out post flight. If there are multiple business continuity plans for different systems, it is important to ensure that not only are they proportionate but also that they are compatible with each other. It is also important to prioritise business continuity plans, both from an RPAS system perspective and from a connected system perspective.
Compliance	
Compliance with Legal Requirements	The RPAS must comply with all relevant legislation. Consideration might have to be given to Intellectual Property Rights (IPR). RPAS records need to be protected in accordance with legislation. This might include; the data protection and privacy of personal information, both the RPAS users and information on collected data; operational

High Level Security Control/measure	Guidance
	information, such as flight paths; and incident reporting information, such as from flight data recorders in an aircraft and voice recorders within an RPAS ground element. RPAS users can also be deterred from misusing RPAS equipment by making them aware of the Protective Monitoring policy.
Compliance with Security Policies and Standards and Technical Compliance	The RPAS authority should regularly check that security policies, standards and requirements are being complied with, this should include technical compliance checking, and annual reports should be made to management on the state of protective security.
Information Systems Audit Considerations	It is important to recognise that audit and compliance checks do not adversely affect the operation of the RPAS. Any audit tools that stay resident on the RPAS must be protected to ensure that they are not available for use during the normal operation of the RPAS.

Appendix D – Acronyms

ATC	Air Traffic Control
BRLOS	Beyond Radio Line Of Sight
CINRAS	COMSEC Incident Reporting Alert Service
FMV	Full Motion Video
GCS	Ground Control Station
HMG	Her Majesty's Government
HR	Human Resources
IA	Information Assurance
ICT	Information Communications Technology
IEC	International Electrotechnical Commission
ISO	International Standards Organisation
L&R	Launch and Recovery
LAN	Local Area Network
LOS	Line of Sight
PIA	Privacy Impact Assessment
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft Systems
RVT	Remote Viewing Terminal
SyOPs	Security Operating Procedures
U/VHF	Ultra/Very High Frequency
VHF	Very High Frequency
VTOL	Vertical Take-Off and Landing

Appendix E – References

ICAO Manual on Remotely Piloted Aircraft Systems (RPAS) (Doc 10019)

ISO/IEC 27001:2013 “Information technology — Security techniques — Information security management systems — Requirements” is available from www.bsi.org.uk

ISO/IEC 27005:2011 “Information technology -- Security techniques -- Information security risk management” is available from www.bsi.org.uk

NIST SP800-53 Recommended Security Controls for Federal Information Systems and Organizations from the US National Institute of Standards and Technology. The April 2013 version is available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

UK CAA CAP 722 Unmanned Aircraft System Operations in UK Airspace (Sixth Edition, 31 March 2015) – Guidance is available at www.caa.co.uk/docs/33/CAP%20722%20Sixth%20Edition%20March%202015.pdf

HMG IA Standard No. 4, Management of Cryptographic Systems, Issue 6.0, April 2014 (OFFICIAL). Available from the CESG IA Policy Portfolio

HMG IA Standard No. 5, Secure Sanitisation, Issue 5.1, December 2014 (OFFICIAL). Available from the CESG IA Policy Portfolio

Information Commissioner’s Office, Guide to Data Protection https://ico.org.uk/for-organisations/guide-to-data-protection/

Information Commissioner’s Office, Conducting Privacy Assessments – Code of Practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Information Commissioner’s Office, In the picture: A data protection code of practice for surveillance cameras and personal information https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf