# Requirements

## Data Assessment for Security and Privacy Assessment

1. **Data Processing**: determine if personal data is being processed. If so a requirement of the Data Protection Act 2018 requires a Data Privacy Impact Assessment be conducted. Conducting a [DPIA](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/) is a legal requirement for any type of processing, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals.

Additionally, if personal data is used, it is also a legal requirement to document processing activities, often in the form of Records of Processing Activities ([ROPA](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/records-of-processing-and-lawful-basis/))

1. **Business Impact Review**: assess value of information assets based against loss of Confidentiality, Integrity, and Availability (CIA). The assigned Information Classification of the data used by the application is used as a starting point to determine criticality.   
     
   A ranking (out of 3) will help determine business criticality when comparing two applications. For example, a critical application would have a ranking of 3:3:3 compared to a non-critical application of 1:1:1, and therefore the critical application will require a greater amount of security controls.

# Design

## Security Architecture

Identity and Authentication

Mutual Authentication

Attack Surface Review

Access Controls

Logging and Monitoring

## Application

## Security Testing

SAST and DAST

Vulnerability Scanning

## Threat Modelling

# Release

## Incident Response Plan

## Documentation

# Create Risk Assessment