# Article information:

Architecture and configuration - NCSC.GOV.UK
<https://www.ncsc.gov.uk/collection/10-steps/architecture-and-configuration>

# Article summary:

1. Understand the context and risks before designing a system, and choose security controls based on those risks.

2. Make systems easy to maintain and update, reduce the attack surface, and make compromise and disruption difficult.

3. Reduce the impact of compromise by preventing lateral movement, use antivirus applications, plan for backup and recovery, and make it easy to detect and investigate compromises.

# Article rating:

Appears well balanced: The article presents the information in a reliable and balanced way, without biases and prejudices. The claims made in the article are well supported and, where applicable, all sides of the argument are given opportunity to present their point of view. The article appears trustworthy and reliable.

# Article analysis:

The article is generally reliable in its content as it provides a comprehensive overview of architecture and configuration from a cyber security perspective. The article covers topics such as understanding the context before designing a system, making systems easy to maintain and update, reducing the attack surface, making compromise and disruption difficult, reducing the impact of compromise by preventing lateral movement, using antivirus applications, planning for backup and recovery, making it easy to detect and investigate compromises, etc.

The article is written in an objective manner without any bias or partiality towards any particular point of view or opinion. It does not contain any promotional content or unsupported claims; instead it provides detailed information about each topic discussed with relevant examples where necessary. The article also mentions frameworks such as MITRE ATT&CK which can be used to help identify possible ways of disrupting an attacker at different stages of an attack.

The only potential issue with the article is that it does not explore counterarguments or present both sides equally when discussing certain topics such as cloud services or zero trust architectures. However this does not detract from the overall quality of the article as these points are mentioned in passing rather than being central to its content.

# Topics for further research:

* Cloud security architecture
* Zero trust architecture
* Network segmentation
* Endpoint security
* Incident response plan
* Security automation

# Report location:

<https://www.fullpicture.app/item/3415eeabb00adcdc9aae3098da48c675>