

# Security Infrastructure Design

Greenham House Asset Management



Colin Cooper

R00240295

Security Architecture (COMP 9080) 2022/23 - Assignment 3

## 1) Executive Summary

Greenham House Asset Management was recently the victim of two separate IT security breaches that resulted in significant business, reputational, and financial impact. In the first attack, an external malicious actor was able to compromise a web server and use it as an entry point to the company's network to breach a critical database server containing business-critical data. This data was exfiltrated and encrypted in an attempt to extort payment from Greenham House. In the second attack, it appears that an internal malicious actor accessed sensitive files that were stored on a file-sharing server and sent them without permission to a journalist.

The company's IT and network infrastructure has evolved from a simple single-office to a multi-office configuration in line with the rapid expansion of the business. With limited IT staff capacity, priority was given to supporting business growth over initiatives to re-assess and re-configure this infrastructure. No particular enterprise architecture was developed to guide the evolution of IT services to support the growing business and instead systems evolved from isolated, tactical projects with no central guiding framework. This resulted in critical weaknesses that were exploited on multiple occasions by both external and internal malicious actors.

This report focuses on the security architecture of the company, analysing the current environment under the Availability, Integrity and Confidentiality (AIC) framework to assess the security requirements of key elements of the architecture and identify gaps to be addressed. Greenham House has already decided to move away from an on-premises environment to using multiple cloud security providers for SaaS, PaaS and IaaS services. Recommendations to address AIC gaps are made with this in mind.

It is recommended that the company:

- Provision new router hardware to support the up-time requirements for the routers that inter-connect the three regional offices, and each office to the public internet. The company should also retain the existing routers in storage as part of a contingency plan for local router hardware failure as the lead-time to order replacement hardware is likely to be outside the acceptable limit for loss of office connectivity.
- Use the AWS Relational Database Service (RDS) with Multi-AZ deployments to guarantee uptime SLA's (99.95%) for the Customer Investment Platform from a data storage point of view. Configure the RDS service to ensure data-at-rest and data-in-transit is always encrypted.
- Rebuild the company web server that hosts the Customer Investment Platform to use a load-balanced, auto-scaling cluster of AWS virtual machines to guarantee the web applications also meet the 99.95% uptime SLA.

- Implement changes to the Customer Investment Platform to improve the security of passwords stored in the backend database from brute-force decryption methods by moving away from an unsecure hashing algorithm and implementing strong password salting.

This report also looks at the security implications of the company decision to move on-premises services to multiple cloud service providers and recommends that a CASB solution that includes threat detection, threat prevention and data loss prevention features from Proofpoint be implemented in parallel with the planned migration.

The costs of the above recommendations under the AIC framework and the CASB recommendation to support cloud migration are estimated at a high-level. A one-off capital expenditure of €6,000 for three new Cisco routers is recommended, along with €32,040 in recurring operational expenditure.

Lastly, the TOGAF and SABSA frameworks are compared and a recommendation to adopt the SABSA framework is made. Using such frameworks will provide a future alternative to ad hoc unplanned architecture change – and is particularly timely as Greenham House plans to stand-up its new cloud infrastructure and applications. SABSA is a scalable framework that is digestible by even small companies like Greenham House and will help to ensure that the future direction of the company's Enterprise Architecture will align with, enable and support the strategic objectives of the company.

## Table of Contents

1) Executive Summary.....	1
2) Introduction .....	4
2.1. Background.....	4
2.2. Purpose.....	4
3) Main Body Report .....	5
3.1. Security Architecture Evaluation.....	5
3.1.1 <i>Introduction</i> .....	5
3.1.2 <i>Evaluation of the Security Architecture at Greenham House</i> .....	5
3.1.3 <i>Product Recommendations</i> .....	8
3.1.4 <i>Conclusions</i> .....	9
3.2 On-Premises to Cloud Migration – Security Product Recommendations.....	9
3.2.1 <i>Introduction</i> .....	9
3.2.2 <i>Product Recommendations</i> .....	11
3.2. Cost Analysis.....	11
3.3. Comparative Analysis of at least 2 Enterprise Architecture Frameworks .....	12
3.3.1. <i>Topic Introduction</i> .....	12
3.3.2. <i>A Comparison of the SABSA and TOGAF Frameworks</i> .....	14
3.3.3. <i>Framework Recommendation</i> .....	21
4) Overall Conclusions.....	21
5) Bibliography .....	22

## 2) Introduction

### 2.1. Background

Greenham House is a specialist asset management company that focuses on investment funds related to renewable energy, energy storage and commercial forestry. It has evolved from a small company with less than a dozen employees located in Cork to over 150 employees who work in offices in Cork, Dublin, and the UK – as well as remote working.

The company currently has €730m of Assets Under Management (AUM) on behalf of institutional and private investors. In 2022, it had a core net income of €7.44m that translated to an operating profit of €2.64m.

	2021 (€m)	2022 (€m)	Change
<b>AUM</b>	658.00	730.00	+11%
<b>Net Income</b>	4.62	7.44	+61%
<b>Adjusted Operating Profit</b>	1.38	2.64	+91%

Greenham House's IT infrastructure is primarily based in a self-managed data centre within its Cork office that contains the company web, email and database servers as well as being the hub for its network infrastructure.

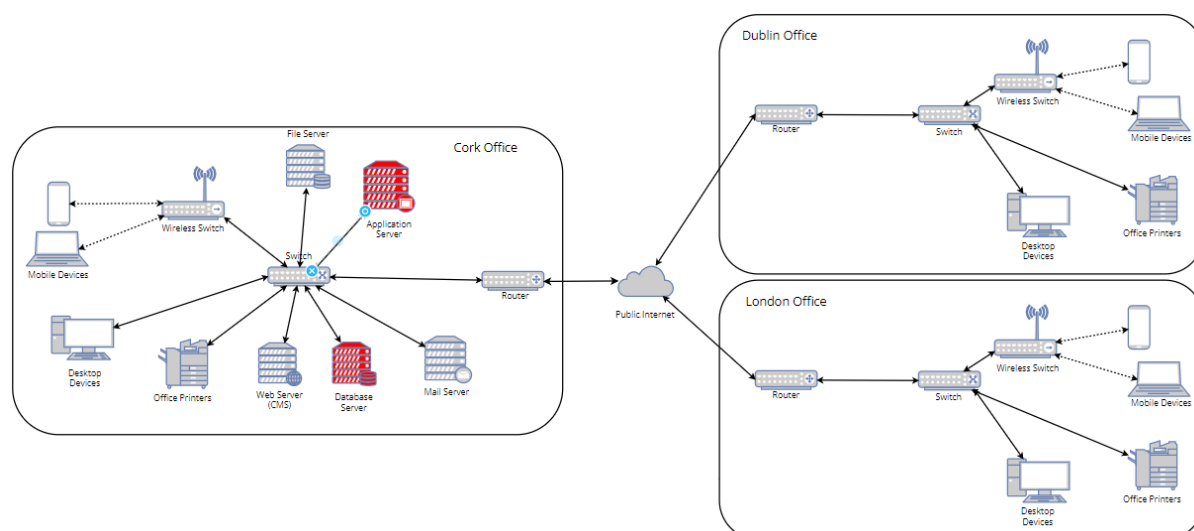


Figure 1 - Greenham House's current on-premises network design

Figure 1 shows the high-level network architecture at the time of the security breaches in 2022.

### 2.2. Purpose

The purpose of this report is to:

1. Evaluate Greenham House's security from an architecture viewpoint and make specific product recommendations to improve it.
2. Identify products needed from a security perspective to support the company's decision to migrate away from their on-premises to a cloud services provider.

3. Perform a high-level cost analysis of all products being recommended.
4. Introduce and compare the TOGAF and SABSA Enterprise Architecture Frameworks and make recommendations on which framework would be most suitable for Greenham House to use to support its ongoing Enterprise Architecture evolution.

### 3) Main Body Report

#### 3.1. Security Architecture Evaluation

##### 3.1.1 Introduction

The Availability, Integrity, and Confidentiality (AIC<sup>1</sup>) triad describes the fundamental principles of information security. *“All security controls, mechanisms, and safeguards are implemented to provide one or more of these protection types, and all risks, threats, and vulnerabilities are measured for their potential capability to compromise one or all of the AIC principles”* [1]

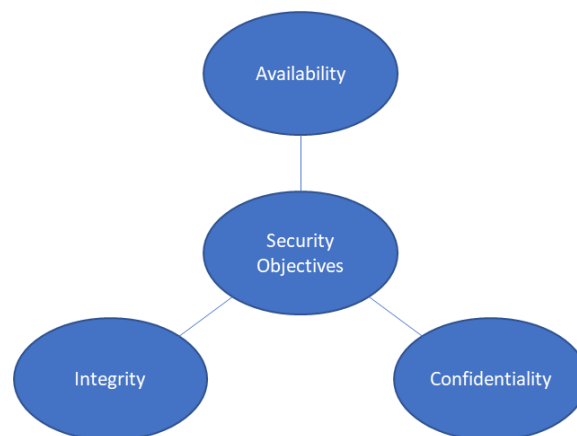


Figure 2: The AIC triad

**Availability** is the degree to which data and resources are accessible to authorised individuals. **Integrity** describes the accuracy of information and systems and assurance that it has not been modified in an unauthorised way. **Confidentiality** is the degree to which only those who should be allowed to gain access are able to do so.

##### 3.1.2 Evaluation of the Security Architecture at Greenham House

The following table is an evaluation of the services and related critical assets associated with Greenham House’s IT architecture. I’ve looked at the controls in place for these assets and identified gaps that should be addressed in a proportionate way.

The company has made a strategic decision to migrate away from on-premises hosted infrastructure to Amazon Web Service (AWS). The controls and recommendations made here assume that minimal to no investment in on-premises system improvement will be

---

<sup>1</sup> or CIA

approved, but that the company will instead implement the controls in a cloud environment.

Data / Service	Related Assets and Associated IAC controls
<p><i>Internet and Inter-office connectivity</i></p>	<p><i>Office Routers</i></p> <p>The on-premises routers (Cisco RV325-K9) support inter-office connectivity between Greenham House sites and to the public internet. Management have estimated that even after the data centre cloud migrations, it is important for each office router to have an 99% uptime (or less than 2 hours per week downtime) Service Level Agreement (SLA) to maintain acceptable business operations and legal agreements with customers.</p> <p>If the company web server and Customer Investment Portal (CIP) were to continue to be hosted in the Cork data centre, then this would require a 99.95% uptime (5 minutes per week downtime). Due to the planned migration to the cloud, this SLA will apply to the CIP cloud infrastructure instead, and 99% uptime is considered an acceptable SLA for the routers in each office site.</p> <p><b>Controls in Place:</b></p> <ul style="list-style-type: none"> <li>• Insufficient on-premises controls are in place. The services are highly vulnerable to device hardware failure or the results of malicious behaviour such as denial of service attacks.</li> </ul> <p><b>Controls Recommended:</b></p> <ul style="list-style-type: none"> <li>• Availability: <ul style="list-style-type: none"> <li>○ The 99% uptime SLA can be achieved without redundant online routers. However, it is recommended that a new router should be provisioned in each of the three sites, with the existing routers stored as a backup in case of catastrophic failure to any of the new routers.</li> </ul> </li> </ul>
<p><i>Customer Data</i> <i>Employee Data</i></p>	<p><i>Databases on the Database Server</i></p> <p>The databases hosted on the Cork on-premises relational database server store data that is used to present account information to customers. It also contains HR and Payroll information needed to manage employees and monthly payroll operations.</p> <p><b>Controls in Place:</b></p> <ul style="list-style-type: none"> <li>• Availability: <ul style="list-style-type: none"> <li>○ The database server contains a RAID 1 disk storage so data is physically duplicated across 2 disks which offers some protection if one of the disks fails.</li> </ul> </li> </ul>

Data / Service	Related Assets and Associated IAC controls
	<ul style="list-style-type: none"> <li>• Integrity: <ul style="list-style-type: none"> <li>○ Data is protected from unauthorised modification through access control managed by the RDBMS software.</li> </ul> </li> <li>• Confidentiality <ul style="list-style-type: none"> <li>○ Data is protected from unauthorised access through the RDBMS software that requires a username and password before any session is created. Customers' account details and passwords are stored in the database itself and used to programmatically determine what records are accessible to each customer.</li> </ul> </li> </ul> <p><b>Controls Recommended</b></p> <ul style="list-style-type: none"> <li>• Availability: <ul style="list-style-type: none"> <li>○ The customer / CRM database has much higher availability requirements than the employee database. It should be provisioned on an AWS Relational Database Service (RDS) with Multi-AZ deployments that have a 99.95% uptime SLA.</li> <li>○ Online and offsite backup and restore plans should be implemented to ensure any future security events that compromise the servers can be remediated quickly within acceptable "Mean Time To Recover" parameters.</li> </ul> </li> <li>• Integrity: <ul style="list-style-type: none"> <li>○ The Amazon RDS database (data at rest) should be encrypted, so that if the data files are accessed directly they cannot be modified.</li> <li>○ Communications between the AWS RDS database and the Customer Investment portal should be encrypted using SSL/TLS to ensure it cannot be tampered with in transit.</li> </ul> </li> <li>• Confidentiality <ul style="list-style-type: none"> <li>○ AWS RDS database encryption will also help to ensure that any stolen data files will not result in the disclosure of confidential information to unauthorised parties.</li> <li>○ All communications (e.g. between the database server and the web server) should use SSL/TLS to ensure it cannot be viewed in transit.</li> </ul> </li> </ul>
<i>Customer Investment Portal (CRM Tool)</i>	<p><i>Company Web Server</i></p> <p>The company Web Server hosts both static website content, dynamic CMS content such as annual reports, announcements and marketing information, and the company CRM system (CIP) that provides access for customers to their accounts.</p>



Data / Service	Related Assets and Associated IAC controls
	<p><b>Controls in Place:</b></p> <ul style="list-style-type: none"> <li>• Availability: <ul style="list-style-type: none"> <li>○ Insufficient controls are in place. The Customer Investment Portal is hosted on a single physical server. If that server experienced an outage, the entire CIP portal would be unavailable for the outage period.</li> </ul> </li> <li>• Integrity: <ul style="list-style-type: none"> <li>○ Access control to the Customer Investment Portal to make account changes is controlled through user accounts and passwords that are stored in the database server. Passwords are hashed using the MD5 protocol.</li> </ul> </li> <li>• Confidentiality <ul style="list-style-type: none"> <li>○ The website implements and forces the use of HTTPS / SSL to ensure that data served from the web server is encrypted in transit to the requesting client.</li> </ul> </li> </ul> <p><b>Controls Recommended</b></p> <ul style="list-style-type: none"> <li>• Availability: <ul style="list-style-type: none"> <li>○ The web server needs to be Highly Available for customers to access their accounts. It is recommended to redesign the portal to use a load-balanced auto-scaling cluster of AWS-hosted web-servers (EC2) that is resilient to failure in any individual server or server component.</li> </ul> </li> <li>• Integrity: <ul style="list-style-type: none"> <li>○ While better than clear-text password storage, the MD5 protocol for password hashing is no longer considered to be secure. It should be replaced with at least a SHA-256 hashing mechanism that also utilises password salting.</li> <li>○ Support and recommend the option for customers to use multi-factor authentication to access their accounts.</li> </ul> </li> <li>• Confidentiality <ul style="list-style-type: none"> <li>○ Password hashing, salting and MFA recommendations also apply here to ensure account information is restricted to authorised individuals.</li> </ul> </li> </ul>

### 3.1.3 Product Recommendations

To support the above recommended controls, it is necessary for the company to invest in several products:

**Router Redundancy:** Cisco Inter-chassis High Availability supports the configuration of pairs of routers to act as backups for each other [2]. The current router in the Cork office does not support this kind of redundancy. If the company had chosen to maintain its on-premise data centre infrastructure it would have been necessary to add router redundancy to ensure uptime SLAs for the Customer Investment Portal were achievable. This could have been achieved by replacing the current router in Cork with two Cisco 4000-series routers that do support High Availability redundancy. With the cloud migration, this level of “live” automatic failover redundancy is not necessary. However, it is still recommended that the company purchase new Cisco C1111-4P routers for each of the three sites and store the old routers in case of catastrophic hardware failure where a replacement router would be needed. It would be undesirable from a timing perspective to have to order a new router to restore business operations.

**Database Failover and Redundancy:** Migrating the Customer Investment Portal database to AWS RDS Multi-AZ brings several inherent benefits for failover and redundancy. A primary database is provisioned in one Availability Zone (AZ, i.e., physical data centre) while a standby instance of the database is provisioned in another AZ. If a failure is detected, Amazon RDS automatically fails over to the secondary database instance in seconds.

**Database Backup:** AWS RDS Backup and Restore is a default feature of the RDS service. The automated backup feature allows automatic backup of databases and transaction logs, that allow the restoration of the database to several points in time if needed.

**Webserver Failover and Redundancy:** A similar solution to the database failover and redundancy solution should be implemented. The current webserver is also running on an out-of-warranty Dell blade server, and it is recommended to be replaced with a load-balanced auto-scaling 2-server cluster of AWS-hosted webserver (EC2) that is resilient to failure in any individual server or server component.

#### 3.1.4 Conclusions

Analysis of just the most critical systems and data in the current architecture through the AIC framework highlights several deficiencies that could lead to failures with significant business impact. Significant improvement in the Integrity and Confidentiality security principles are possible with adjustments to the configuration of existing DBMS software to ensure that data is no longer left unencrypted at rest. Investment in redundant hardware is required to address the gaps highlighted by the Availability principle perspective. Critical business operations are dependant on single assets that can (and mostly likely will) fail. To ensure graceful failure with minimised impact for the most critical business operations, this out-dated hardware needs to be replaced with clustered systems in the cloud that can survive a fault or failure in any single node.

### 3.2 On-Premises to Cloud Migration – Security Product Recommendations

#### 3.2.1 Introduction

After a careful cost-benefit analysis, Greenham House has made the strategic decision to migrate its on-premises infrastructure to the cloud using Amazon Web Services as its main cloud service provider, and Dropbox as its document storage solution to replace local

network file shares. Using a cloud infrastructure does not obviate the need for security systems to be in place and careful consideration needs to be given to how security is managed from physical infrastructure through to identity and access management in the new environment.

In a cloud environment, the cloud service provider assumes responsibility for the physical buildings, network, and host infrastructure. They need to monitor and control physical data centre access and ensure that hardware within the data centre is operating normally and replaced when needed. Greenham House will need to retain all the responsibilities around data access and identity management. Depending on the cloud service being used, AWS or Greenham House may have responsibility for application management, network control and operating system management.

The cloud does not guarantee security – misconfigurations can still exist; software can still contain exploitable vulnerabilities; and users can still compromise their identity to malicious third parties. Intrusion Prevention and Detection remain key security concepts even in the cloud. In some ways, moving to the cloud complicates security. In the on-premises + managed device model, the company fully controls the perimeter of the data centre (through VPN gateways, IPS, IDS, Firewall, and web proxies) and the devices that employees use. In the cloud model, that simple perimeter no longer exists. Sanctioned SaaS applications like Dropbox are accessible from the public internet by employees and threat actors using unmanaged devices. Employees can also access unsanctioned SaaS applications (“shadow IT”) such as using a personal Google Docs account from their managed devices and thereby creating a security blind spot for the company.

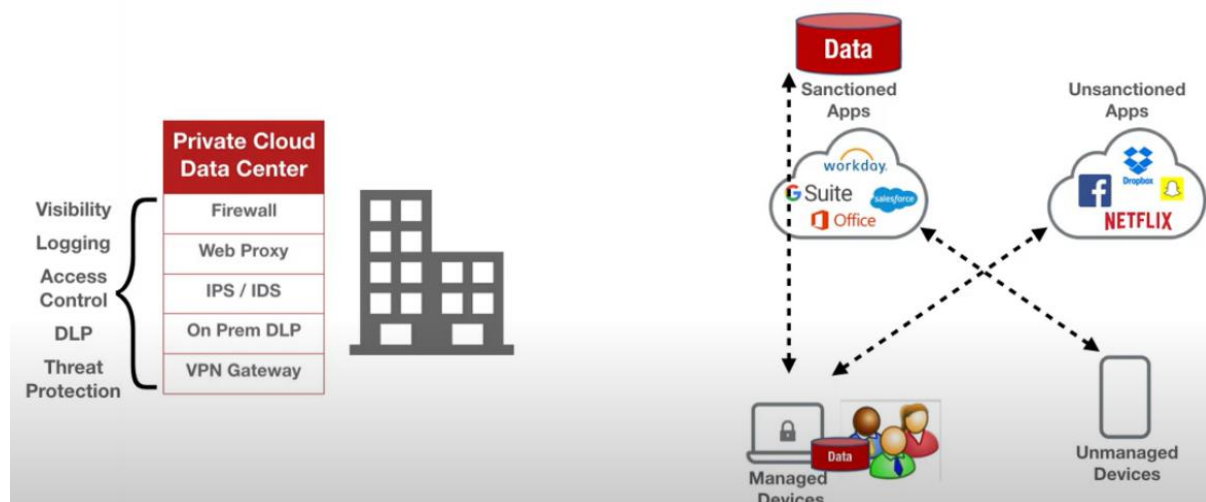


Figure 3: Moving from an on-premises model (left) to a public cloud model (right) increases the complexity of securing services and data

Cloud Access Security Broker (CASB) products help to address these new security challenges from companies moving their data, applications, and infrastructure to the cloud. The key product features of a CASB include [3]:

- **Cloud API Scanning:** CASB solutions use APIs from sanctioned cloud applications to scan them to determine how the data is shared, whether it's publicly accessible and

whether unauthorised data is stored within those applications. Some solutions can also take action based on these API scans, such as removing inappropriate sharing or encrypting the data.

- **Forward Proxy:** A forward proxy uses an endpoint agent or configuration to route access from managed devices to cloud services. This allows unsanctioned cloud applications to be blocked and for access to sanctioned cloud applications to be monitored in real time. The use case for a forward proxy is controlling how internal stakeholders such as employees access cloud applications, so they are only using permitted services and doing so in a way that is compliant with security policy.
- **Reverse Proxy:** A reverse proxy is agent-less and so also controls how unmanaged devices access the company's permitted cloud services. When a valid user or threat actor attempts to access these cloud services, they are redirected to a single-sign-on (SSO) process that can and should include multi-factor authentication.

The strengths and drawbacks of each feature is summarised below:

Security Control	Cloud API Scanning	Forward Proxy	Reverse Proxy
Controls Managed Devices	N/A	Yes	Yes
Controls Unmanaged Devices	N/A	No	Yes
Blocks unsanctioned applications	No	Yes (Managed Devices)	No
Controls access to sanctioned applications	No	No	Yes
Security Action Timing (e.g. block / alert)	Batch / Regular Scan / Reactive	Real-time	Real-time

### 3.2.2 Product Recommendations

I strongly recommend that the project to enable migration of existing on-premises services to cloud service providers be accompanied by a plan to adopt the Proofpoint CASB solution. This solution supports API Scanning, Forward Proxy, and Reverse Proxy features. Proofpoint is one of the minority of CASB providers that caters its pricing model towards businesses with less than 1,000 employees.

### 3.2. Cost Analysis

Recommendation	AIC Concern	Recommendation	Cost
Router Redundancy	Availability	2 X Cisco C1111-4P	3 X €2,000 = €6,000  Total: €6,000 capital expense
Database Redundancy	Availability	AWS RDS Multi-AZ	€2,000 per month =€24,000 per annum
Database Backup		300 GB Storage 5 TB Backup Storage	
Webserver Redundancy	Availability	2 X t3a.xlarge instances	€150 per month = €1,800 per annum

		1 X load balancer	€20 per month = €240 per annum
Proofpoint CASB	Integrity, Confidentiality	400 X enduser licenses @ €15 per licence	€6,000 per annum
TOTALS:		Upfront CapEx:	€6,000
		Annual Recurring Opex	€32,040

### 3.3. Comparative Analysis of at least 2 Enterprise Architecture Frameworks

#### 3.3.1. Topic Introduction

An Enterprise Architecture (EA) is a conceptual model of an enterprise, consisting of multiple diverse documents, or artifacts [4] that together describe the integration of business, applications, data, and technology components. An EA can represent multiple organisational states – the current as-is relationship between the business and supporting IT assets, as well as a future interim or end-state that represents the desired evolution of the business-IT relationship [5]. In this context, EA can be thought of as a deliverable or outcome of an analysis or design process.

The term “Enterprise Architecture” is also used as a description of an analysis and design process. Gartner defines Enterprise Architecture as *“a discipline for proactively and holistically leading enterprise responses to disruptive forces by identifying and analysing the execution of change toward desired business vision and outcomes”* [6]. It’s clear from this definition that this process is not a single point in time exercise, but one where the EA is continuously evaluated in light of changing internal and external forces such as organisational changes, strategy changes market, and competitor changes and changes in the enterprise’s regulatory environment.

The purposes of an EA include:

- Representing the current and future desired vision of an enterprise
- Aligning business strategy and IT strategy within that enterprise
- Supporting business operations with the use of IT in a cost-efficient manner by identifying and removing unnecessary duplication, and promoting appropriate sharing of systems and data [5]

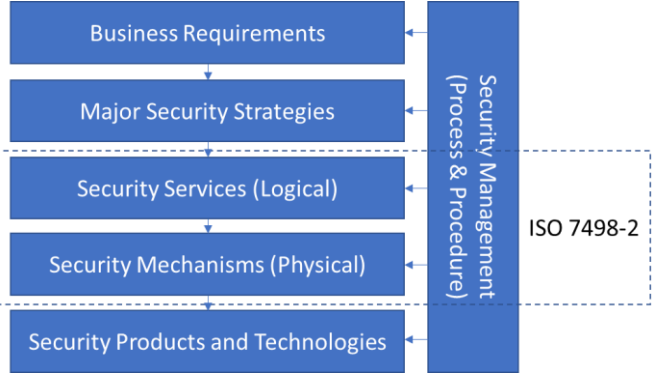
An analogy for EA would be the design of a city. The “architecture” of the city would represent the relationships between the city’s objectives for itself (to be liveable, green, business-friendly), and the infrastructure that supports that through housing, transport, energy, and spatial infrastructure. “Good” architecture understands the city’s articulated objectives and develops policies and plans to support these objectives within the city’s financial and logistical constraints. This process of designing a well-architected city is by nature iterative, as technological, economic, ecological, and societal changes require the architectural plans to be reviewed and adapted. In contrast, the poorly architected city is one where decisions are made without reference to a longer-term vision: services are inaccessible where they’re needed; different parts of the city are not well-connected and investments in the areas of housing and transport conflict with each other.

In an enterprise context, “good” architecture is derived from an excellent understanding of the enterprise’s strategy which is supported by appropriately integrated applications and data flows applied on top of scalable and adaptable IT infrastructure. This architecture is regularly reviewed and adapted to react to both external and internal changes and identified future risks. The poorly architected enterprise is one that struggles to adapt to support the business objectives (if they are articulated at all); where data islands exist that make it difficult to share and exploit that data; and a history of departmental-level tactical investments in IT has resulted in inefficient and costly IT subsystems that are not well integrated. This “*deviation of the currently present state of an enterprise from a hypothetical idea state*” is described by Hacks et al [7] as Enterprise Architecture Debt.

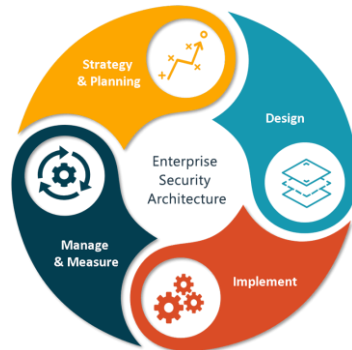
An Enterprise Architecture Framework is the *collection of processes, templates and tools that are used to create an Enterprise Architecture* [8]. Whereas the EA itself is a conceptual blueprint, an EA Framework can be considered as a set of commonly well-understood tools and techniques that help business analysts, architects, and designers to construct that blueprint in a repeatable, standardised way. Participants in an architectural design process executed within an EA framework can share language, artifacts and processes that are rooted in an accepted set of standards and definitions. The popular frameworks in use within industry and government are themselves a distillation of decades of research and experience that EA practitioners can exploit to start with the best-known methods and avoid critical omissions and mistakes when developing an EA.

### 3.3.2. A Comparison of the SABSA and TOGAF Frameworks

	SABSA – Sherwood Applied Business Security Architecture	TOGAF – The Open Group Architecture Framework
<b>Origins &amp; Problem Statement</b>	<p>The SABSA Framework was originally developed in 1995 by John Sherwood as part of the SWIFT interbank transfer project to develop an information security architecture for SWIFT. The framework was a response to several challenges articulated by John Sherwood.</p> <ul style="list-style-type: none"> <li>• Information Security was seen as synonymous with stopping operational evolution. <i>“The corporate information security team was seen... as the ‘business prevention department’. ‘No, you can’t do that, it’s not secure’ was the catch phrase that had earned that reputation in many organisations.”</i> [9]</li> <li>• Information security solutions were often <i>“designed, acquired and installed on a tactical basis”, with “no opportunity to consider the strategic dimension” and “no strategy that can identifiably said to support the goals of the business”.</i> [10]</li> </ul> <p>The SABSA framework is described as a <i>“methodology for developing business-driven, risk and opportunity focused Security Architectures”</i> [11].</p>	<p>TOGAF originated as a generic framework and methodology for development of technical architectures, but it evolved into an enterprise architecture framework and methodology [12]. In 1995, the first version of TOGAF as a comprehensive EA Framework was published by The Open Group. Since its original publication, TOGAF has been updated and refined several times and the latest version of the framework (TOGAF 10) was published in April 2022.</p>
<b>Genealogy</b>	<p>SABSA extended the ISO standard 7498-2 model [13] to address the above challenges by adding a business layer and a strategic layer to embed the need for the security</p>	<p>TOGAF was built originally upon a US Department of Defense framework called TAFIM (Technical Architecture Framework for Information Management). [14]</p>

	<p>architecture to be developed in a business-driven context (see Figure 4).</p>  <p><i>Figure 4: ISO 7498-2 Conceptual Relationships extended to include business and strategy layers</i></p>	
<b>Lifecycle</b>	<p>The SABSA lifecycle consists of four phases [15]:</p> <ul style="list-style-type: none"> <li>• Strategy &amp; Planning</li> <li>• Design</li> <li>• Implement</li> <li>• Manage &amp; Measure</li> </ul>	<p>At the heart of TOGAF is the Architecture Development Method (ADM), a process framework for developing organisation-specific EAs that address the requirements of the business. Within the ADM there are nine phases.</p>

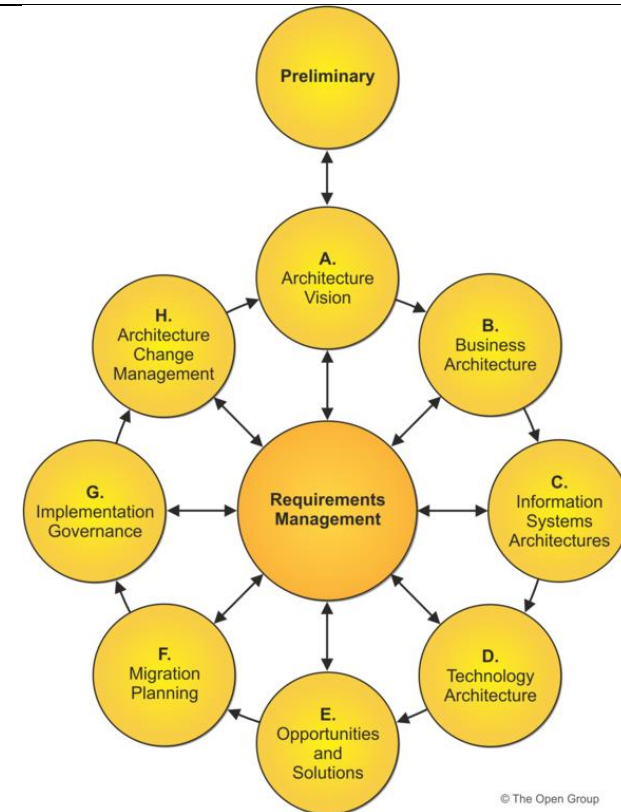




This lifecycle is a Deming circle “Plan-Do-Check-Act” feedback loop that is popular in iterative design and Agile software development methodologies.

In the **Strategy & Planning** phase, the objectives and environment are analysed to identify the risks that might prevent the objectives from being met as well as opportunities that may result from better-than-expected delivery. Appropriate control requirements are then identified. The outcome of this phase is a Security Strategy that includes business capabilities (“attributes”), performance targets, and metrics of performance for those capabilities.

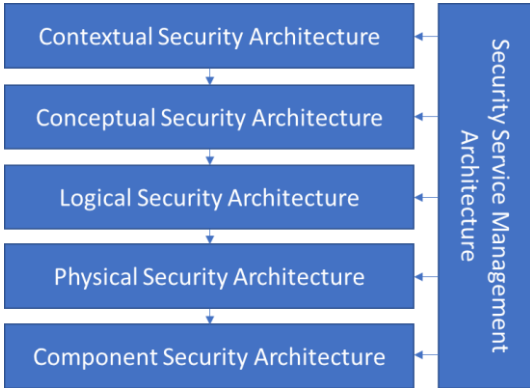
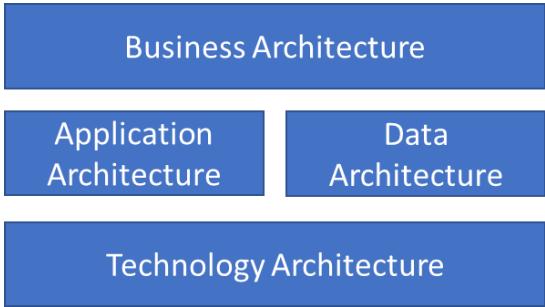
In the **Design** phase, the outcomes of the Strategy & Planning phase are used to create logical representations of the business information and services, determine the best mechanisms to implement these services and design the security management processes in which they will be used. The outcome of this phases are the designs, processes, and implementation steps.



© The Open Group

- The **Preliminary Phase** describes initiation activities needed in preparation for developing an EA that needs business needs. This phase is concerned with bootstrapping the EA team, for example through definition of the organisation model, roles and responsibilities, budgets, constraints and governance. “*The Preliminary Phase is about defining ‘where, what, why, who, and how we do architecture’ in the enterprise concerned*” [16]

	<p>In the <b>Implement</b> phase, the security and risk management controls are developed, implemented, tested and prepared for deployment to the enterprise. Once ready, they are passed to the Service Management operations team to execute and manage on a day-to-day basis.</p> <p>In the <b>Manage and Measure</b> phase, the security performance information is collected to assess the performance of the controls. Based on potential changes in the threat and opportunity environment, risk owners may identify desirable changes to their policies or how the controls are implemented. This triggers another iteration of the lifecycle so the requested changes can be assessed and rolled out.</p>	<ul style="list-style-type: none"> <li>• <b>Phase A: Architecture Vision</b> describes activities needed to develop an aspirational vision of the capabilities and business value to be delivered by the proposed EA.</li> <li>• <b>Phase B: Business Architecture</b> describes the business structure, organisation structure, process flows and what the intended business goals are.</li> <li>• <b>Phase C: Information Systems Architecture</b> focuses on developing application and data architectures needed to support the Architecture Vision.</li> <li>• <b>Phase D: Technology Architecture</b> involves developing the physical and virtual technologies that are needed to underpin the application and data architectures.</li> <li>• <b>Phase E: Opportunities &amp; Solutions</b> focuses on developing an initial architecture roadmap for how the target architecture can be delivered either incrementally or in more disruptive “big bang” roll-outs.</li> <li>• <b>Phase F: Migration Planning</b> finalises the architecture roadmap as well as an implementation and migration plan that is circulated and understood by key stakeholders.</li> <li>• <b>Phase G: Implementation Governance</b> involves ensuring that the implementation projects that underpin the architecture migration are in conformance with the target architecture and any proposed changes are under change control.</li> <li>• <b>Phase H: Architecture Change Management</b> involves ensuring the expected benefits of the target architecture are being achieved.</li> </ul>
--	--	--

		<p>Joining all the phases together is a Requirements Management phases that is continuous with them. Phase H feeds back into the Phase A Architecture Vision in an iterative manner to repeatedly improve on each cycle of framework execution.</p>
<b>Layers &amp; Viewpoints</b>	<p>SABSA defines six layers of architecture change. Each model layer presents a view from the perspective of key enterprise stakeholders in its processes [17].</p>  <p>The Contextual and Conceptual Architecture layers are defined during the Strategy and Planning phases of the lifecycle:</p> <p>The <b>Contextual</b> Architecture layer represents the business view and identifies and captures the business context of the enterprise.</p> <p>The <b>Conceptual</b> Architecture layer represents the architect's view and takes the business context captured in the Contextual Architecture layer to identify the main priorities from an information security and risk management perspective.</p>	<p>TOGAF defines four primary architecture domains: business, data, application and technology.</p>  <p>These look like a lower-resolution view of the SABSA layers with Business Architecture mapping to the Contextual and Conceptual Security Architectures in SABSA; the Application and Data Architectures mapping to the SABSA Logical Security Architecture; and the Technology Architecture mapping to the SABSA Physical and Component Security Architecture viewpoints.</p>

	<p>The Logical, Physical and Component layers are defined during the Design phase.</p> <p>The <b>Logical</b> Architecture layer represents the designer's view. The conceptual deliverables from the Conceptual Architecture are used to create a logic representation of them.</p> <p>The <b>Physical</b> Architecture layer represents the builder's view and selects best data structures and technical mechanisms to implement the logical security service.</p> <p>The <b>Component</b> Architecture layer represents the technician's view and deals with how specific tools, product vendors are integrated into the solution.</p> <p>The <b>Service Management</b> Architecture represents the manager's view and defines all the activities designed to provide assurance, operations and management of the security architecture. This layer is executed during the Manage and Measure phase of the SABSA lifecycle.</p>	
<b>Emphasis &amp; Strengths</b>	<p>A major emphasis of the SABSA framework is on traceability from the top-level business objectives through to components and activities involved in managing enterprise risk. It should be possible to trace the decision to implement a particular control by following the traceability model to information documented at all higher levels of the layered model.</p> <p>The SABSA framework and whitepapers are open source and free to use.</p>	<p>TOGAF is very comprehensively described in the available documentation</p> <p>Documentation is extremely comprehensive and detailed. It is also accessible without the necessity of making a download request from The Open Group.</p>

<b>Limitations</b>	<p>SABSA is not a repository of ready-to-go solutions, but rather a guiding framework that is customisable by enterprise architects to apply in their business context.</p> <p>The whitepapers underpinning the SABSA framework need to be requested from the SABSA Institute and are not freely available online.</p>	<p>Although in theory TOGAF claims to be scalable to any enterprise size, in reality it may be too unwieldy for smaller businesses to implement. It is reported that even larger enterprises take a cut-down view of TOGAF when applying to real-world scenarios used more as guidance than as a prescriptive process. [18]</p>

### 3.3.3. Framework Recommendation

I am recommending usage of the SABSA framework for Greenham House. The principal reason for this is that while TOGAF is the best known Enterprise Architecture standard used in large enterprises, the applicability to small and medium enterprises like Greenham House is consideration of costs and benefits is controversial [19]. The SABSA model is appropriate for smaller business because it *“provides an adjustable and scalable guideline instead of a list of requirements.”* [20]

## 4) Overall Conclusions

Greenham House’s IT infrastructure has been demonstrably vulnerable due to its ad hoc evolution. Security has been an after-thought of the recent breaches that cost the company much time and money. The lack of security consideration is itself a symptom of an absence of proactive Enterprise Architecture planning, or the use of any simple framework such as AIC to identify Information Systems assets, the business needs of those assets, or the risks facing them. As a result, significant single points of failure remain present that pose material risks to business operations if a negative action such as hardware failure, or a further breach of database environments occur.

In moving to the cloud, the company must given parallel consideration to implementation of a CASB solution to help protect cloud assets from inappropriate access, monitor for undesirable behaviour and protect company data from leaking to unauthorised cloud services.

Finally, Greenham House should adopt a formal Enterprise Architecture framework in the form of SABSA to help ensure that future IT development is in line with, and supportive of business objectives.

## 5) Bibliography

- [1] S. H. CISSP, in *All In One CISSP Exam Guide Sixth Edition*, McGraw Hill Education, 2013, p. 22.
- [2] Cisco Systems Inc, "Cisco 4000 Series ISRs Software Configuration Guide, Cisco IOS XE Gibraltar 16.12.x," [Online]. Available: [https://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/xe-16-12/isr4400swcfg-xe-16-12-book/configuring\\_high\\_availability.html](https://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/xe-16-12/isr4400swcfg-xe-16-12-book/configuring_high_availability.html). [Accessed 03 12 2022].
- [3] Skyhigh Security, "What are Proxies," [Online]. Available: <https://www.skyhighsecurity.com/en-us/cybersecurity-defined/what-are-proxies.html>. [Accessed 4 Dec 2022].
- [4] S. Kotusev and S. Kurnia, "Roles of Different Artifacts in Enterprise Architecture Practice: An Exploratory Study," in *Forty-First International Conference on Information Systems*, India, 2020.
- [5] N. E. Hewlett, "The USDA Enterprise Architecture Program," 2006.
- [6] "Information Technology - Gartner Glossary - Enterprise Architecture," Gartner, [Online]. Available: <https://www.gartner.com/en/information-technology/glossary/enterprise-architecture-ea>.
- [7] S. Hacks, H. Höfert, J. Salentin, Y. C. Yeong and H. Lichter, "Towards the Definition of Enterprise Architecture Debts," 2019 IEEE 23rd International Enterprise Distributed Object Computing Workshop, 2019.
- [8] A. S. Gillis, "Enterprise Architecture Framework," TechTarget, February 2021. [Online]. Available: <https://www.techtarget.com/searchapparchitecture/definition/enterprise-architecture-framework>. [Accessed 25 November 2022].
- [9] J. Sherwood, "A Brief History of SABSA: Part 1," The SABSA Institute, 2017. [Online]. Available: <https://sabsa.org/the-chief-architects-blog-a-brief-history-of-sabsa-21-years-old-this-year/>.
- [10] J. Sherwood, "SALSA: A method for developing the enterprise security architecture and strategy," *Computers & Security*, vol. 15, no. 6, pp. 501-506, 1996.
- [11] The SABSA Institute, "SABSA Executive Summary," [Online]. Available: <https://sabsa.org/sabsa-executive-summary/>. [Accessed 27 November 2022].
- [12] M. Lankhorst, in *Enterprise Architecture at Work: Modelling, Communication and Analysis*, Springer, 2005, p. 25.

- [13] International Organization for Standardization, "Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture," 1989.
- [14] The Open Group, "The TOGAF Standard, Version 9.2," 2011. [Online]. Available: <https://pubs.opengroup.org/architecture/togaf9-doc/m/chap01.html>. [Accessed 28 November 2022].
- [15] M. Platt, "What is SABSA Enterprise Security Architecture and why should you care ?," 26 August 2019. [Online]. Available: <https://medium.com/@marioplatt/what-is-sabsa-enterprise-security-architecture-and-why-should-you-care-a649418b2742>. [Accessed 28 November 2022].
- [16] The Open Group, "Chapter 5 - Preliminary Stage," [Online]. Available: <https://pubs.opengroup.org/architecture/togaf92-doc/arch/>.
- [17] H. Al-Turkistani, S. Aldobaian and R. Latif, "Enterprise Architecture Frameworks Assessment: Capabilities, Cyber Security and Resiliency Review," in *2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA)*, 2021.
- [18] S. Kotusev, "Enterprise Architecture Is Not TOGAF," The British Computer Society, January 2016. [Online]. Available: <http://www.kotusev.com/Enterprise%20Architecture%20Is%20Not%20TOGAF.pdf>.
- [19] R. Alm and M. Wißotzki, "TOGAF Adaption for Small and Medium Enterprises," *Lecture Notes in Business Information Processing*, vol. 160, 2013.
- [20] R. Yudhiyati and A. Putritama, "What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case," *Journal of Information, Communication and Ethics in Society*, vol. 19, no. 4, p. 1, 2021.
- [21] Oracle, "Using Oracle Database Backup Cloud Service," Oracle, [Online]. Available: <https://docs.oracle.com/en/cloud/paas/db-backup-cloud/csdbb/oracle-database-backup-cloud-service.html>. [Accessed 3 December 2022].