SECURITY AUDIT SCOPE GUIDELINE (NON INTRUSIVE)

Scope guideline

Date: 18/07/2019

Do the below keywords ring a bell?

- Disrupted elections
- State-sponsored attacks
- Ransomware
- International bank heists

Most likely they do, as most of us have read about these in the past few months with the intensity and sophistication of cyber crimes on the rise. Here are some statistical data to help us understand the depth of what is at stake and how big a problem it is.

$6 trillion	$1 trillion	3.5 million	4 billion	$11.5 billion
Annual cyber crime damage costs by 2021	Cybersecurity spending from 2017 to 2021	Unfilled cybersecurity jobs by 2021	People online worldwide by 2020	Predicted global ransomware damage by 2019

Regulatory authorities expect all companies small and big to do more to protect their systems and data, and now penalise them if there is evidence that enough steps were not taken by an organisation to prevent a hack which caused a data leak.

We at sapna security understand that

- security can be daunting for both small and big companies
- organisations may not know what they are expected to do
- huge costs may keep them from conducting security audits

Accordingly sapna security attempts to offer security assistance at reasonable price to match your needs.

For non intrusive security audit we have a team which has experience over several years in web programming, database, network architecture, server hosting, security audits, and security testing. Our Assessment approach, our findings will ensure you get a detailed idea of the issues. We will be available for help and discussions at each step.

1. Our Assessment approach

Data classification

	Public/Unrestricted	Sensitive/Confidential	Internal	Trail-log/ modification-restricted
Definition	Data that may or must be open to the general public. No specific controls are required to protect this data, although some control might be required to prevent the unauthorized modification or destruction of data.	All sensitive Data required to be kept confidential as per law is considered sensitive and confidential. Extra controls need to be put in place to ensure the data is protected from unauthorised access. This includes PII data. Protection methods including hardening of devices on which this information is stored, encryption during storage, and/or transport. Staff training is required to ensure this information is always treated as per the ICO guidelines of data protection.	Internal data is all the information internal to the working of MFC. This may contain information sensitive to the business. This information is neither public nor sensitive, and MFC may choose to decide if it wants to reveal this information or not.	Data which includes logs of events, etc. for which special controls have to be put to ensure data is not modified.
Justification	Some information should be freely available to public for ease of access.	Some information required to be shared for the purpose of business may contain sensitive personal information. Releasing such information should be vetted and only the necessary data should be shared.	Some information should not be share with anyone outside the organization and should be restricted only to the authorized group of users. Sharing of this information may cause harm to the business.	This set of data is useful for audit purpose for analysing any security event, and hence should not be modified. The integrity of this data is important.
Examples	Articles, Blogs, Marketing Material	PII data	Business roadmap, Financial Data	Audit trail
Consequence of Public Disclosure	No adverse consequence	Loss of trust, Loss of reputation	Loss of business	Loss of trust

Data classification is the process of organizing data into categories for its most effective and efficient use. A well-planned data classification system makes essential data easy to find and retrieve. This can be of particular importance for risk management, legal discovery, and compliance.

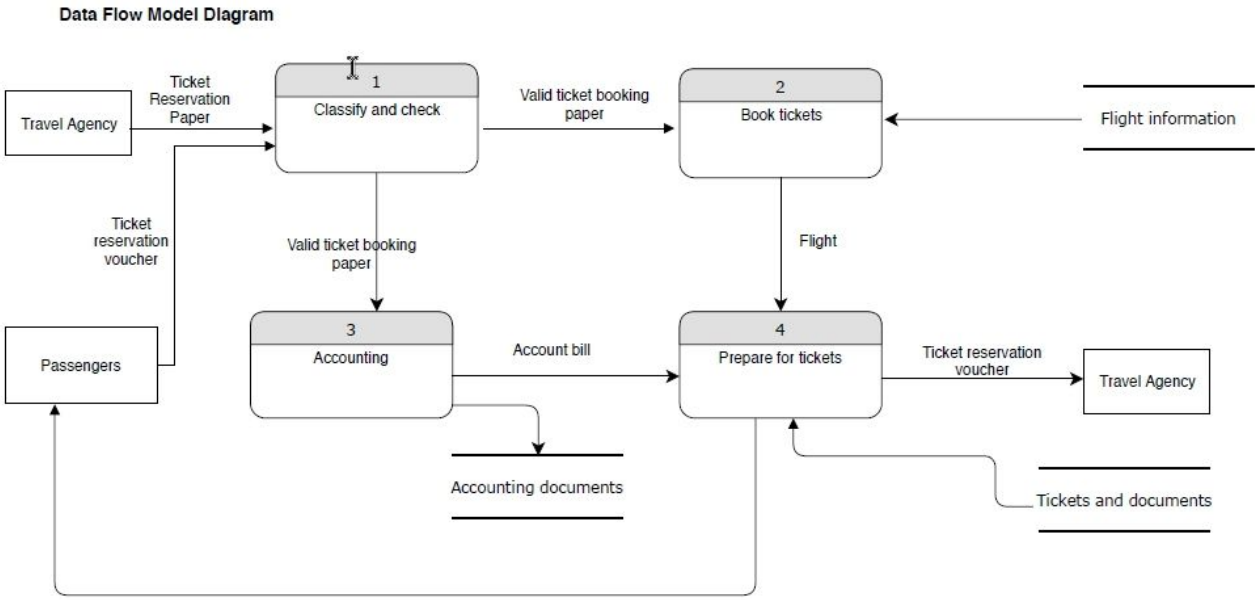
Supplier/Processor list

See below a small snapshot of a demo supplier/processor list.

Name of supplier/processor	Contact name, email id, phone	Used by (exporter)	Service type	Type of processing activitie	purpose of processing activiti
Sapnagroup	Jonny Hubner, jonny@sapnagroup.com Nilesh Nayak, nilesh@sapnagroup.com Anurag Jain, anurag@sapnagroup.com hello@sapnagroup.com Contact number: +44 1737 887808	Sapnagroup services	Web service	Software development/Server	to be able to develop and mainta client
Hetzner	Email: info@hetzner.de Tel.: +49 (0)9831 505-0	Sapnagroup services	Web service	Server ISP	
Hetzner	Email: info@hetzner.de Tel.: +49 (0)9831 505-0	Sapnagroup services	Web service	DNS	

It's important to keep a list of all your suppliers/processors, and check what data exposure they have. This is to important as you have a complete picture of how your data is shared, and you can minimize risk by reducing the exposure if needed. This also forms the basis for data flow diagram.

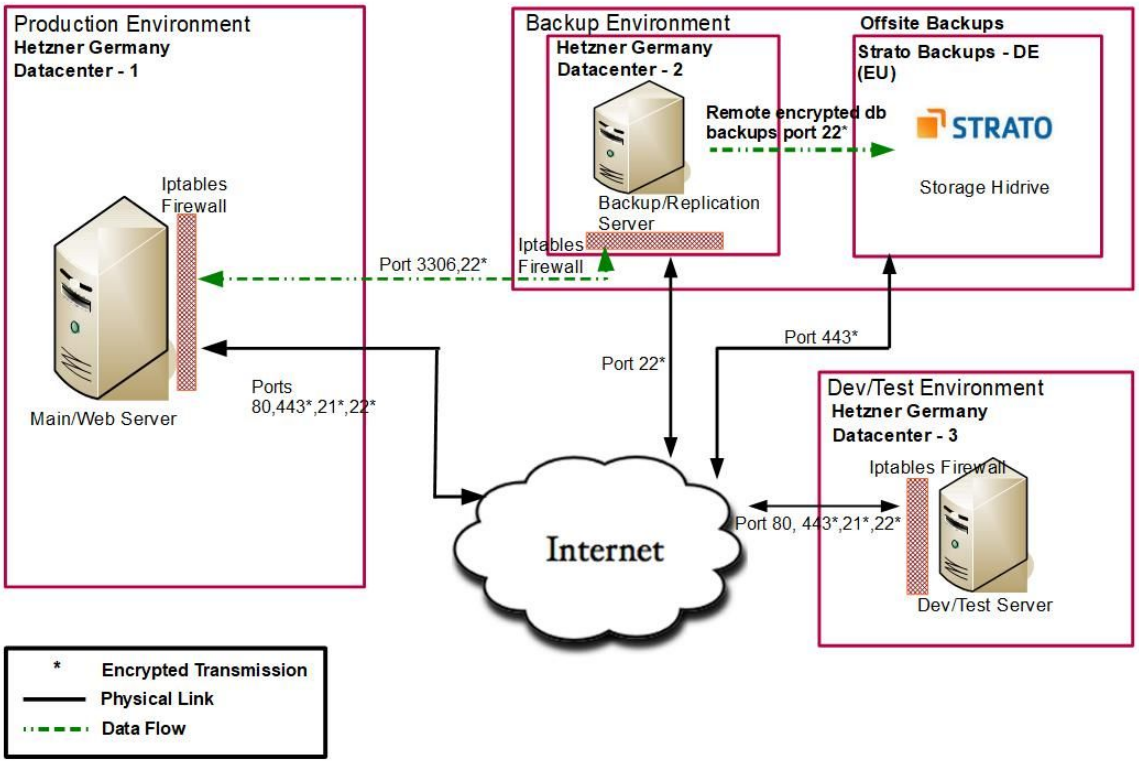
Data flow diagram



Data flow diagrams (DFD) are used to graphically represent the flow of data in an information system. DFD describes the processes that are involved in a system to transfer data from the input to the file storage and reports generation to end user. It gives an overview of the entities that interact with the system and the processes linked with it. Like all the best diagrams and charts, a DFD can often visually "say" things that would be hard to explain in words, and they work for both technical and nontechnical audiences, from developer to CEO.

Network diagram

A network diagram is a visual representation of a systems network or telecommunications network. It shows the components that make up a network and how they interact, including routers, devices, hubs, firewalls, etc. A logical network diagram also describes the way information flows through a network. This is useful to understand the way the data flows through the different components in the network and how it can be secured.



Security audit fact finding

Our team of experts will first set the scope of the assessment, and then meticulously go through various security fact finding like checking your password policy, to checking the infrastructure. We will need your support during the entire phase as this covers the application in scope and also the operation team you may have to support the application.

Advanced security audit is also available, which is more rigid, and requires us to collect evidence to confirm standards are being met.

The security audit fact finding includes the following areas:

Application security: This section focuses on application development and application security. Fact finding is done on a range of issues including software development lifecycle process, encryption technologies used in the application, use of 3rd party software etc. Having resolved issues in this section increases your application security and limits exposure of your data through the vulnerabilities in the application.

Data security: This section focuses on how your sensitive data is used in your system. This uses the DFD diagram as a basis as well, and checks if eg live sensitive data is being used in test environment, or how backups are done and secured. Having resolved issues of this section increases the way data is stored and transmitted, limiting leaks and exposure.

Infrastructure: This section focuses on the network and infrastructure both at local premise and online where your application is hosted. Physical firewall, Security patches, disaster recovery etc are checked. Having resolved issues of this section reduces your data leaks across the network.

Access Management: This section focuses on the users in the system and the access controls available. From how users are added or removed from the system, review controls, to password policies, we go through various checklists to ensure your sensitive data exposure to end users is evaluated. The supplier/processor list is an important part of this evaluation. Having resolved issues of this section reduces your data exposure to unwanted entities.

Monitoring and Logging: This section focuses on the various logging activities happening in your application and infrastructure and the kind of monitoring done on them. This also includes security of these logs. Having resolved issues of this section help ensure evidence gathering is possible in a security incident event.

Organisational Policy: This section focuses on the organization's processes, procedures and documentations. From security policies including email or internet usage policy, to communicating these to the employees, to audits being conducted. Having resolved issues of this section reduces data exposure by human errors.

2. Our assessment findings and recommendations

Our assessment findings and recommendation are presented in the form of a risk register. Risk register helps in risk management where the objective is to identify risks, assess threats, control risks, and review risks. The risk register shows details of individual risks. The following are required

- Area: Generic area with which risk is associated with
- Owner: Risk Owner is the person(s) responsible for managing risks and is usually the person directly responsible for the strategy, activity or function that relates to the risk
- Risk description: Should clearly describe the event/cause and the result
- Risk status (Probability/Impact/Overall/Acceptable)
- Existing mitigating actions
- Future mitigating actions: Actions planned, owner responsible, due date

Below are sample findings and recommendations chart.

Company:			L	likelyhood of the risk occuring (1 - Very Low, 5 Very High)			
Date:			C	consequences of the risk occuring i.e. damage to the company (1 - Very Low, 5 Very High)			
Document owner:			R	Risk = L*C			
Risk Register							
ID	**Area**	**Description**	**L**	**C**	**R**	**Existing mitigation**	**Plan**
1	Network	No Physical firewall used. Physical firewall add an extra layer of protection in front of the network.	4	5	20	IPtables firewall in place	
2	Hardware	MySQL database should be on another dedicated server. This is to follow 3-Tier architecture	4	4	16	None	

3. Risk register evaluation and risk scoring

Risk traffic light scoring

Risk is characterised and rated by

R (Risk status) = L (likelihood/probability) x C (consequences/impact)

The traffic light scoring helps us focus and put risks in different groups based on the score. We assign a risk status so that risks can be prioritised. A high impact high likelihood risk should be given more attention than a high impact low likelihood risk;

Probability						
Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)		Impact
Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)	Very High (5)	
Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)	High (4)	
Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)	Medium (3)	
Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)	Low (2)	
Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)	Very Low (1)	

Risk probability

Probability of the risk actually happening

- Very low (0-5% - extremely unlikely or virtually impossible)
- Low (6-20% - low but not impossible)
- Medium (21-50%) fairly likely to occur
- High (51-80% - more likely to occur than not)
- Very high (81-100% - almost certainly will occur)

Risk impact

Impact on the company if the risk does actually arise

- Very low (is expected and can be managed through already approved operations)
- Low (likely to have a minor impact to the organisation)
- Medium (requires intervention to manage and resolve)
- High (will have a significant impact on the operations of the company)
- Very high (severely impairs the ability of the company to operate)

4. Next steps

While our security audit gets completed with the risk register report we pass you, we will also arrange a discussion on the risk register where security audit team will go through the report with the client team to explain the issues, and answer any queries the client team might have.

You can always hire us to oversee the risk register and help close issues and evaluate on an ongoing basis. This helps in lowering your risk exposure and help evaluate new risks as they come into the system.

We also highly recommend an ethical hack on your application by our vulnerability assessment team. This is an intrusive additional security assessment and helps identify issues which the non intrusive security audit cannot evaluate. Please contact us at info@sapnasecurity.com for more information.