Azure Security Review

Confidence in your Security | Controlling spend | Keeping up

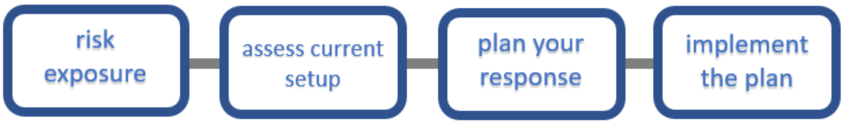
On a regular basis we are helping organisations, which may even already have ISO27001 accreditation, to identify and mitigate considerable security risk. A badge isn't enough if you want to protect your organisation – through this review you will receive expert, frank feedback and practical advice on the steps you can take to reduce risk and, very often, considerable cost all at the same time.

There is no one-size-fits-all for security, nor is there a single-fix product you can buy that solves it all. It is easy to think you are protected when you are not – and it is easy to pay too much for unsuitable products and tools. We will help you determine what is the most appropriate set of tools and approaches for you and we will help you implement them.

Through this process, we will use the below matrix to build your plan from:

	External Actors	Internal Actors
Prevent	*How do we keep relevant external actors out of the system?*	*How do we prevent internal actors from accidentally or maliciously leaking data?*
Detect	*How do we know if an external actor is attacking the system right now?*	*How do we know if internal actors access data they shouldn't be?*
Mitigate	*How do we reduce the impact of a successful attack?*	

Our process goes through the following steps:



risk exposure

assess current setup

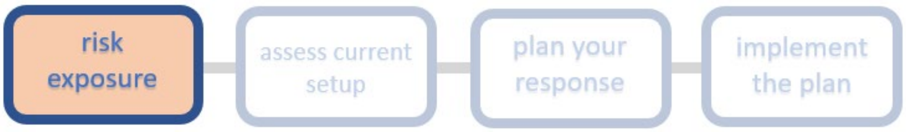
plan your response

implement the plan

1. Determine your risk exposure.
2. Understand your current setup.
3. Plan a suitable response based on your specific situation, taking into account your risk level and where you are today
4. Help you to implement the plan.

Each step is outlined in more detail below, with example questions. We will ask you many more questions during the consultation. Do bear in mind that many of the questions are over the top for many scenarios; we will evaluate the appropriateness with you based on your specific context.

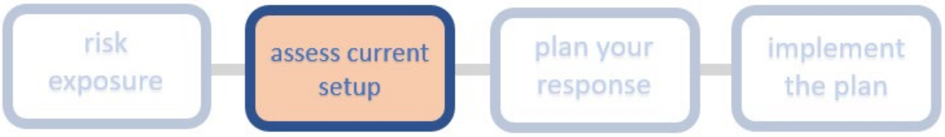
Exposure



What obligations are on you? What is the real risk to you and your customers?

	Data Breach	Denial of service
Contractual	*What do you have in your customer contract or terms of service?*	*What is your SLA?*
Legal (incl. GDPR)	*What types of data do you store on how many people?*	*Would the system being down have an impact on your GDPR obligations?*
How interesting a target are you?	*Is your data valuable in itself? To whom? Is there a ransom value?*	*Do people have reason to want to hurt you? Is there a ransom scenario?*
What kind of actors are likely to want to attack you? **(from drive-by up to state actor).**	*Similar questions to above.*	*Similar questions to above.*
What would the real-world consequence of one of these types of attacks be for…		
Your customers		
You		
Users and/or subjects of the system		

Current situation



risk exposure

assess current setup

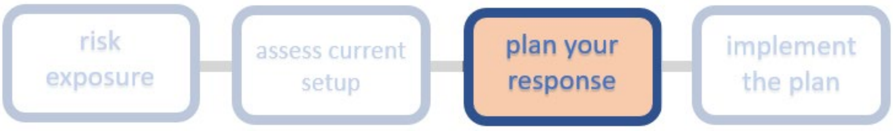
plan your response

implement the plan

Area	Example questions
What is your application architecture?	• How does it segregate data? • How well does it cope with spikes in usage?
What does your infrastructure look like?	• How is the system hosted? • How does authentication between the sub systems work? • Is there network segregation? • Is there message authentication? • How is your CI/CD pipeline protected and monitored?
What is your code like?	• What languages and frameworks do you use? • How old is the code? • How confident are you in the security of the code? • How confident are you in the security skills of your development team?
What monitoring do you have in place?	• Application trace logs? • An APM tool? • Any automated base lining, monitoring or alerts?
What processes do you have in place?	• How do you control who in your organisation has access to what data? • Do you have a way to check that? • Do you know if and when people in your organisation access data from the system? How? • Do you have an ISMS or similar in place?

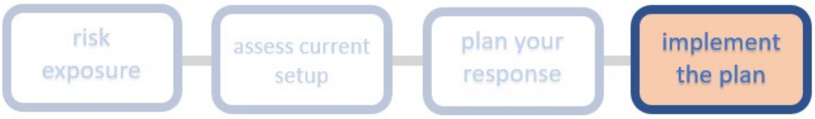
Plan

We will fill this in with the specific initiatives that are appropriate to your scenario.



	External Actors	Internal Actors
Prevent		
Detect		
Mitigate		

Implement



NewOrbit can help you to implement part or all of the plan:

- help you deploy and configure a range of Azure tools, monitoring and alerts.
- advice on the kind of internal processes you may need to implement and how they can be supported by Azure tools.
- ongoing service to monitor your logs and respond to alerts in order to detect attacks.
- potentially even become your Azure Cloud Services Provider, as an ongoing partner, to help you monitor your systems and infrastructure, advise on contractual security requirements, on an ongoing basis, and help you stay current.
- having reviewed the market over the last 10 years we also have selected partners to assist with both manual and automated pen-testing, etc if needed.

Contact us
to gain confidence in your system's security

Get in touch