IS YOUR BUSINESS SECURE? A CYBER SECURITY MATURITY CHECKLIST

www.dig8ital.com

dig8ital

Contents

How to use this guide 3
1 Contextual Layer: The business view 4
2 Conceptual Layer: The architect view 5
3 Logical Layer: The designer view 6
4 Physical Layer: The builder view 7
5 Component Layer: The tradesman view 8
6 Operational Layer: The service manager view 9
Measure your maturity 10
Need help? We're here for you 10

How secure is your organization from cyber threats? And not just threats coming from outside the company – but also, potentially, from within.

The larger the enterprise, the harder it is to answer this question. That's why we've produced this maturity checklist to hand you the secrets of professional security architects and help you measure your own cyber risk exposure.

What is security architecture? Security architecture is like regular architecture, but for cyber security. It is a process that involves breaking down the business into its base components, determining where costs and revenues come from, identifying key threats, and building and implementing mitigation strategies with new security services - like drawing a blueprint for a house, it draws a blueprint for a more secure organization.

How to use this guide

This guide has been designed as both a checklist and set of instructions. For **organizations further along in their maturity**, it is an opportunity to compare what you have and have not yet implemented. For those **beginning their journey for the first time**, it will act as a list of best practices to follow to start implementing better security *straight away*.

Take your time and walk through each phase of the security architecture process using this checklist to guide you, ticking off items that you've already completed and marking ones that you have not. Repeat this for each business unit in your organization, working with key stakeholders in those areas for their expertise and opinion.

Each line in the checklists will give you a point. At the end of this guide, you can tally up your total to help determine your current risk exposure. Any line item that you haven't yet implemented gets a score of 0. **Additionally, items that you might find difficult and for which you may need help from a security architect *have been marked in purple***.

This is a general guide only. Because your business is unique, your final score here may not fully align with the reality of your organization. After tallying your points, we would encourage you to compare the final score with your organizational risk appetite and policies to help you consider it against your individual threats.

1

Contextual Layer: The business view

In the contextual layer, also known as the business view, we're determining goals and objectives to produce our organizational 'as-is' state – this is where the business is now, and it will act as a benchmark to measure future development.

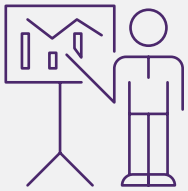
Objective	Y/N?
Brainstormed and built an org structure chart that takes into account not only business units, but also HODs and chain of command.	
Threats and opportunities can come from anywhere, from the smallest to the largest business unit. Therefore, it is vital to establish a visual guide to the business to ensure you can view at-a-glance its many components as well as who 'owns' them.	
Established goals and objectives of each business unit as they pertain to the wider organizational strategy.	
Nothing works if there's no strategy to it. Here you are identifying clear goals for each unit and relating them to the wider organizational mission to make sure they are aligned.	
Determined business drivers for each business unit.	
Business drivers are key inputs and activities that either drive revenue or reduce costs. I.e. 'number of products sold' or 'raw material costs'. Click here to learn more.	
Produced a list of high-level threats for each business unit.	
These are 'high level' threats - we aren't digging deep, but looking at wider industry trends, changing customer habits, national or global economic factors. This is a zoomed-out view of the business's threats.	
Produced a list of high-level opportunities for each business.	
This is the same step as above, except for opportunities - potential areas of improvement or expansion, new customer opportunities, and so on.	
Total:	

KEY TIP

Remember to keep everything in this layer at a high level. We want to zoom out and view the entire organization, its components and its people. We're looking at general threats and opportunities in the market, not digging deeply into the business for specific threats to specific drivers. That will come later!

2

Conceptual Layer: The architect view



In the conceptual layer, known as the architect view, we are transferring all this high-level information into a roadmap to success built out of key milestones. This helps us figure out where our desired state is - so we know the gap between where we are now, and where we want to be.

Objective	Y/N?
Sat down with department managers and other key stakeholders to brainstorm a list of business attributes.	
Business attributes are traits - written as adjectives - that describe the key metrics for success of your people, processes and products (broken down by individual business units). E.g. "On Time", "Future Proof" or "Accessible". Click here to learn more.	
Clearly defined each business attribute and determined how it can be measured.	
Anyone must be able to look at a business attribute and understand its intent - so each one has to be clearly defined in one or two sentences. Additionally, as metrics of success, they must be measurable.	
Established which business attributes depend on which others across the entire enterprise.	
It's rare that attributes work alone. Usually they depend on those from other departments - for example, good customer service will undoubtedly rely on smooth logistics.	
Asked department managers and other key stakeholders what they want to achieve.	
What are their future goals? Where do they want to take their department? This can help you build out your desired state using on-the-ground expertise.	
Reviewed current security policies to see what exists, and what needs improving.	
Identify what security policies you already have in place, and what they cover. Are they still relevant? Anything that is no longer fit for purpose must be updated.	
(If there are no policies) Added the creation of these to the top of the architectural roadmap.	
A lack of security policies is a big red flag. The creation of these will go to the top of the to do list when we come to the later phases.	
Have built a service catalogue of the services your enterprise has in place and how they operate.	
Knowing your key service streams and their pipelines is a critical step to being able to plug security gaps later on, or to identify potential opportunities. If you feel you are missing key services based on your new goals and drivers, make a note of these for now.	
Have combined the above information to generate milestones and desirable timeframes for improvement.	
The purpose of this exercise is to create a roadmap, which must include ideal timelines for improvement. We will return to this roadmap in the future as we identify new priorities.	
Total:	

KEY TIP

Research is vital to success in this layer. You must speak with key people across the business by hosting interviews and workshops to get accurate, up-to-date information from the people who know best.

3

Logical Layer: The designer view

In the logical layer, known as the designer view, we want to pull together our as-is and desired states and turn them into hard, well-defined policies and analyses. This guidance, and the data we'll generate, will form the bedrock of the lower layers.

Objective	Y/N?
Created well-defined policies for key security domains.	
You already know the gaps in your current policies, so it's time to fill them. This is where you will dig deep and fully articulate your expectations around everything security related. Think access levels, password protocols, hardware updates, rules for third-party vendors, and so on.	
Produced information flow diagrams about how information is communicated within the business.	
Information flow diagrams depict how each business unit is connected, how they depend on each other, and the data that flows between them.	
Performed a threat analysis on every business attribute across each business unit in the organization.	
Each business attribute has its own set of threats - whether from outside or within the organization. What poses a risk to your attributes? What could harm them?	
Performed an impact analysis on threats across the business to determine priorities.	
An impact analysis compares threats together to see which are more likely, which are more harmful, and which are both. This allows you to prioritise threat mitigation strategies in the lower layers.	
Built an inventory of information assets.	
If an asset produces or holds data, it must be accounted for in a central, easy to navigate register. Every asset of business data must be listed.	
Produced post-workshop reports from key stakeholder meetings in previous architectural layers.	
All of the discussion generated in previous stakeholder workshops could be vital. Consider what was achieved in these sessions, the conclusions you came to, and so on.	
Total:	

KEY TIP

When prioritizing threats based on their potential impact, you can change the order of priority based on individual business units or across the entire organization - depending on how you want to tackle them later. And don't forget your third-parties! They too pose a threat, and have threats of their own that might impact you.

4

Physical Layer: The builder view

Now that we have come to the physical layer, or the builder view, we are starting to turn strategy into action. Here we'll build control strategies and figure out how to close identified security gaps.

Objective	Y/N?
Have chosen an existing or have defined your own security architecture framework to follow.	
A framework is a bit like this checklist itself - a guide of best practices to follow, when to implement them, and tips to ensure success. Each department can follow one framework, or use a different one depending on its needs.	
Identified control strategies that will work to mitigate threats as found in the previous layer.	
With threats identified, now you can consider what methods - known as control strategies - will help to reduce the impact or likelihood of those threats.	
Created an asset and risk register consisting of all the information gathered above for this layer's security controls.	
By collecting all of the information you have within each business unit pertaining to its assets and risks, other business units may be able to use this information to help them with their own strategies.	
Create a set of patterns, reference architectures and blueprints that can be followed by security departments across the business.	
Sometimes, having a set of references to follow can be helpful to ensure security alignment across the business. Creating these references, patterns to follow, and example architectures will help guide potentially disparate teams to a singular goal.	
Created an awareness campaign and accompanying training sessions to build a better cyber-aware culture.	
Staff tend to be the biggest security weakness in any organization. Building awareness of identified threats and training people on their role in mitigating them will help reduce the chances of a costly mistake.	
Total:	

KEY TIP

Control strategies can be technical or non-technical. For example, new security services don't just have to be tools or technology, but could be about incorporating security into HR policies, defining employee access levels, and so forth.

5

Component Layer: The tradesman view

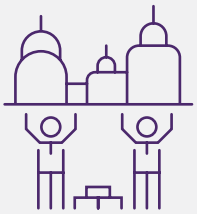
In the previous layer, a number of security control strategies were devised. In this layer, those strategies will be implemented.

Objective	Y/N?
Added control strategies as milestones on the roadmap.	
It's time to revisit the roadmap and add all of these new control strategies as milestones. Be aware - this layer can take years, depending on the scope.	
Prioritized the implementation of control strategies based on threat level.	
New security services should generally always be implemented in order of priority. That way you are using your budget in the most efficient way, and closing the potentially deadliest gaps faster than those which are less important.	
Created a system to investigate the root cause of a problem, in the event a control strategy doesn't fit into place.	
Sometimes you will see controls that don't seem to fit, something is lacking, you don't know where to begin. Look for the root cause of the problem to determine if someone is not following the new rules, if there's a procedure lacking, or the wrong training is in place.	
Total:	

KEY TIP

In this phase we start to see even more value from our process of building an org structure, identifying drivers and defining business attributes. Everything must be traceable back to the business's goals - goals drive all the lower layers, like this one. Because we have that information clearly defined, we can look for services that will help us achieve our goals (i.e. we may not need the latest tools that another company would, because they don't service our unique business goals).

6



Operational Layer: The service manager view

The ultimate goal of any security architect is to get to a point where they are no longer needed. It is far more efficient for any business to be able to build their in-house expertise up so that key stakeholders can take over their own departments and operate their framework independent of a third-party expert. This can be your goal too.

Objective	Y/N?
Department managers are well-informed of the new changes and why they were implemented.	
Awareness is the first step to acceptance. If HODs understand why this process has been followed and why the new changes are being implemented, they can turn into champions of future change and will be more enthusiastic about operating the implementation.	
Developed a system to monitor changes in order to look for further improvement.	
The world will not stop changing just because you have completed this checklist. You need a system in place for architecture owners to be able to monitor their KPIs (as defined earlier) and look for areas of future improvement using this same checklist.	
Department managers have been thoroughly trained in the architectural process and understand the what, why and how of each layer.	
While this checklist has helped you today, it can also help your future architecture owners. If they understand how to implement best practice security architecture, they can revisit this process time and again to iterate, improve and stay ahead of threats.	
Department managers feel comfortable taking over the architectural process from now on in order to improve their own departments moving forwards.	
It's one thing to build awareness and key skills, but another entirely to build comfort. You will need to sit down with key stakeholders however many times is necessary to walk them through taking over this process and check in with them to see how they are progressing.	
Total:	

KEY TIP

Change management is critical to the success of this layer. People are generally inherently resistant to change. By building awareness piece by piece, communicating openly and frequently, and asking for feedback at critical stages, you can help smooth some of that resistance by turning people into change champions. Thankfully, by utilizing key stakeholders throughout the architectural process (i.e. in our workshops), you will have already introduced a variety of your peers to the concept and its purpose.

Measure your maturity

If you've been through this entire checklist, you will have an idea as to your current gaps and where you need to go. Each line in this guide gave you a score of either one or zero. Go back through each of the chapters and count up how many points you scored and refer to the table below to get your final Maturity Level.

Layer	Total
1. Contextual Layer: The business view	
2. Conceptual Layer: The architect view	
3. Logical Layer: The designer view	
4. Physical Layer: The builder view	
5. Component Layer: The tradesman view	
6. Operational Layer: The service manager view	
Final total:	

Score	Risk exposure*	Result
26-31	Low Risk	Your organization has entirely or mostly secured itself from its identified threats.
16-25	Medium Risk	Some priorities have been tackled, but you have more work to be done urgently to secure your gaps.
0-15	High Risk	Your business is at risk. Its gaps have either not been identified or not filled, increasing the chance you will fall victim to a cyber threat.

*Remember to compare your risk exposure here with your risk appetite and security policies.

Need help? We're here for you

There are many lines in this checklist that will be difficult to achieve on your own – especially if you're already time-poor. However, they're still absolutely vital if you are to completely secure your business and mitigate the chance that a high-impact threat will strike your company.

This is where dig8ital comes in.

We have vast expertise in the latest cyber security trends, including the evolving threat landscape and changing government legislation. Our security specialists have worked with some of Europe's biggest brands across sectors, and we're ready to help you, too.

To learn how we can help you build a modern security architecture framework,

contact us today for a free consultation.

W: dig8ital.com
E: contact@dig8ital.com

dig8ital