Data Sheet

DTS SOLUTION
CYBER SECURITY REDEFINED

Cyber Security
Risk and Maturity Assessment

DTS Solution's Cyber Security and Risk Maturity (CSRM) service measures the effectiveness of the process that support cyber security and improve these consistently over time, ensuring a proper focus on cyber security over time, not just waiting for the next crisis.

Cyber security maturity is one area that is often overlooked by organizations. Maturity in cyber security is an underestimated discussion point, assessing the organizations maturity in the discipline of cyber security and cyber risks is paramount due to its very on-going, continuous, evolving nature.

Cyber Security and Risk Maturity (CSRM) is an attempt to measure the effectiveness of the process that support cyber security and improve these consistently over time.

It is a model to ensure a proper focus on cyber security over time, rather than waiting for the next crisis to sharpen our focus.

It is an attempt, in short, to ensure that cyber-security is approached with the same discipline and professionalism as other aspects of company operations, and to ensure that it receives the same level of executive focus on an ongoing basis.

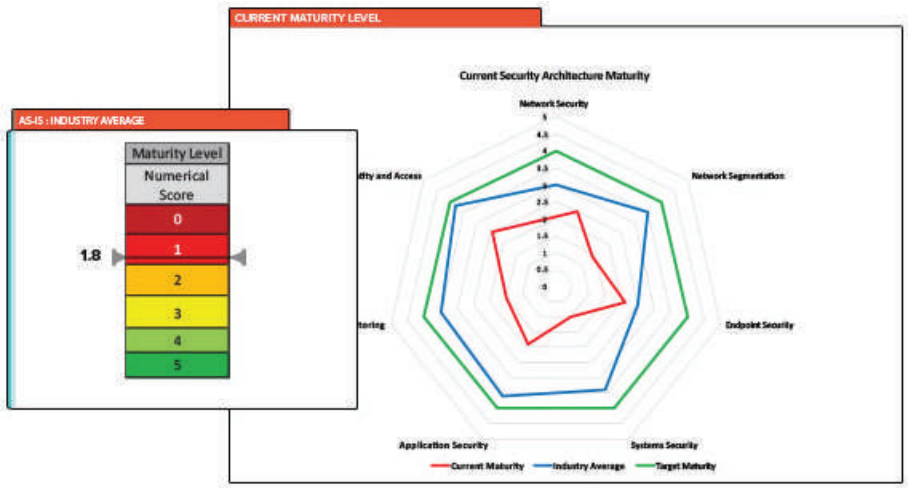
DTS Solution can establish the **cyber security and risk maturity** of your organization by conducting a detailed exercise and can support you in putting that framework together that will ensure your maturity is reviewed on an annual basis to support your continuous improvement plans.

There are some well-established risk maturity frameworks introduced such as the FFIEC for the Financial Industry (adopted by some central banks across the world), Fair Institute and alike and our approach would be to take these frameworks into perspective.

It is important to note that **cyber security and risk maturity** should be aligned to your inherent risk profile, without which the maturity assessment would not be very accurate. It is fundamental that organizations know their risk appetite and risk profile as the required or target maturity would be proportionate. As an example, an organization that has a high-risk profile due to a large attack surface, highly exposed user environment and faces constant cyber-threats would need to have a very high level of cyber maturity. This, compared to an organization with a low risk profile, little data to protect and not facing many security incidents would require a lower level of maturity.

During our **CSRM assessment** we would first identify your inherent risk profile, identify you target maturity levels across various different security domains and then perform the maturity assessment across these domains against the target that has been identified.

Information Security Standards such as **ISO27001:2013, NESA IAS, Dubai ISR, SAMA, NIST CSF** are all great frameworks to establish cyber security within your organization but little is mentioned or covered around building maturity. You can be compliant to a security control mentioned in ISO27001:2013 such as establishing a procedure to control against malware which would make you compliant from a standards perspective. But the question that should be asked, is if the procedure is effective, measured and monitored, well known across the different audiences, tested and verified etc. to really know the level of maturity.



DTS SOLUTION
CYBER SECURITY REDEFINED

DUBAI: Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
T: +971 4 338 3365 | **E:** info@dts-solution.com

800 HACKED

ABU DHABI: Office 253, Al Bateen C6 Tower - Bainunah, King Abdullah Bin Abdulaziz Al Saud Street | **T:** 971 2 2076777
LONDON: 160 Kemp House, City Road, London, EC1V 2NX, United Kingdom | **T:** +44 2081230 387 (DTS)
www.dts-solution.com