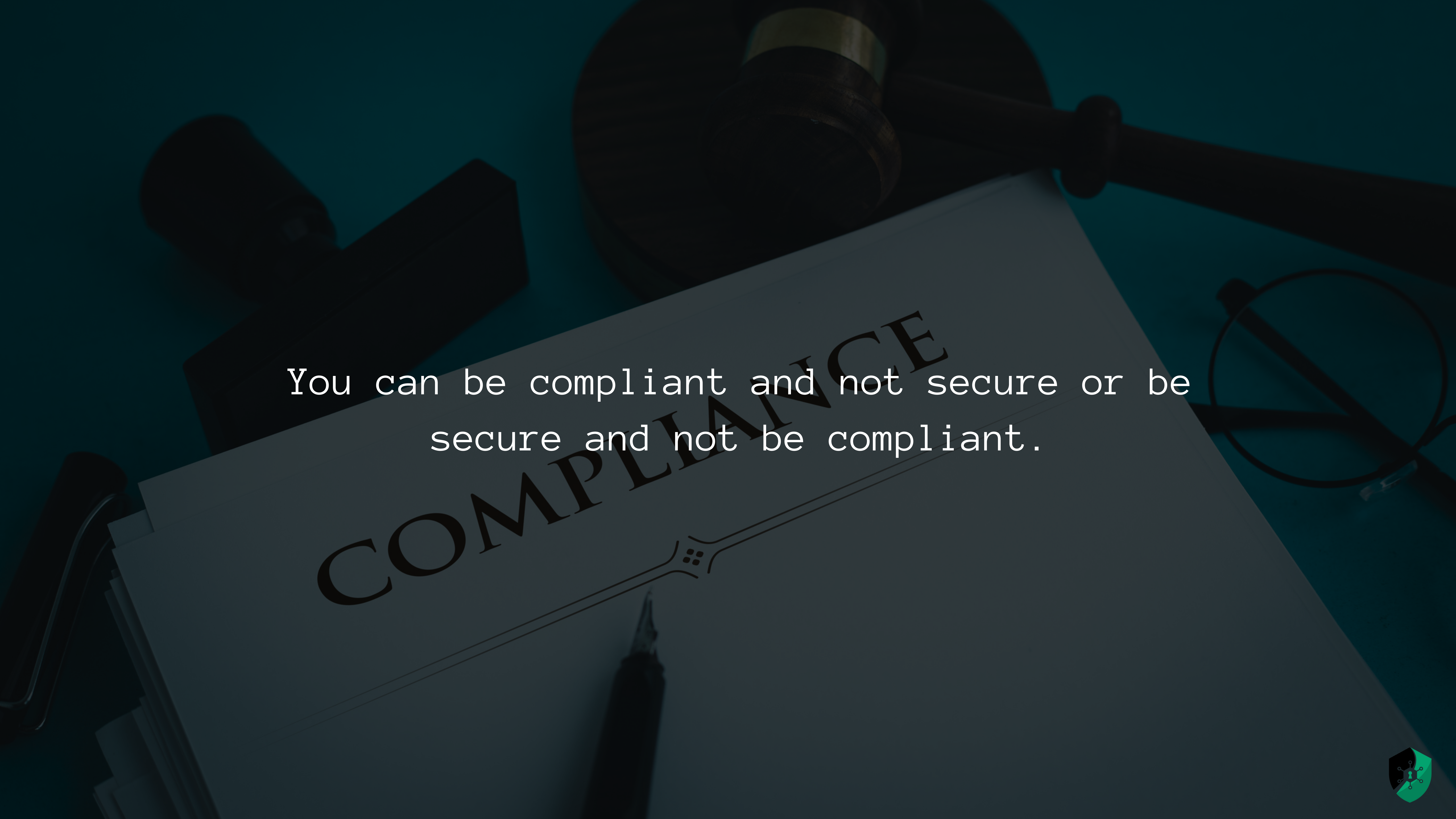
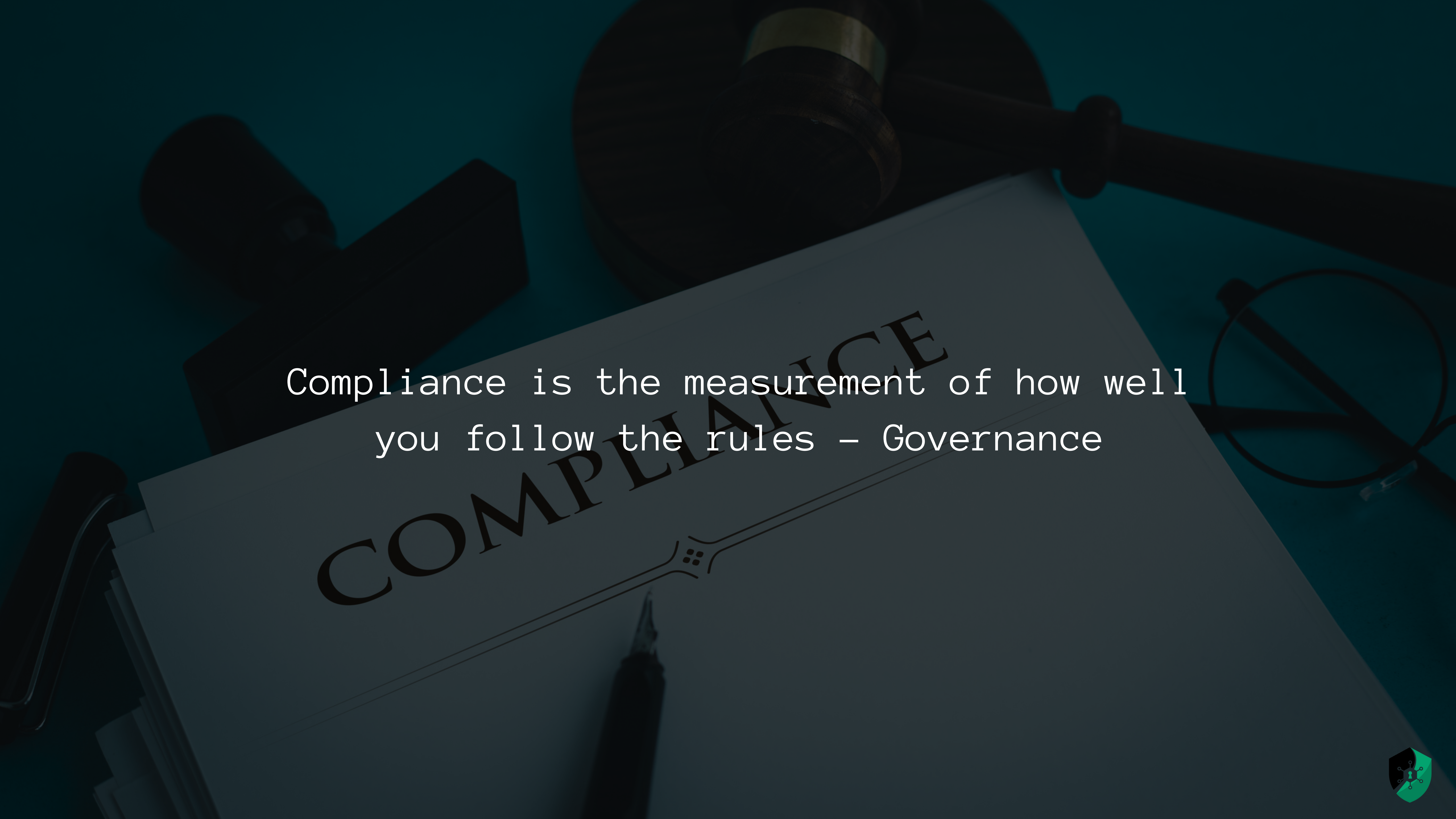
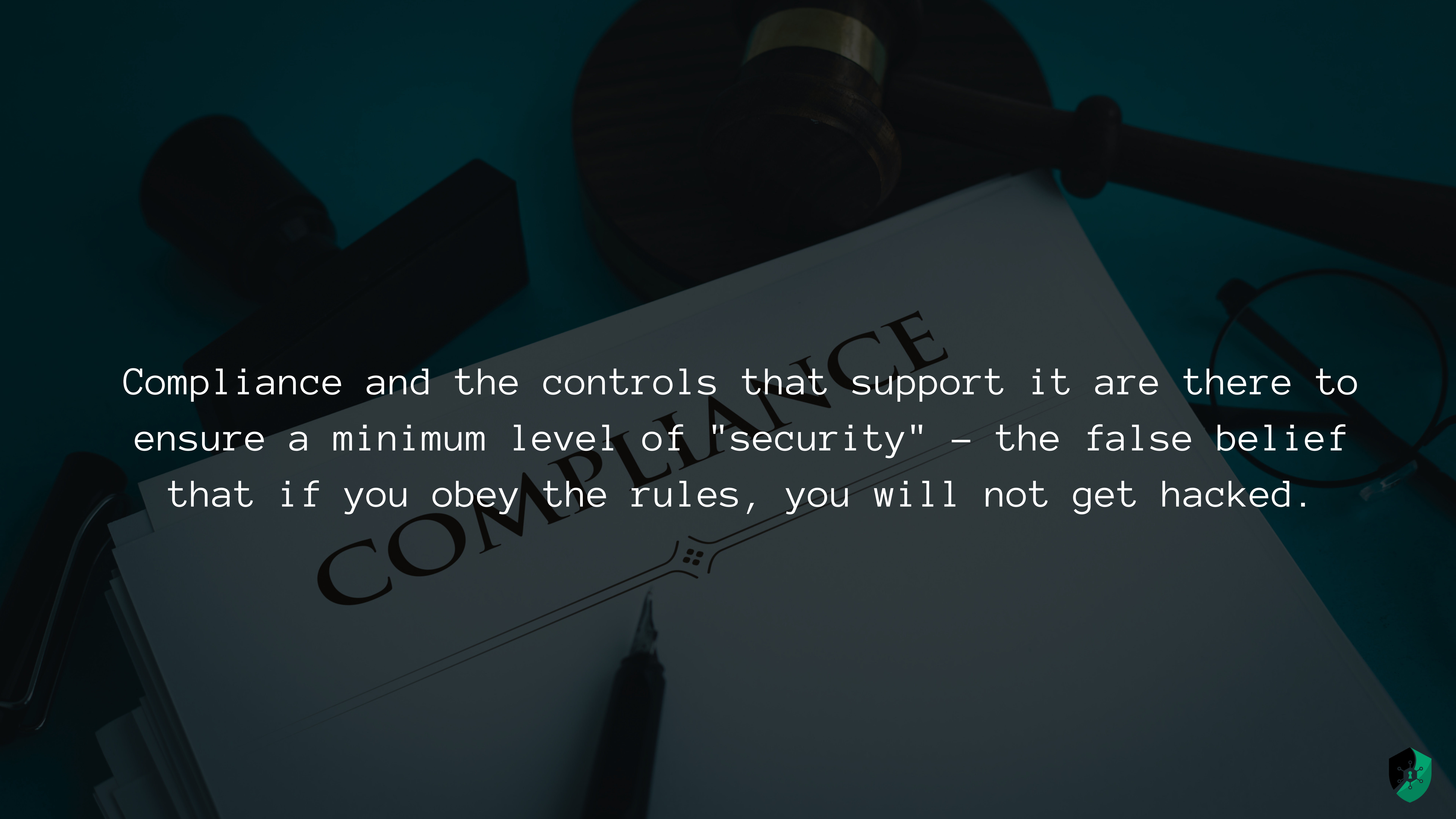
COMPLIANCE



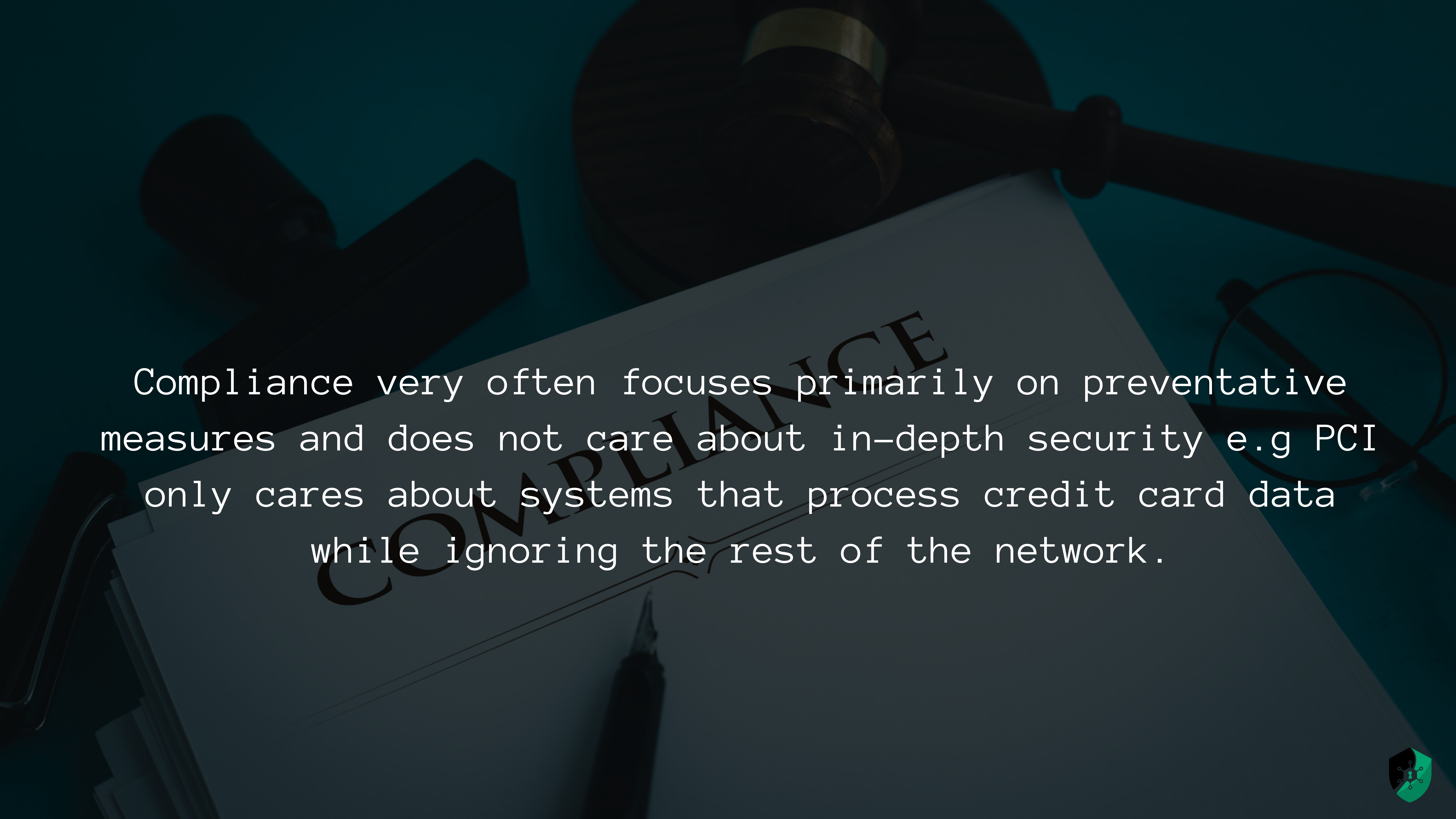
You can be compliant and not secure or be secure and not be compliant.



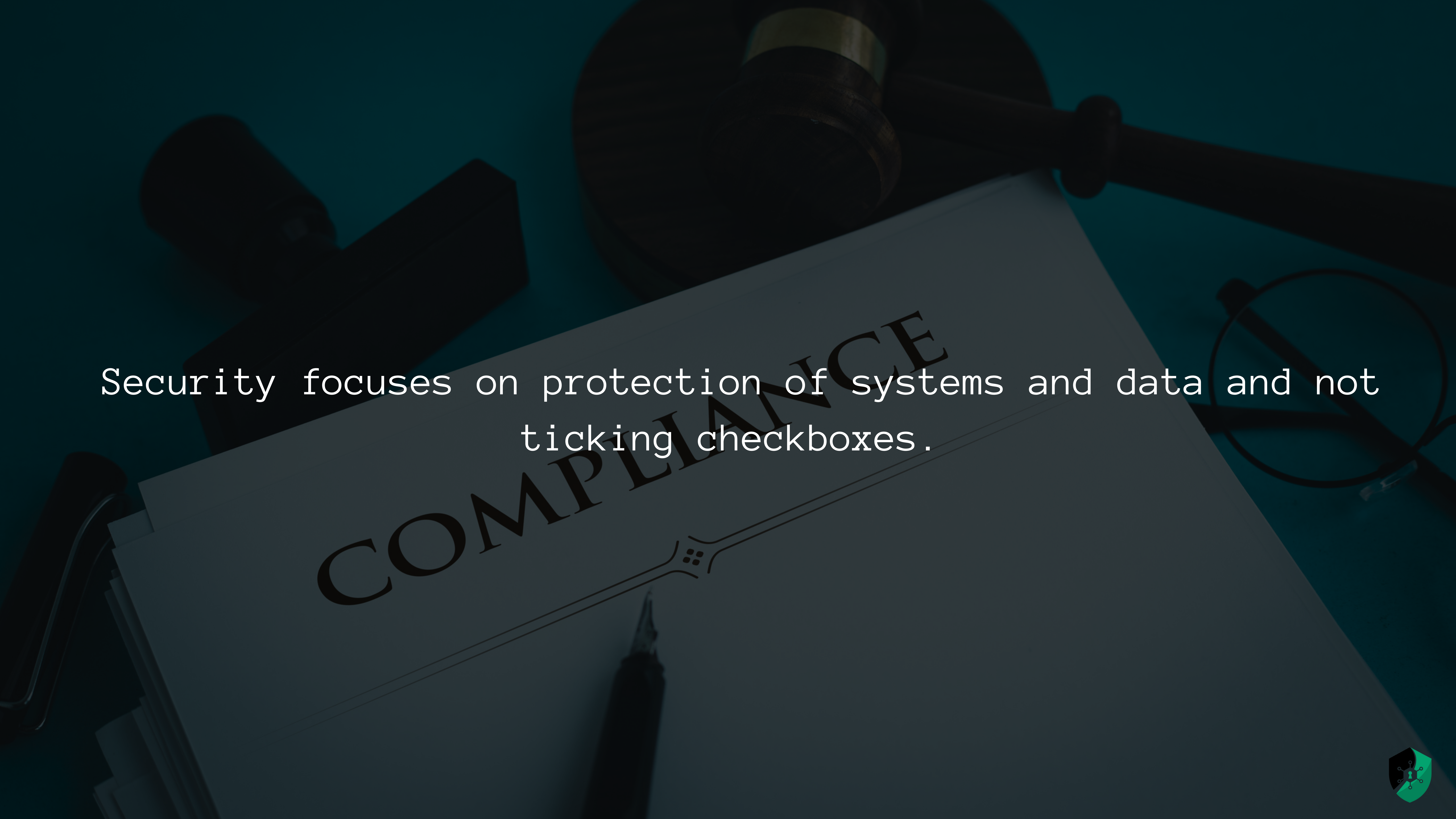
Compliance is the measurement of how well you follow the rules - Governance



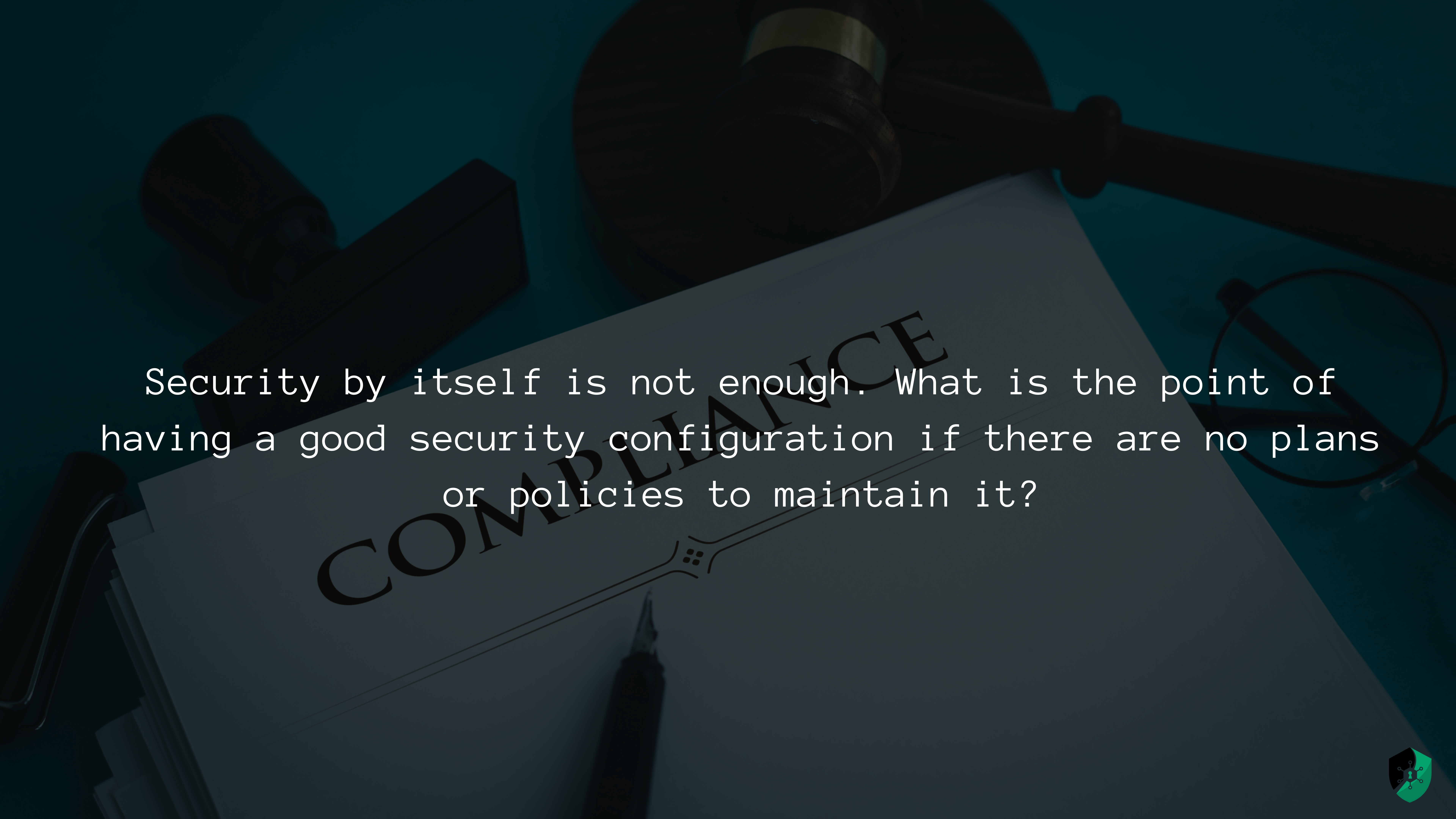
Compliance and the controls that support it are there to ensure a minimum level of "security" – the false belief that if you obey the rules, you will not get hacked.



Compliance very often focuses primarily on preventative measures and does not care about in-depth security e.g PCI only cares about systems that process credit card data while ignoring the rest of the network.



Security focuses on protection of systems and data and not ticking checkboxes.

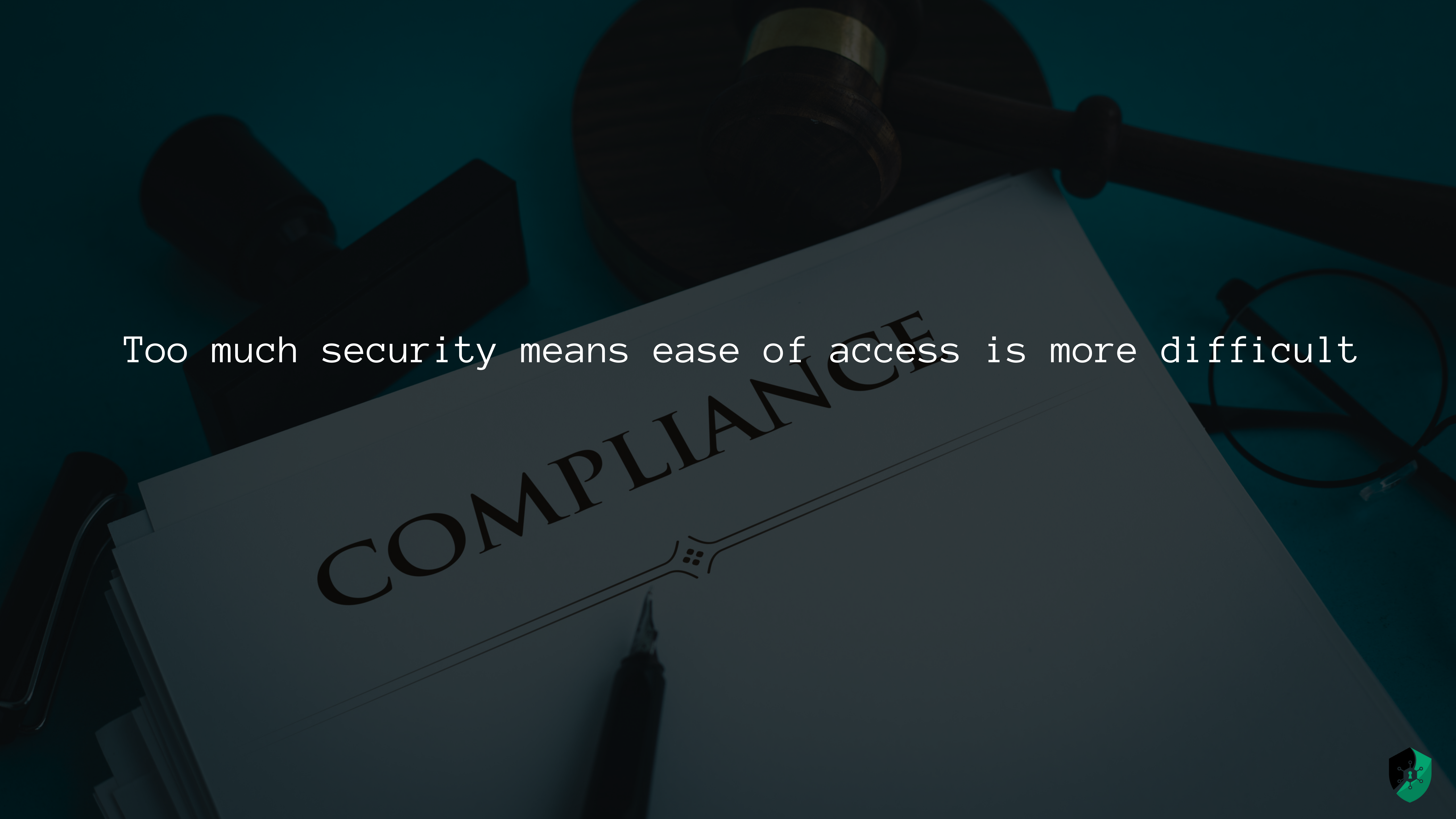


Security by itself is not enough. What is the point of having a good security configuration if there are no plans or policies to maintain it?

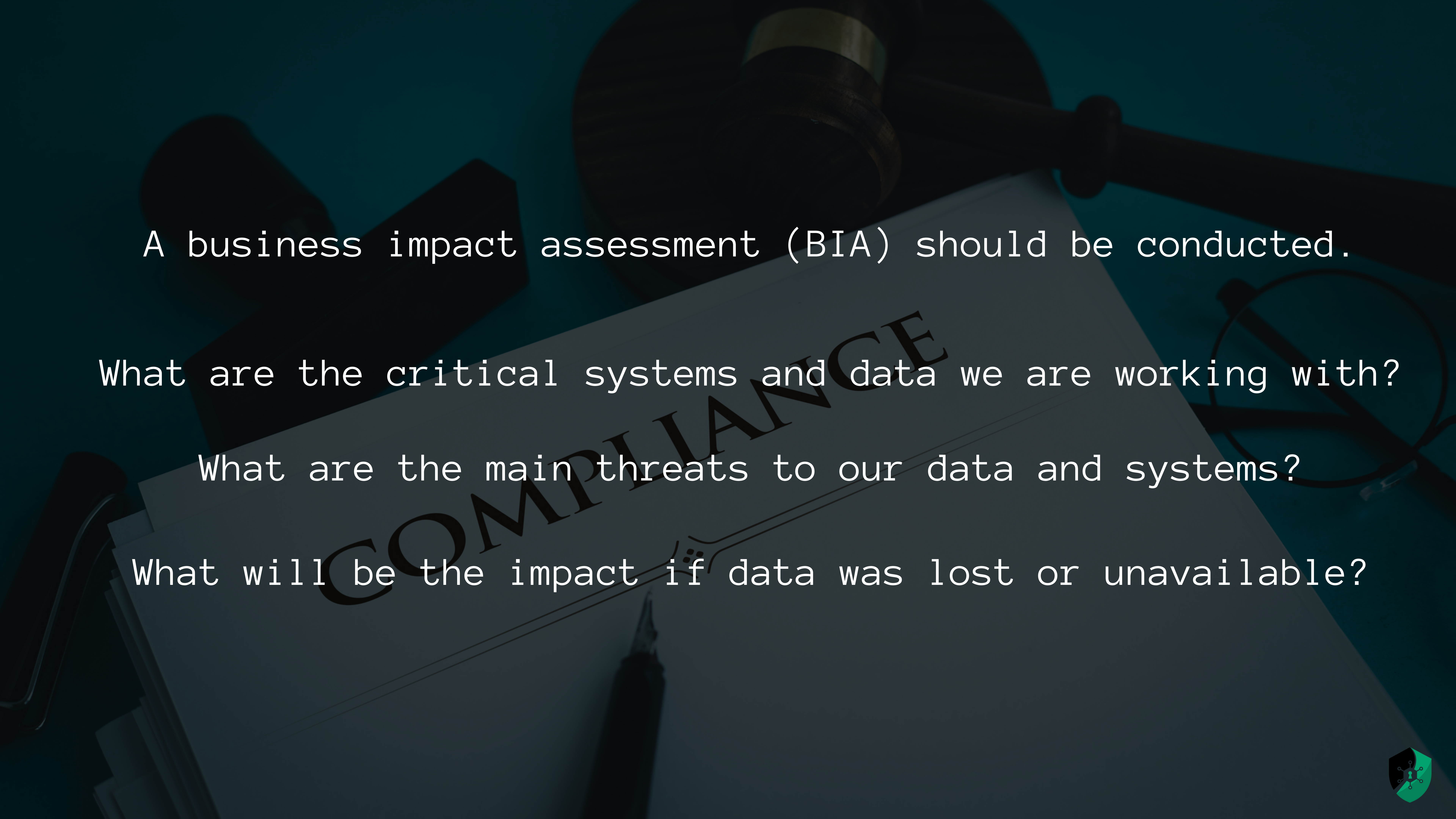
How can we be secure and compliant at the same time?

Security comes first and compliance later

Don't over protect or under protect.



Too much security means ease of access is more difficult

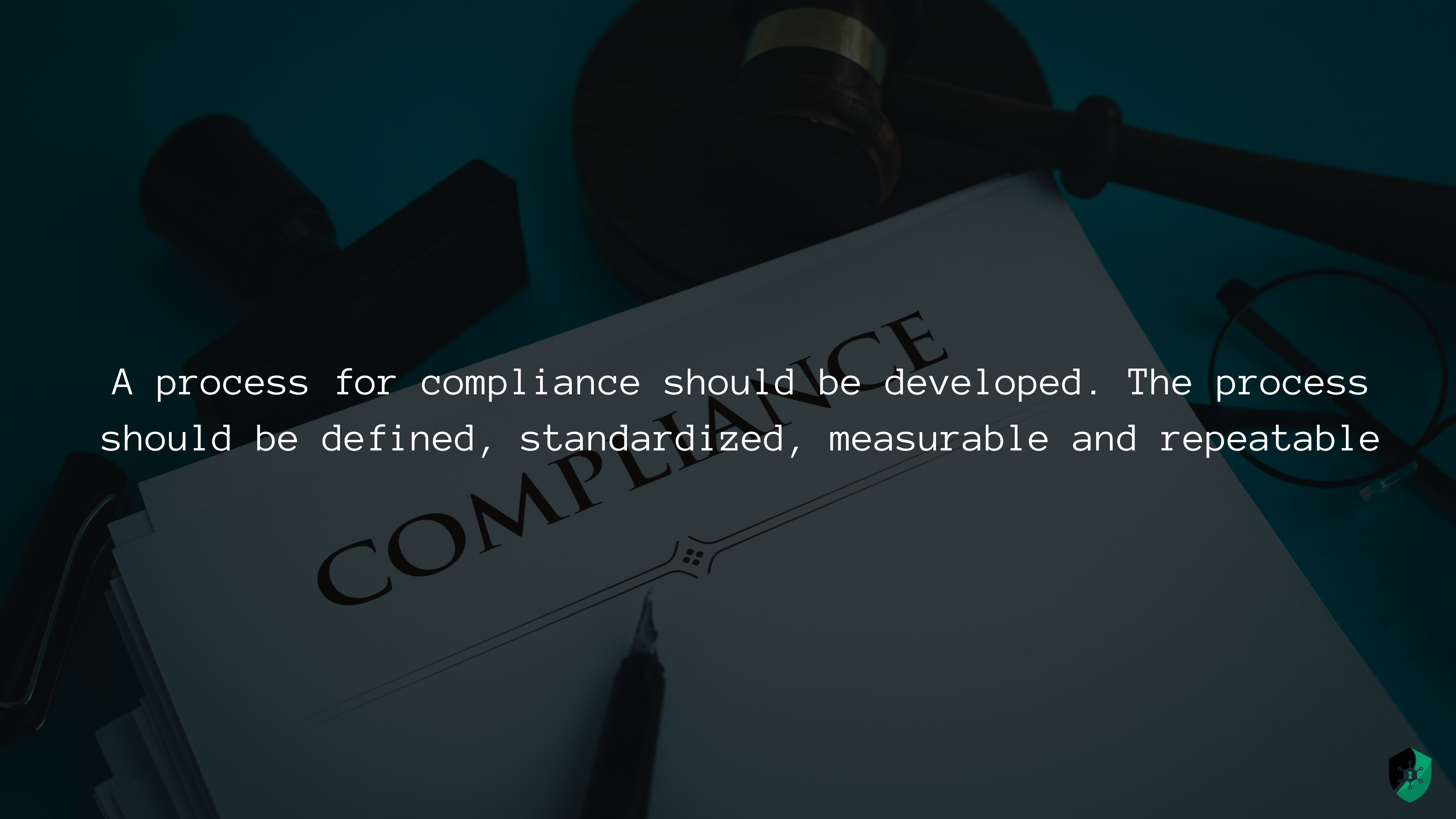


A business impact assessment (BIA) should be conducted.

What are the critical systems and data we are working with?

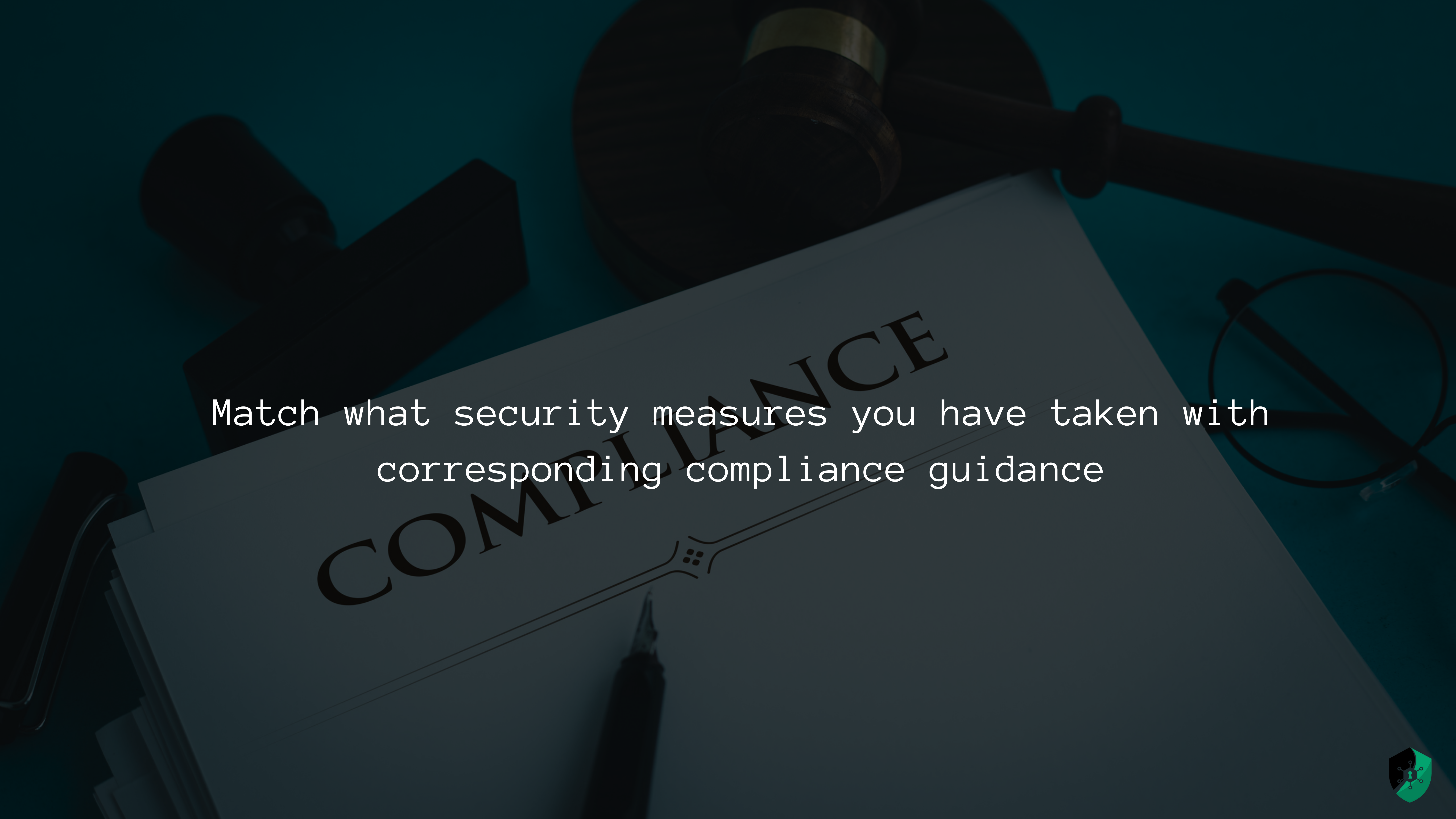
What are the main threats to our data and systems?

What will be the impact if data was lost or unavailable?

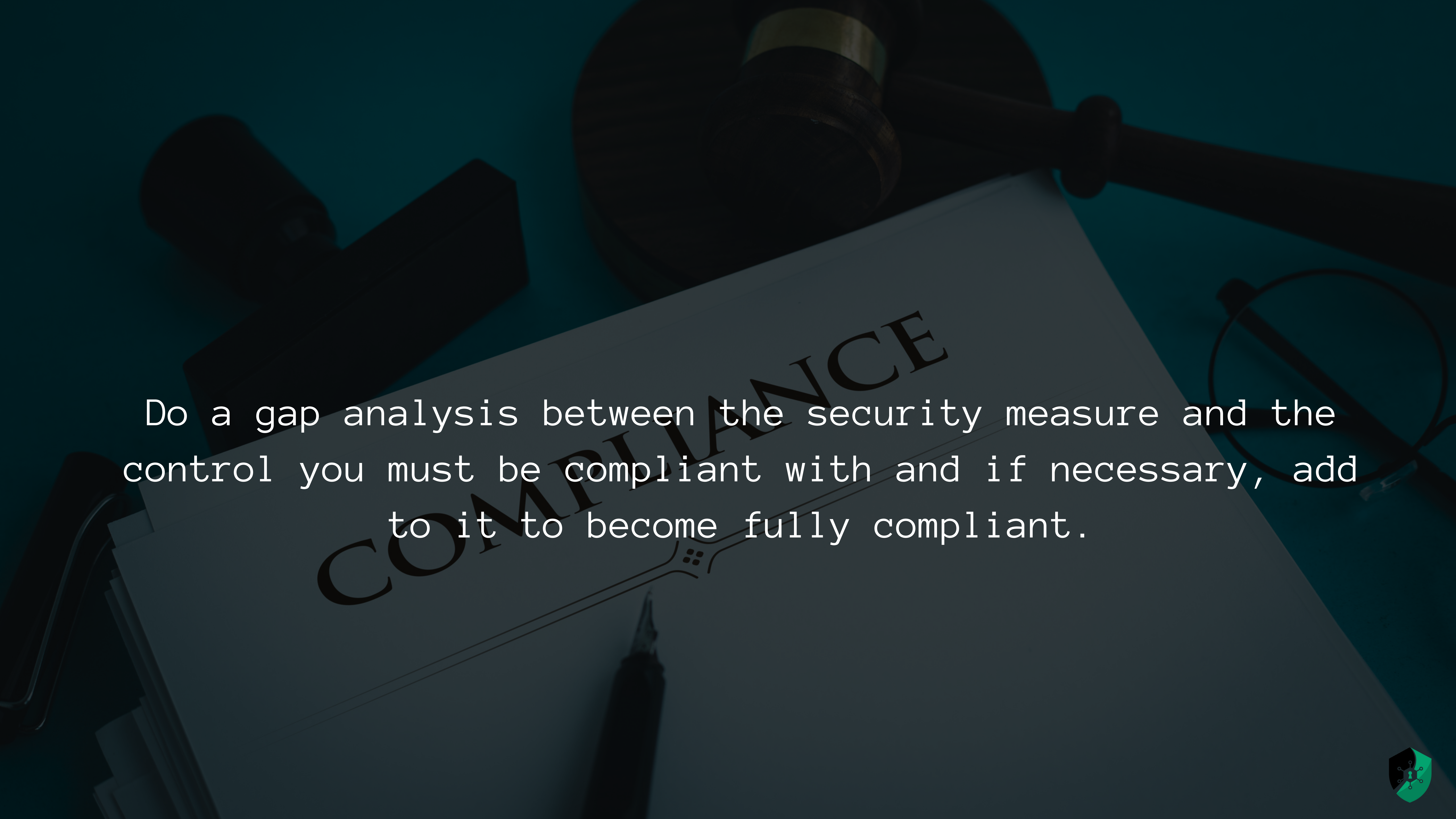


A process for compliance should be developed. The process should be defined, standardized, measurable and repeatable

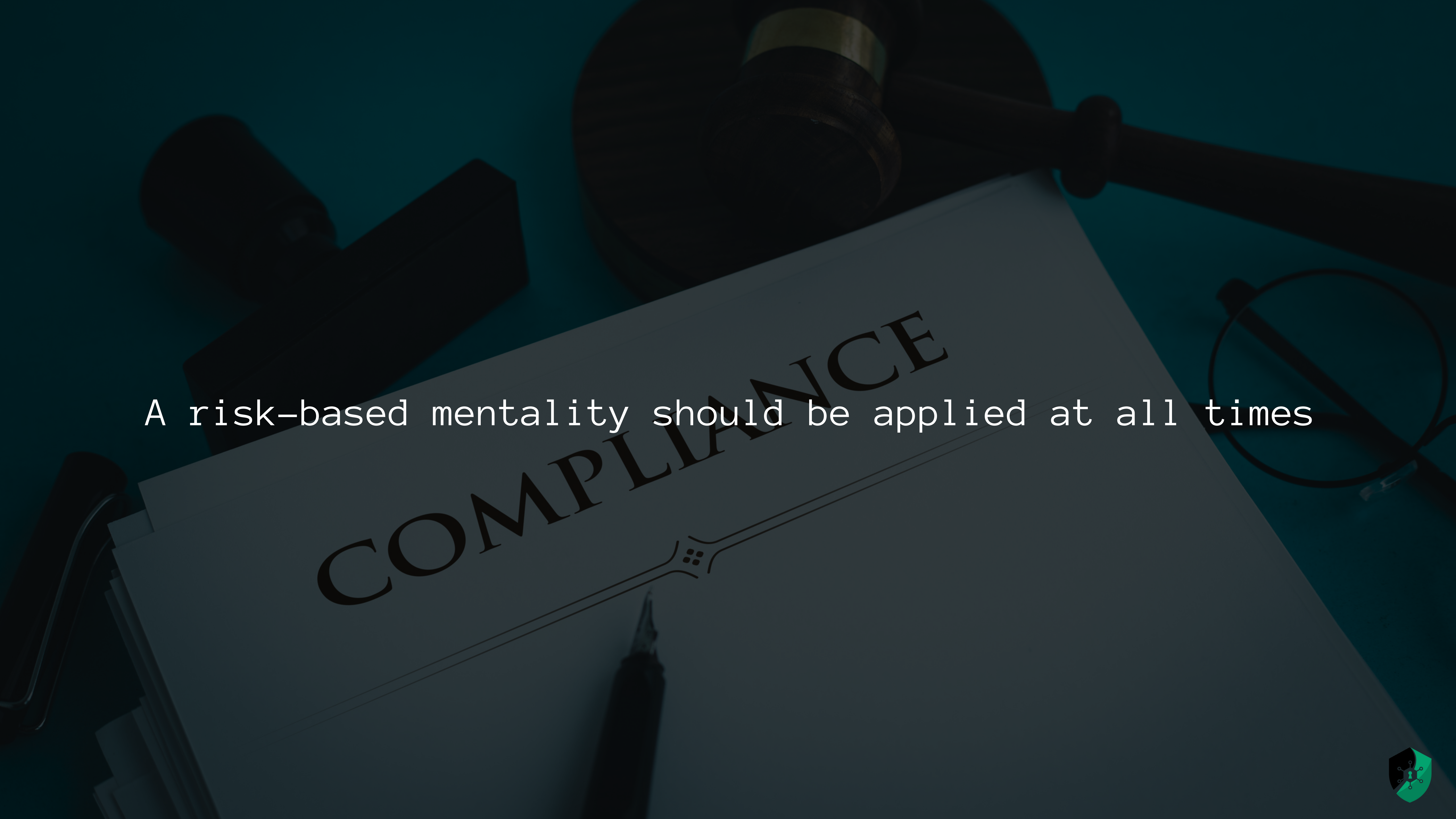
Develop documentation for controls implemented, compliance and exceptions including mitigations.



Match what security measures you have taken with corresponding compliance guidance



Do a gap analysis between the security measure and the control you must be compliant with and if necessary, add to it to become fully compliant.



A risk-based mentality should be applied at all times