The Book of Compliance

Chapter 1 – Compliance Is Security

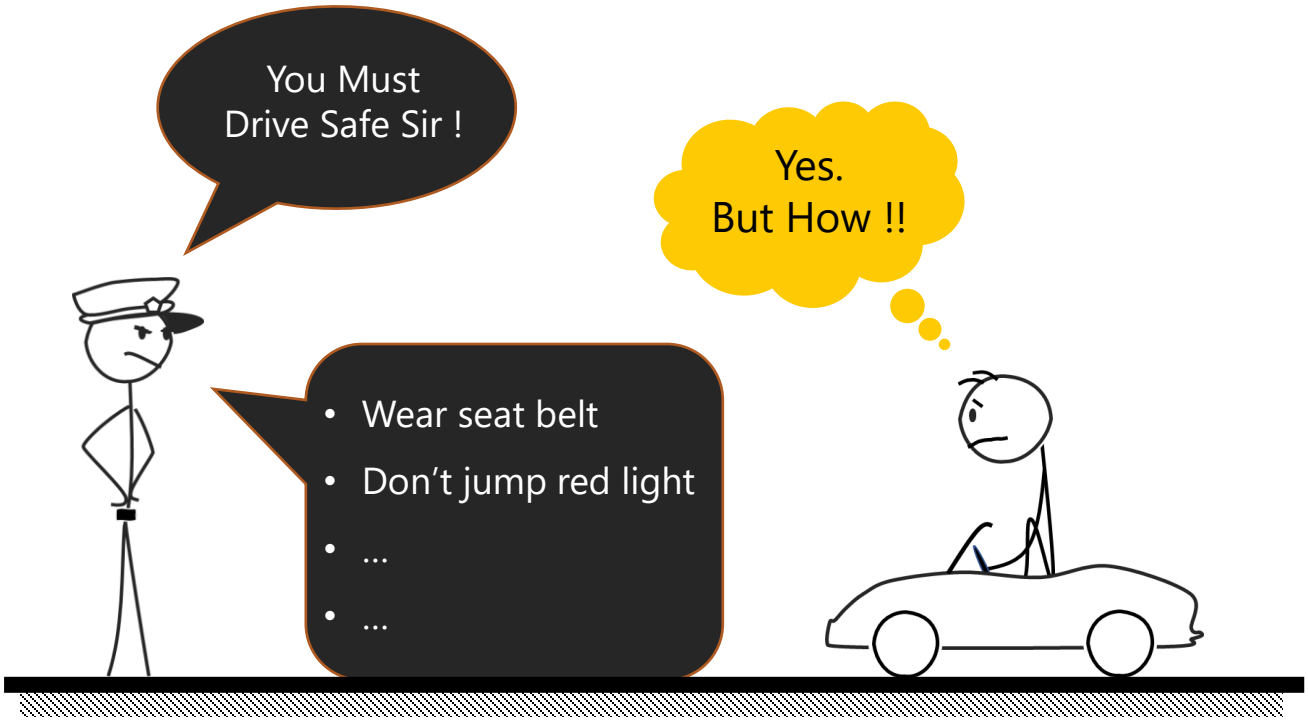
Compliance Is Security

Don’t let anyone tell you otherwise.

Download this chapter
https://bit.ly/ComplianceHandbookCh1

More aptly put, Compliance is the measure of Security.

For instance, it wouldn't make sense if we were told to drive safely without explaining what that means. We need set of rules to check if we are driving safely or not.

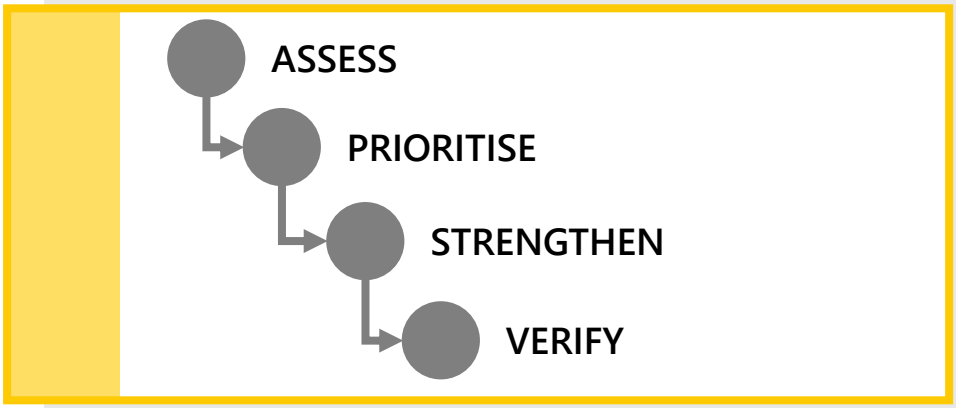


As with traffic rules, Compliance standards for information security provide set of Rules (Controls) to Measure Safe Operation.

Download this chapter
https://bit.ly/ComplianceHandbookCh1

Four steps to successful deployment

When thinking of implementing a GRC program, think of these 4 steps:



Most organisations have an existing compliance program, so it's about assessing and re-calibrating.

Things we all know, but forget:

- Coverage is important. Done rolling out MFA? – check. Did you think about coverage of your frontline workers?
- It's all about Data, even when it's not.
  Security controls cover all aspects of an organisation - access controls, device protection, backup, internet security. But in the end, it's all about keeping pertinent data secure.
- Risk Acceptance is a valid option, but only after you've assessed requirements, evaluated gaps and considered the impact.

Download this chapter
https://bit.ly/ComplianceHandbookCh1

ASSESS — PRIORITISE — STRENGTHEN — VERIFY

To evaluate if you are following the right rules (aka Regulatory Posture Assessment), start by assessing what Laws (Standards) apply to You.

Qualify Based On:

Geography

Country / State of operation.

Just like - Country / State where you are driving

Data you are managing

- Financial Data
- Personal Information (PII)
- Health Records
- National secrets

Just like - Who you are carrying in your vehicle:

- Passengers
- Family
- Cargo
- Patient

Target audience for systems / data

- Regulated industry (e.g. Defence)
- Customer / Social
- Security monitoring
- Ad targeting

Just like – What is your cargo meant for:

- Public transport
- NASA equipment
- Oversized delivery for construction

Leverage the selected standards to conduct Gap Assessment and prioritise control sets to implement.

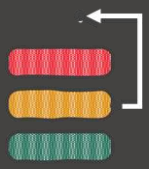
Download this chapter
https://bit.ly/ComplianceHandbookCh1

ASSESS | PRIORITISE | STRENGTHEN | VERIFY

Q How do you eat an elephant?

A One bite at a time

In other words, **Prioritise**.

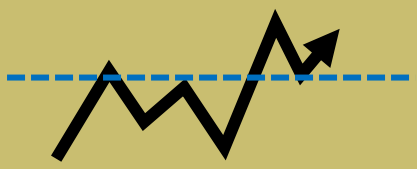


Use the axis of:

- Scope – on basis of service, entity and / or scale. As an example, some cloud services provide more out-of-box controls and comprehensive reach than others.
- Control Set – choose control sets that provide easier return and momentum to carry on.
- Maturity Level – select the maturity level with closest jump in compliance and build from there.

Download this chapter
https://bit.ly/ComplianceHandbookCh1

ASSESS PRIORITISE STRENGTHEN VERIFY



Implementing controls inherited from given standard(s) provide a Good Baseline of security measures to build upon.

While not sufficient, **A Baseline Is A Must** to have a strong security foundation.

Download this chapter
https://bit.ly/ComplianceHandbookCh1

ASSESS PRIORITISE STRENGTHEN VERIFY

Top Up The Controls with guidance from a more exhaustive (and Voluntary) Security Framework.

- Zero Trust
- SASE
- NIST CSF

Download this chapter
https://bit.ly/ComplianceHandbookCh1

ASSESS PRIORITISE STRENGTHEN VERIFY

Sprinkle with common-sense guidelines

- Defence-in-Depth
- KISS (Keep-it-simple-silly) – At least from user experience perspective.
- Start Small / Fail Fast

Download this chapter
https://bit.ly/ComplianceHandbookCh1

ASSESS — PRIORITISE — STRENGTHEN — VERIFY

Run a Self-Audit

Why

- Review and assess your posture.
- Draw attention to areas for improvement.
- Reinforce right behaviour.
- Ensure Compliance.
- As an added perk, Be more Ready for the next external audit.

How

Many standards supply their recommended assessment templates. If you are spinning up your own, here are a few attributes to include:

Sample

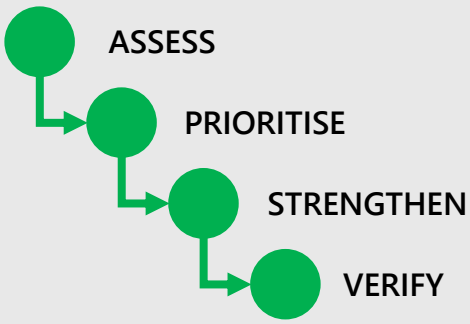
Category	ID#	Control	Assess	Coverage	Remarks	Rating	Ranking
Access Control	AC-001	Single sign-on policy	Access control policy for	- Covered - Partial - No Coverage	TBA	Rate and Rank for statistical assessment and trend check	

Look out for blind spots.

For e.g., when thinking of data protection, it's common to assess access control, encryption software, patching and back, however overlook data privacy training for employees.

Download this chapter
https://bit.ly/ComplianceHandbookCh1

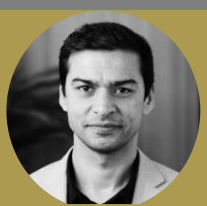
So, there we have it:



For and Further Reading Reference

- **Risk Assessment Guide for Microsoft Cloud**
- **Microsoft Purview Compliance Manager**
- **Zero Trust Guidance Center**
- **What is secure access service edge (SASE)?**
- **Zero Trust Mindset**

Connect



← Tap me on LinkedIn to discuss or know more about how Microsoft can help.

Download this chapter
https://bit.ly/ComplianceHandbookCh1