# **Mosi's Compliance Maturity Model**

## **Adversarial** Investigation

### Adversarial investigations of static environment

Security requirements selected by external party and rarely change

Non-compliance with externally-mandated tech migration (e.g. TLS versions, ads targeting)

Auditors selected by external party to conduct few, routine audits

External investigation of few M&As or divestitures

#### Friendly assessments of static environment

Security requirements selected by management rarely change

Technology adoption lags behind external changes

Auditors selected by management to conduct few, routine audits of limited scope

Management conducts due diligence reviews of very few M&As or divestitures

#### Adversarial investigations of dynamic environment

Security requirements selected by external parties updated with many regulatory changes

Many externally-mandated tech migrations & adoptions to keep pace with external changes

Auditors selected by external party to conduct many audits at different times of different scopes

External investigations of many M&As or divestitures

#### Friendly assessments of dynamic environment

Security requirements continuously updated by management with regulatory & business model changes

Technology migration & adoption keeps pace with internal & external changes

Auditors selected by management to conduct many audits of different scopes

Management regularly conducts due diligence reviews of multiple M&As or divestitures

### Friendly Assessment

### Static Environment



**Credit: Mosi Platt, Senior Security Compliance Engineer @ Netflix** 

### Dynamic Environment

