What (the bleep) is a Control?

A lot of lingo gets tossed around in the compliance world: Criteria, Standard, Point of Focus, Narrative, Control Owner, Test of Operating Effectiveness, and on and on and on. One of the most common terms is a control. A succinct, well written control will be easy to 'prove', or easy for an auditor to test. A poorly written control will confuse an auditor and lead to unnecessary back and forth. At Strike Graph, we are commonly asked, "What the heck is a control and how do I write one?"

A 'No Audit Lingo' Definition

If you search online, you will find many definitions of what a control is. Unfortunately they are very technical and confusing, and are not very helpful unless you are a compliance geek or an auditor. We advise our customers to think of a control as the process step you put in place to address or solve for a specific risk, or that succinctly describes a key cyber security action.

A control will follow a basic formula which answers:

- Who performs the activity? (Use a job title, not the actual name of the person)
- What is happening? (Brief description of the activity or action taking place)
- How often the activity happens? (For example daily, monthly, annual, as needed)

In other words, a control includes an actor, an action, and a frequency. Sometimes the frequency is not included, but is tracked as a separate characteristic of the control in a spreadsheet or database. Some controls will be more complex in order to accurately describe the action or process, but the formula above is a solid starting point.

The Audit Angle

Auditors interpret controls literally, and they will generally test exactly what is stated in the control. An experienced auditor understands that some controls have a bit of wiggle room, which, in audit lingo is called the spirit of the control. For example, if a control states that "All employees sign an Acceptable Use Policy (AUP) upon hire", the auditor may be looking for signatures on paper in an HR file. However, if you have an automated HR task tool where all documents must be reviewed prior to moving to the next onboarding task, it is likely that no signature will be collected. The workflow is such that they couldn't move on in the onboarding process until they read the AUP. The spirit of the control is that all new hires have ***acknowledged*** they have read the AUP, whether there is a signature present or not.

A Real World Example

Controls are generally in place to address a risk. For example, if you don't change the oil in your car on schedule, there is a risk that you will damage the engine. The control is that the oil is changed every 12 months or 6,000 miles by a mechanic. To prove that the control happened, you have a receipt showing the date, the type of oil used, and the make, model and mileage of your car. From the receipt, an independent party can confirm that the oil was changed, on schedule.

Avoid Writing a Vague Control

"Annually, the CTO reviews and re-approves security policies." This control is too vague - exactly which policies? Do you have to list each policy that requires an annual review? Not really, but it wouldn't hurt. A more concisely wording control may be: ***"Annually, the CTO reviews and re-approves the security policies related to Change Management and Logical Access."***

There's nothing worse than having an auditor fail a control because you didn't intend for ***everything*** implied within it to be tested!

Another Example

You have a small team of developers and due to the size of the group, they have to wear many hats. As VP of Engineering, you mandate that any code that enters production is reviewed, tested and appropriately merged. To ensure that no rogue code enters production you implement a control that all code is reviewed and approved and that if one developer creates code, a different developer will test it. You also have a control stating that no developer can merge their own code.

More Control Examples

- ***Employees are required to sign NDAs prior to starting work.*** The frequency of this control is not stated, but it implied that it will occur anytime a new hire is on boarded.
- ***No access is granted to back end systems without approval by the Engineering Manager or backup approver.*** The frequency is also implied - it is for each request.
- ***Monthly vulnerability scan results are triaged and actioned per defined SLAs. The CTO may approve a delay on any Severe or High findings.*** The monthly frequency can be replaced with the actual frequency with which the scan is performed, and any exception approvals are 'as needed'. This is really two controls, but lumped together because they are integrated processes and can be tested together.
- ***All employees are required to take security training upon hire and annually thereafter.*** The frequency is both annual and every time a new hire comes on board.

The Good News

The Strike Graph solution comes with an audit-proven library of controls that can be used or tailored for your audit. You don't have to create controls on our own! As a bonus, the controls in our library span various levels of maturity, from manual paper based to fully automated controls.

ABOUT STRIKE GRAPH

Strike Graph is a compliance SAAS solution simplifying security certifications such as SOC 2 Type I/II or ISO 27001. These certifications dramatically improve revenue for B2B companies. Facilitated by the Strike Graph platform, key actors in the process including Risk Managers, CTO's, CISO's and Auditors can work collaboratively to achieve trust and move deals. For more information visit https://www.strikegraph.com.