

Welcome

March 27, 2024
OWASP-LA



Agenda

- Intros
- Making s'mores
- GRC Flow of work
 - Influences
 - Regulations
 - Frameworks
 - Company Documents & Controls
 - Control execution
 - Evidence gathering & Repositories
 - Audit lifecycle
 - Continual Improvement

Disclaimers



Women + Cybersecurity = Women's Society of C...
25,221 followers
1w •

Applying Key GRC Flow of Work Principles Workshop
When: 4/20/2024 • 9:00 AM - 12:00 PM PT
Where: Google Irvine Building 1, Irvine, CA + Virtual
Register: <https://lnkd.in/g2ve-85F>

Standing up or optimizing a GRC program is all about pattern. We will discuss key GRC principles and how they can be used to build or optimize GRC maturity. The components are the same across company industry, company size, and company maturity.

Instructor **Karina Klever** has spent over 30 years in technology, starting in 1989 as a computer operator! Join us virtually or in-person at Google Irvine Building 1 in Irvine, CA.

#womenincybersecurity #cyberjutsutribe #infosec #cybersecurity #cyberjutsu
#womencyberjutsu #womenintech #nonprofit



Applying Key GRC
Flow of Work
Principles Workshop
with Karina Klever
April 20

Irvine
CA

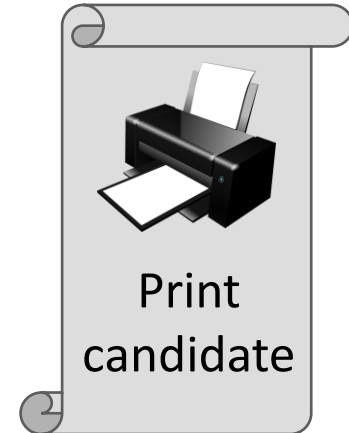
Google

CYBER
JUTSU

Google

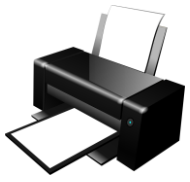
This is a 'learning' deck to be used Apr.20

- Some slides will have lots of words
- Intended to be printed out & taken to work



Tried to make this deck generic!

- Companies come in all shapes & sizes
- Approach should be vague enough to apply to any company



Alphabet soup

GRC COE: Governance, Risk & Compliance Center of Excellence

What is **GRC**?

Governance: Managing operations in a defined & Standardized way

Risk: Understanding/Mitigating external or internal company threats

Compliance: Maintaining compliancy with the influences that govern our company

“GRC” is also being referenced as “**IRM**”:

... Integrated Risk Management

“Vendor Management” may also be getting referred to as “**TPRM**”

... Third Party Risk Management

Simplify your understanding

Introducing Klever Compliance

Founded by Karina Klever

- Started IT in April 1989 as a computer operator
- Moved into AS400 programming, but never got good requirements from the project managers, so
- Moved into Project & Program managing – until an old boss called saying “name your price”, so
- Moved into GRC in 2002 – been here since & loving it...



Successes

- Designed, operationalized and matured GRC COEs at insurance companies, retail companies, financial institutions, healthcare providers, pharmaceutical/biotech, and technology firms
- Used inherent ticketing systems to implement supporting workflows triggered by GRC operations
- Provided services to companies of various sizes in the last 20+ years; From Fortune 100 to mid-sized
- Proven ROIs saving manual compliance efforts. If the company has roughly...
 - 10 people manually supporting compliance functions @
 - \$40/hr fully-loaded {this is very modest} @ 2080 annual working hours, totals
 - totals \$832,000.- annual spend

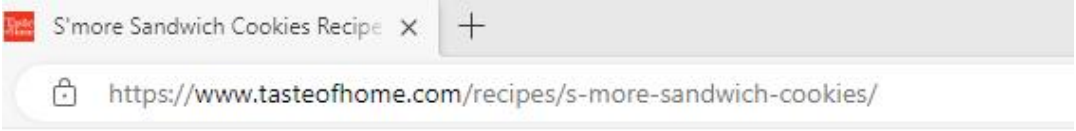
Many of these functions can be automated

Most companies have more than 10 people in manual GRC functions

- M&A alignment of in-coming or out-going GRC organizations/functions



Making S'mores



Taste of Home



S'more Sandwich Cookies Recipe photo by Taste of Home

Ingredients

- 3/4 cup butter, softened
- 1/2 cup sugar
- 1/2 cup packed brown sugar
- 1 large egg, room temperature
- 2 tablespoons 2% milk
- 1 teaspoon vanilla extract
- 1-1/4 cups all-purpose flour
- 1-1/4 cups graham cracker crumbs (about 20 squares)
- 1/2 teaspoon baking soda
- 1/4 teaspoon salt
- 1/8 teaspoon ground cinnamon
- 2 cups semisweet chocolate chips
- 24 to 28 large marshmallows



Overachiever



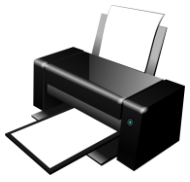
Ingredient overload



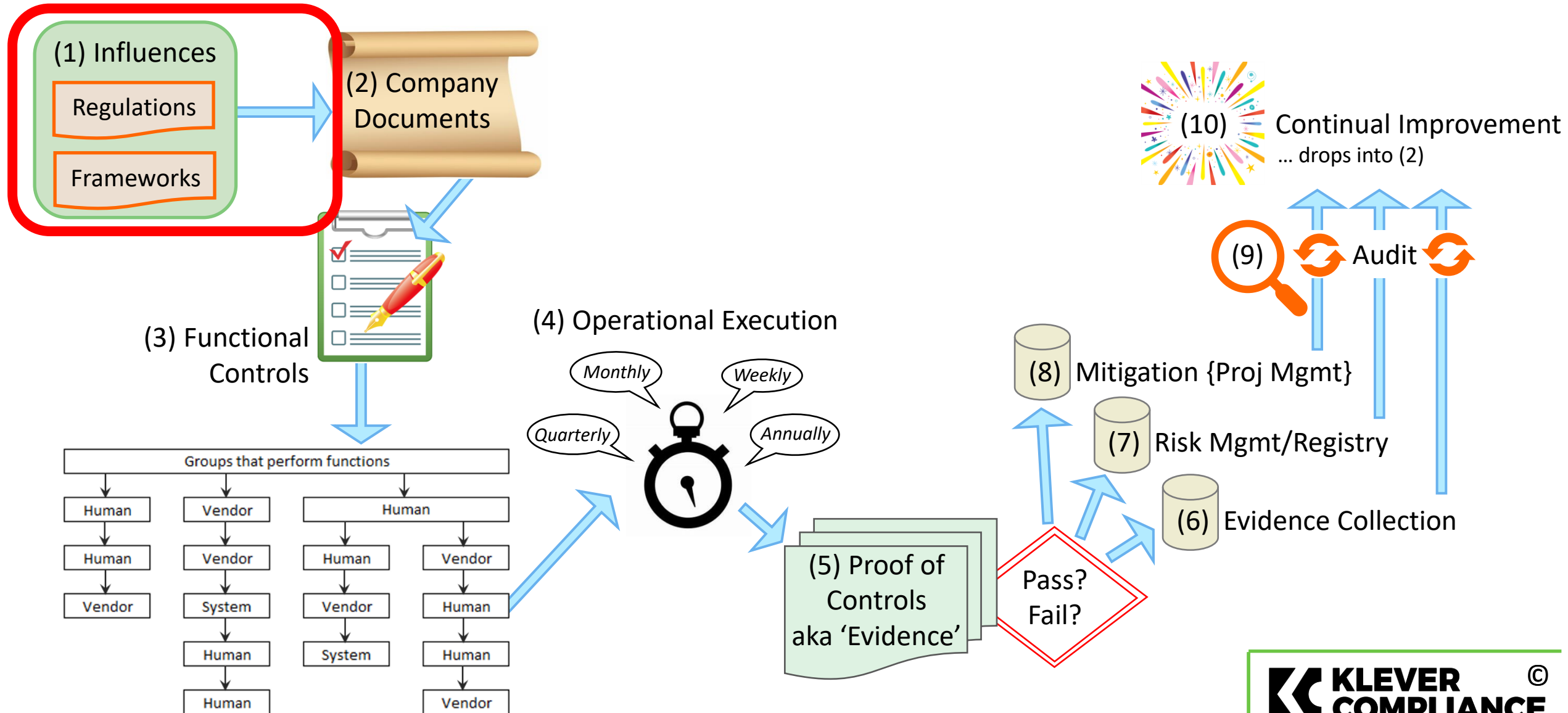
... maybe we should pay attention to appropriate quantities ...?

Ingredients

- 3/4 cup butter, softened
- 1/2 cup sugar
- 1/2 cup packed brown sugar
- 1 large egg, room temperature
- 2 tablespoons 2% milk
- 1 teaspoon vanilla extract
- 1-1/4 cups all-purpose flour
- 1-1/4 cups graham cracker crumbs (about 20 squares)
- 1/2 teaspoon baking soda
- 1/4 teaspoon salt
- 1/8 teaspoon ground cinnamon
- 2 cups semisweet chocolate chips
- 24 to 28 large marshmallows



Core GRC Flow of Work



(1) Influences: Frameworks



Framework Construction

How do frameworks come to be?

Super smart people gather
... and write them out



What's the most important thing in a framework?

Broad applicability

- Maturity** levels can differ
- Industries** can vary
- Company **size**, doesn't matter
- Platform** vagueness
- Recommended **adoption** extents

Translating Framework Language

Framework language:

- vague
- ethereal
- nebulous
- indifferent
- fantasy
- pie-in-the-sky
- ultimate goal



Your real operations:

- specific
- detailed
- exact



(1) Influences: Regulations



Enron auditors: We knew nothin'

By TIMOTHY J. BURGER
DAILY NEWS WASHINGTON BUREAU

WASHINGTON — Top officials of Enron's disgraced ex-accounting firm pleaded ignorance yesterday about murky partnerships that apparently were key to the energy giant's collapse into bankruptcy.

Arthur Andersen brass also swore to a House Energy and Commerce subcommittee that they knew nothing about alleged improper document destruction and accounting glitches until it was too late.

Andersen officials C.E. Andrews, Michael Odom and Nancy Temple, an in-house lawyer, tried to pin the debacle on fired partner David Duncan — after he invoked the Fifth Amendment in an apparent bid for immunity.

A competing hearing led by Sen. Joseph Lieberman (D-Conn.) featured former Securities and Exchange Commission Chairman Arthur Levitt, who recommended new regulations to boost the SEC's power.

Levitt described a "cultural economic erosion" during the 1990s in which companies used questionable accounting practices to meet profit expectations. Once some started, others had to do the same to remain competitive, Levitt said.

Lieberman said he will seek subpoenas for Enron's and

IN HOT SEAT Fired Arthur Andersen auditor David Duncan (c) took the Fifth during hearing in Washington yesterday.

New York Daily News Jan 25, 2002



"Our books are balanced. 50% of our numbers are real and 50% are made up."



(1) Influences: Regulations

Timeline governing ePHI/PHI

HIPAA PRIVACY ICONS



Certifications



Personal data



Security



HIPAA security



Personal health



Medical information



Medical Compliance



Password Security



Cloud Medical Data

- Aug. 1996 became law (**fax machine!**)
- Dec.2000 Privacy Rule
- Apr.2005 Security Rule
- Feb.2006 Enforcement Rule
- Feb.2009 HITECH enacted
- 2013: Combined Breach Notification, Security, Privacy & Enforcement under HITECH: Collectively called “Omnibus Rule”



(1) Influences: Some other Regulations

https://www.ftc.gov

An official website of the United States government [Here's how you know](#) Español Report Fraud

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Take Action

- Report fraud
- Submit a public comment
- File an antitrust complaint
- Get your free credit report
- Report identity theft
- Register for Do Not Call



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Gramm-Leach-Bliley Act

https://www.fda.gov

An official website of the United States government [Here's how you know](#)

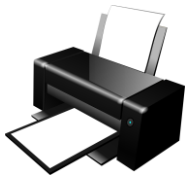
U.S. FOOD & DRUG ADMINISTRATION

PRODUCTS WE REGULATE

- [Food](#)
- [Drugs](#)
- [Medical Devices](#)
- [Radiation-Emitting Products](#)
- [Vaccines, Blood, and Biologics](#)
- [Animal and Veterinary](#)
- [Cosmetics](#)
- [Tobacco Products](#)

United States Department of Transportation

Federal Aviation Administration



(1) Influences

(1) Influences

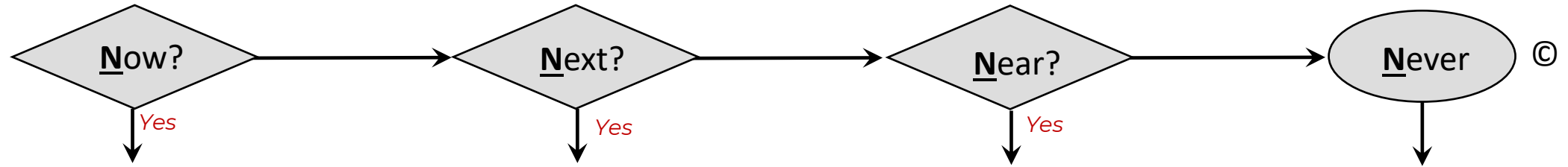
- Regulations
- Frameworks

What's applicable to **your** company is based on **your** industry, size, maturity

- Regulations are a must
- Frameworks are optional

You do ***NOT*** have to abide by all of it!

N⁽⁴⁾
 Appropriating influences based on your company



Functionally occurring now

- Document it
- Start gathering evidence
- Associate to risk
- Low hanging fruit

1 YR Targets

- Prioritize
- Create a project plan
- Assign ownership

3-5 YR Targets

- Strategic Goals
- Roadmapped

Inapplicable

- It's ok to not have ***everything*** apply to your company!
- see: 21 CFR 135.115



What are the auditors looking for?

Hey, um.... Where do I find me some NIST or SOX?

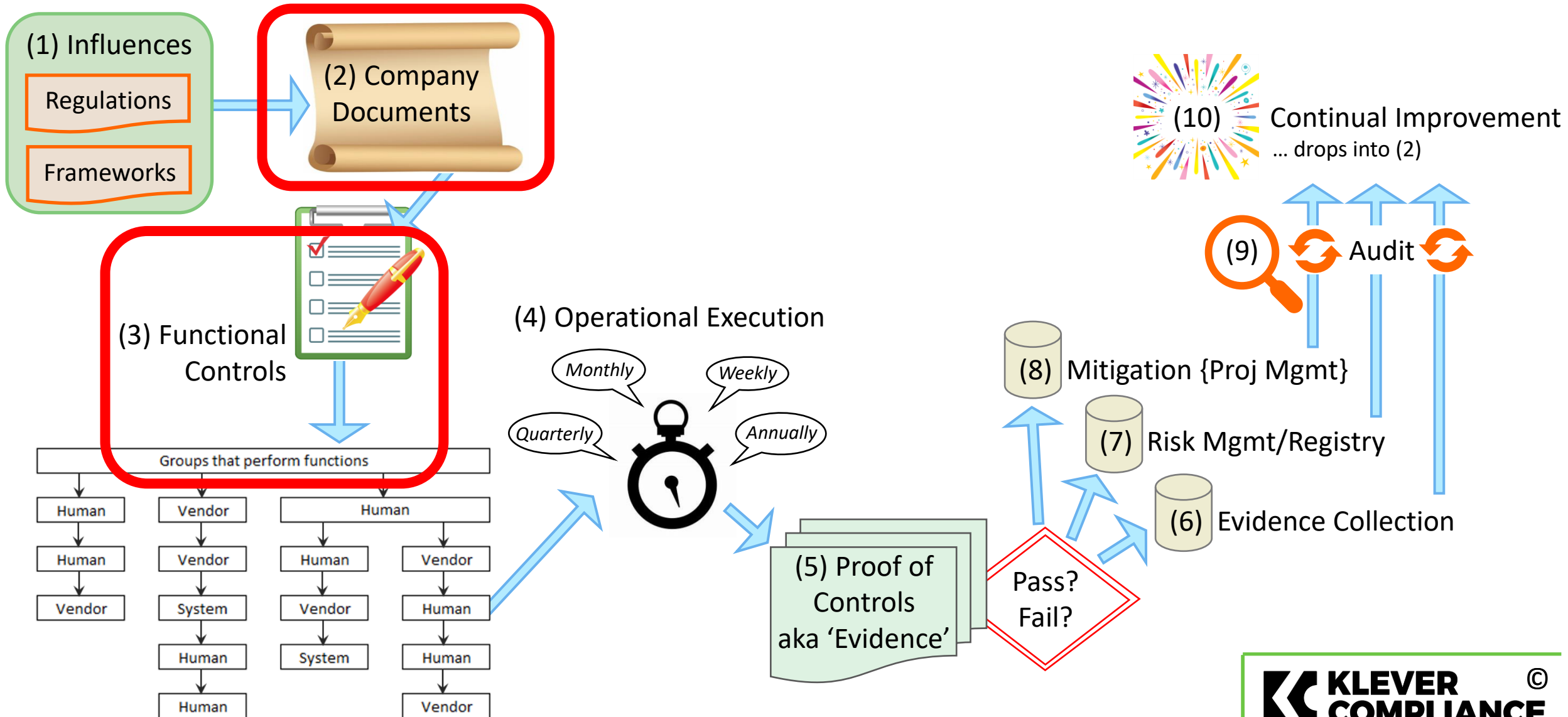


They don't show up to get a **regurgitation** of the Influence Documents

Auditors know what the Influence Documents say!

Auditors want to know how controls within your Company Documents are **satisfying** Influence Documents

Core GRC Flow of Work



(2) Company Documents



(2) Company Documents



There are two purposes to Company Documents

- Provide workers **guidance** of how to be successful in their positions
- Provide structure for all **company operations**

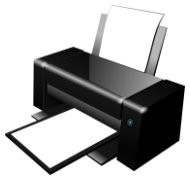
Acceptable ... policies, processes, standards, procedures, templates, work instructions, knowledge bases ...

Documents (& document templates!) are defined within your GRC COE

(2) Company Documents & (3) Functional Controls



- Make sure that your Company Documents
- **Align** to Influence Documents
 - **Align** to your operational structure/grouping/departments
 - Repository and access of **published documents** is well defined
 - **Cross-Reference** exists (content is to live in one source document; if referenced in another document, it's just a pointer & not a rewrite)



Warning about templates!

Occasionally

Periodically

Routinely

From time to time

Frequently

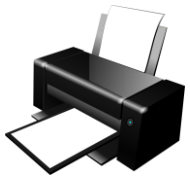
Recurringly

Controls live inside Company Documents

They must be written in a **specific & measurable** way

- How is the control triggered?
- How often does this occur?
- Who (exactly) does this.. Which role or system or vendor/third party?
- What does a success or fail look like?

If controls are not specific they will never, ever, be automated



The most important document

Data Classification

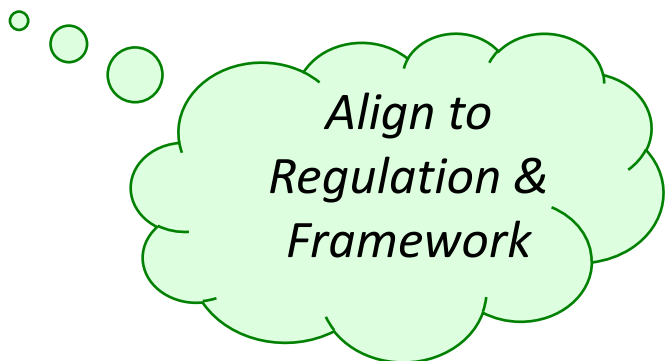
All your data & information is to be associated into a classification

Make sure all your types of data or information are addressed

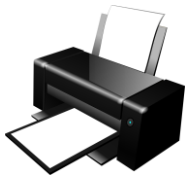
Forces identification of

- The data
- The groups/systems/vendors somehow leveraging data
- Supporting information

- Financial
- Client
- Company Proprietary
- Intellectual
- PHI / ePHI
- Consumer / Privacy / PII / SPI



*Align to
Regulation &
Framework*



Data Classification the Linchpin

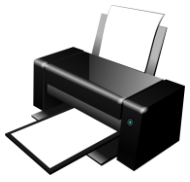
- ✓ Where is your data?
 - Stored
 - Transported
 - Processed
 - Include vendors!
- ✓ Who has what level of access to which data type?
 - Logical
 - Physical
 - System:System
- ✓ How long is each data type retained?
 - Duration
 - Protections (encryption?)
- ✓ Which data type gets the most focus during an incident?
 - Prioritization
 - SLAs
- ✓ Which data type gets backed up & when?
 - Tiering
 - Recovery requirements
- ✓ Which data type requires rigid destruction practices
 - Get that confirmation!

Groups that perform functions

- ✓ Incident Management
- ✓ Access Management
- ✓ Vulnerability Management
- ✓ Patch Management
- ✓ Change Management
- ✓ Procurement / Vendor Mgmt

- ✓ Asset Management
- ✓ Problem Management
- ✓ Human Resources
- ✓ Encryption Management
- ✓ Data Management
- ✓ Risk Management

**There can
more. Maybe
this is too
many**



A word about access control

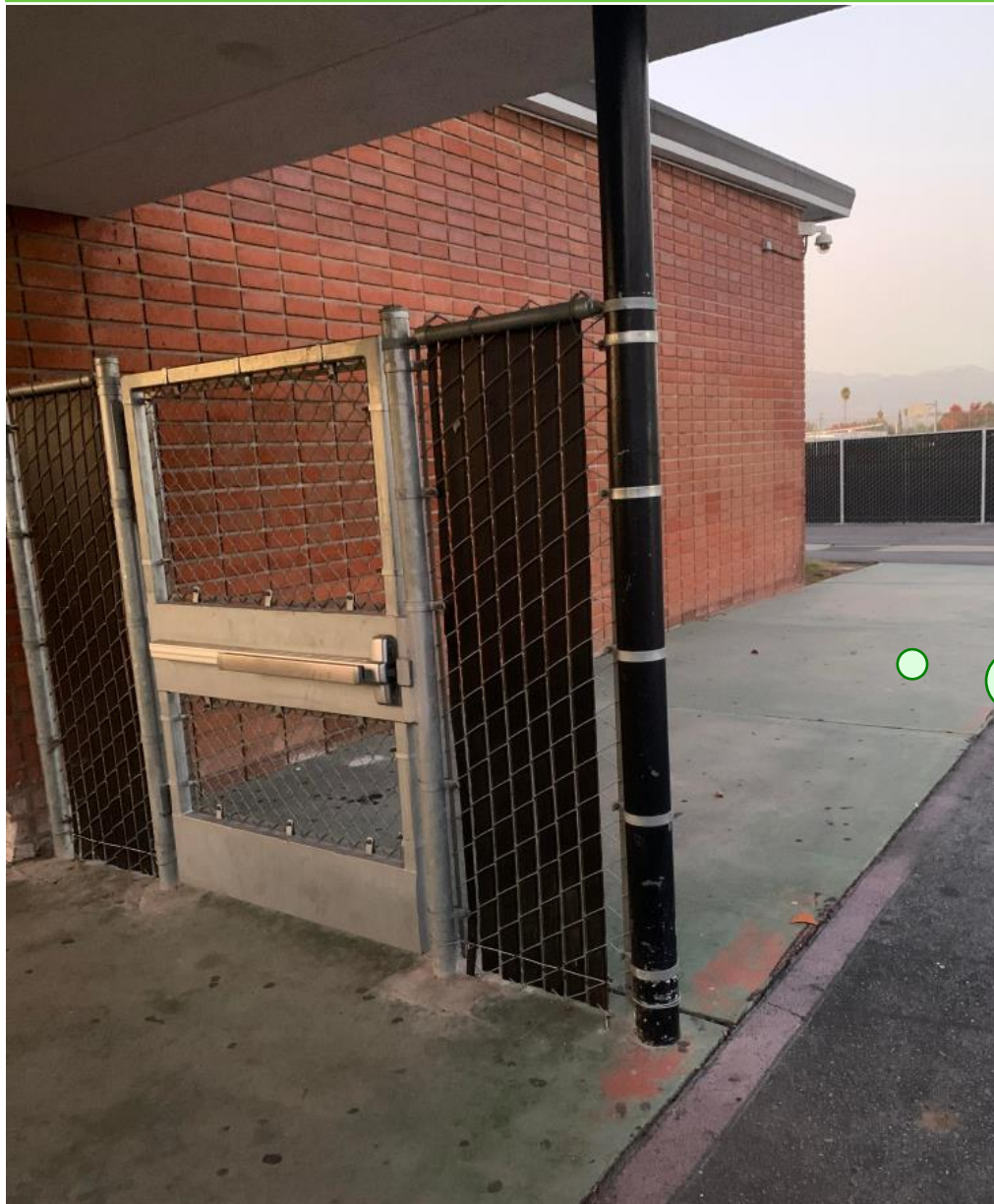
Finance Group	System 1	System 2	System 3
Jr. Finance Analyst	none	read	read & edit
Finance Analyst	none	edit	read & edit
Sr. Finance Analyst	read	read & edit	full: r, e + d
Supervisor	read & edit	read & edit	full: r, e + d
Dept. Leader	full: r, e + d	read & edit	full: r, e + d
Executive	read only	full: r, e + d	approve only

Never grant access based on another person's current access

- Align access to **roles** *ONLY*
- Gather **approvals** for any add'l access
- Update access each time there's a **role change**
- Identify entire scope for **terminations**
- Consider **LOA**

INCLUDE NON-EMPLOYEE WORKERS

More than just a checkbox



Which controls have been met?

- Camera in place
- Physical access restricted
- Visibility limited

Do these checkboxes mean this area is secure?

*Prioritizing satisfying the checkbox is
our LARGEST vulnerability right now*

*We must pivot and create governance
that actually makes sense*

Skipping appropriating & aligning

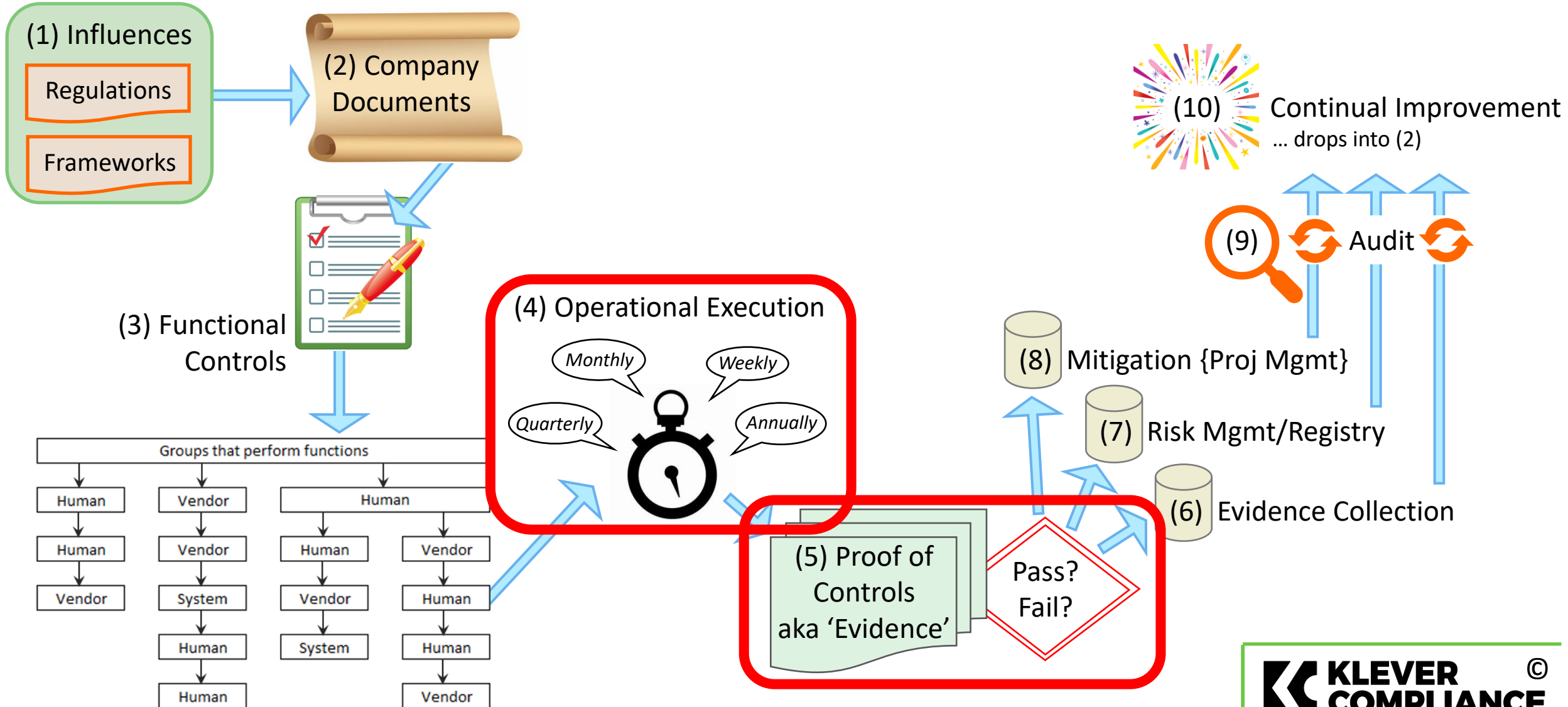
Will cripple your GRC Program

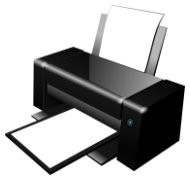


You will get waaaaaaay more than what's needed or useful

- Too many controls
- Controls that don't apply to your company
- Vaguely written controls
- Controls that have nothing to do with your actual operations
- No clue who owns which control
- Missing system:system references
- Fluffy executables that happen "sometimes", "occasionally" or "periodically" with "deep concern"

Core GRC Flow of Work





(4) Operational Execution



Controls in action!

The specificity of the controls must include the frequency of operationally executing that control

- Executed controls across the company must be tracked
- Vendors/Third Parties may contribute to executed controls
- Execution is proof that the control exists (aka 'Evidence'); Evidence must route correctly
- Over time the controls that are behaving as designed ... become automation candidates

- Execution instructions are very specific within controls including
 - Timing
 - Ownership
 - Target outcome & **success/fail criteria**

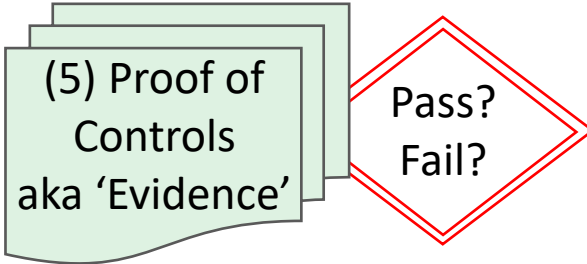


- Proof of executed control(s) appropriately routed
- Focuses on internal operations
- Automation candidate controls are identified
- System: System control executions are accounted for
- Dependencies and instructions for gathering evidence from vendors/third parties is accounted for

(5) Proof of Controls

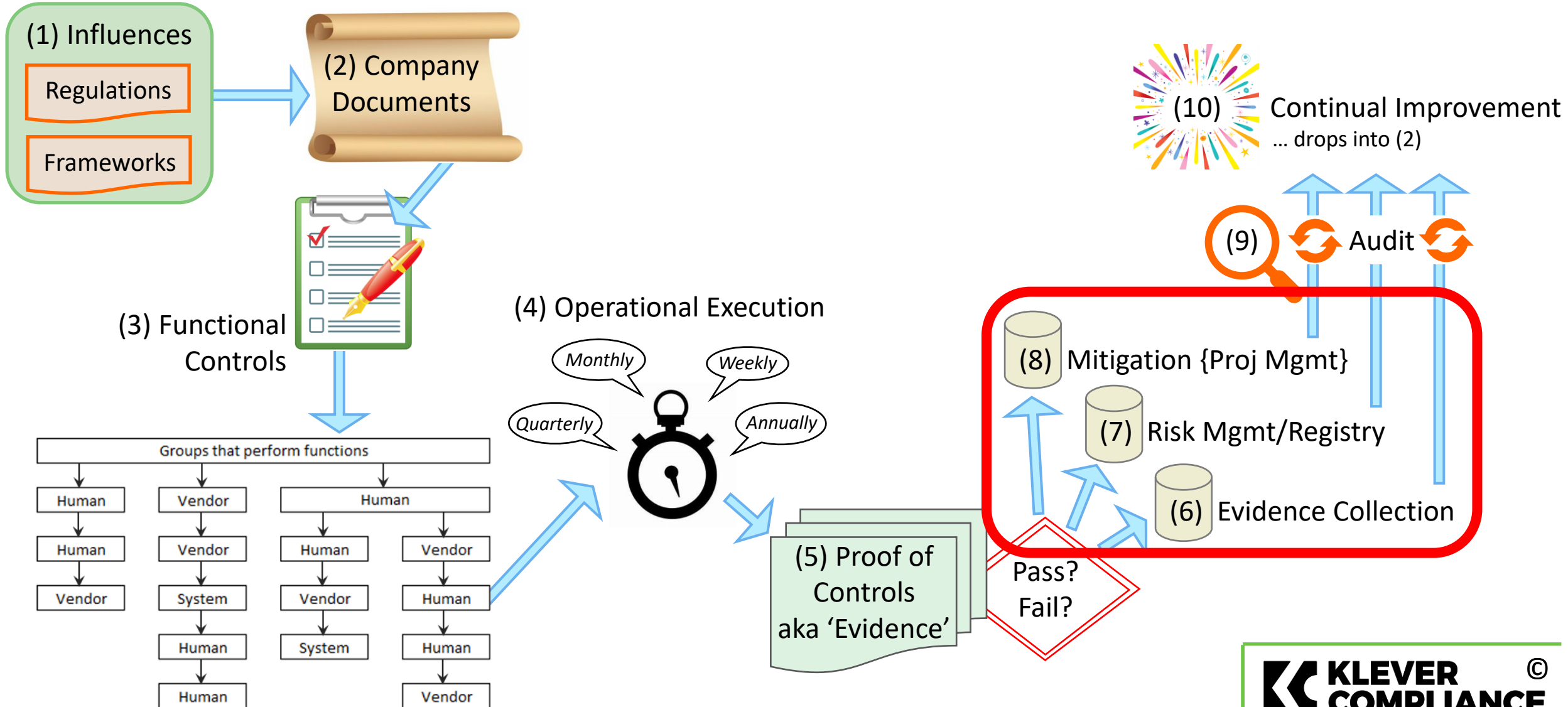
Evidence combined with control success/failure determination...

- Fulfills regulatory/framework requirements
- Identifies highest risks faster & easier
- Invites collaboration with other groups (accept the invite)
- Supports audit readiness (internal & external audits)
- Can count as “self-audits” (required for some regulations/frameworks)
- Nirvana: Evidence collected via automation
- Shapes continual improvement of GRC COE



Don't allow these folks to be bothered more than absolutely necessary!

Core GRC Flow of Work



(6) Evidence Collection

Organization is # 1 trick!



Few options on how to store:

- Per competency or document (control)
 - Incident Mgmt
 - Change Mgmt
 - ... etc
- Per data type
 - Sensitive Data controls
 - Public Data controls
 - ... etc
- Per audit or certification cycle
 - Auditor Type (internal, external, federal, etc)
 - Target (SOX, HIPAA, ISO, etc)

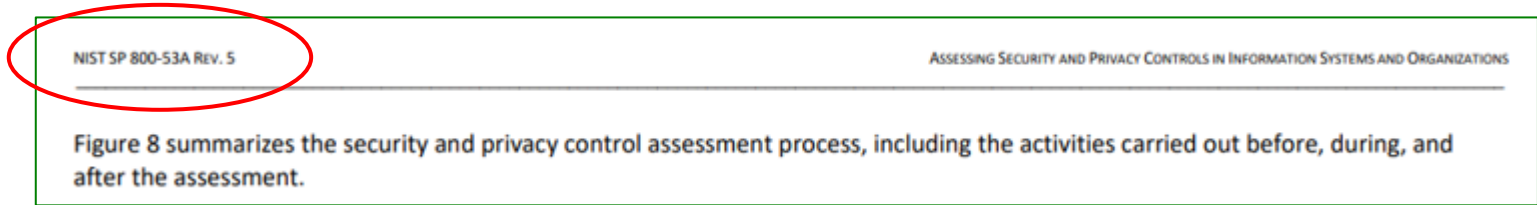
You want to repurpose these over & over & over & over & ...

Establish a standard & stay consistent!

(7) Risk Mgmt or Risk Registry

First type of “risk”

Based on Risk Framework

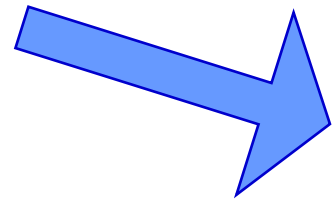
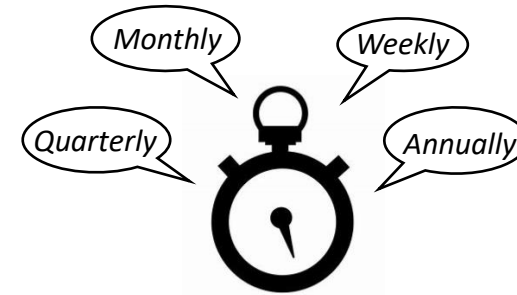
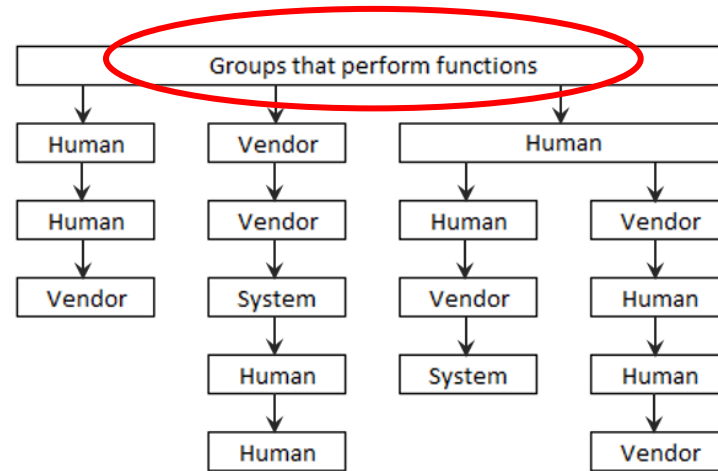


CIS Risk Assessment Method (RAM)



(7) Risk Mgmt or Risk Registry

Second type of “risk”: Based on **YOUR CONTROLS**

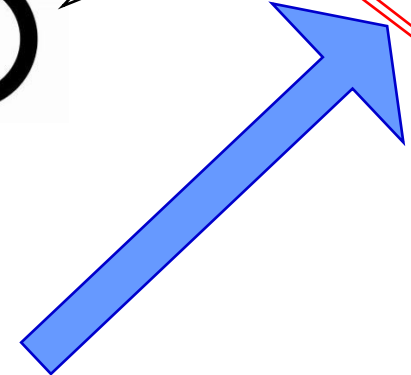


Log onto risk registry

Prioritize & align to corp priorities

Update GRC COE Dashboards & Metrics

Create mitigation plans & projects



(8) Mitigating Efforts

Identifying your own mitigation needs, shows maturity...

- Auditors love it!
- Executives love it!
- Eeeeeveryone loves it!

Just be sure to track mitigation seriously!



Search bar containing the text: "type of project management methodologies" with a microphone icon and a search icon.

About 27,600,000 results

Project management methods or models

Generated using AI



AGILE
Project management principle



Kanban
Visual workflow method



Extreme programming
Fast-paced project method

Critical chain project management (CCPM)
Resource leveling method



Waterfall
Linear project methodology



PRINCE2
Controlled environment method

Scrumban
Hybrid of Scrum and Kanban

Lean
Waste reduction method



Scrum
Agile sprint cycle method

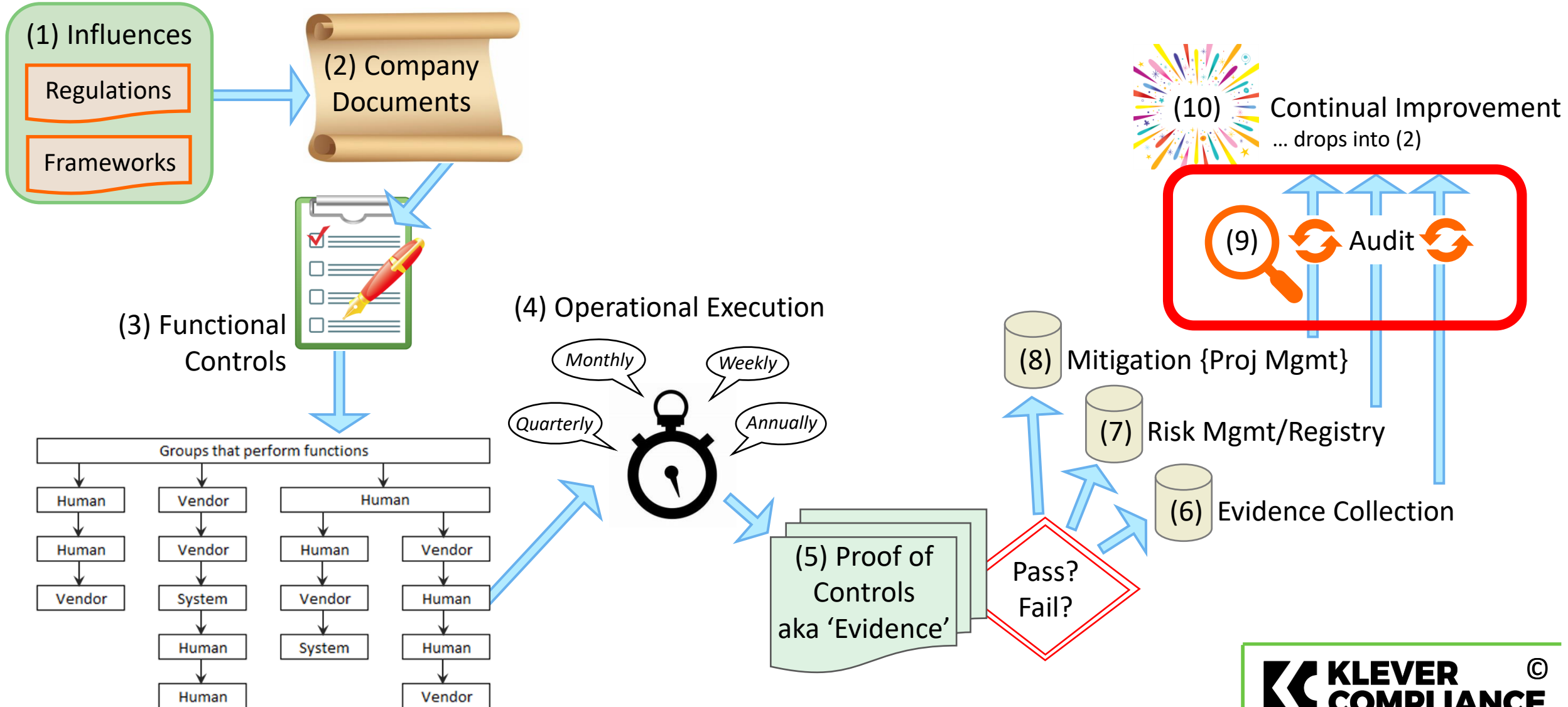


Critical path method
Task dependency method

Six Sigma
Quality management philosophy

PMBOK® Guide
Project management best practices

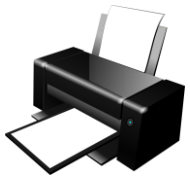
Core GRC Flow of Work



Don't over-complicate the audit unnecessarily



- ✓ Show off how well organized you are!
- ✓ Don't provide more than what's asked
- ✓ Evidence should have been being passively & actively collected
- ✓ Watch for silence
- ✓ Watch for 'favors'



(9) Audit



“Audit” is a massive competency

Remember, auditors know what the regulations/frameworks say. They want to see how you implemented the controls for your company

Prepare for your audit or certification

- Facilitate any audit engagement notice clarifications
- Gather and prepare audit scope relevant evidence
- Preemptively coach SMEs on being audit-facing
- Warning to technologists!

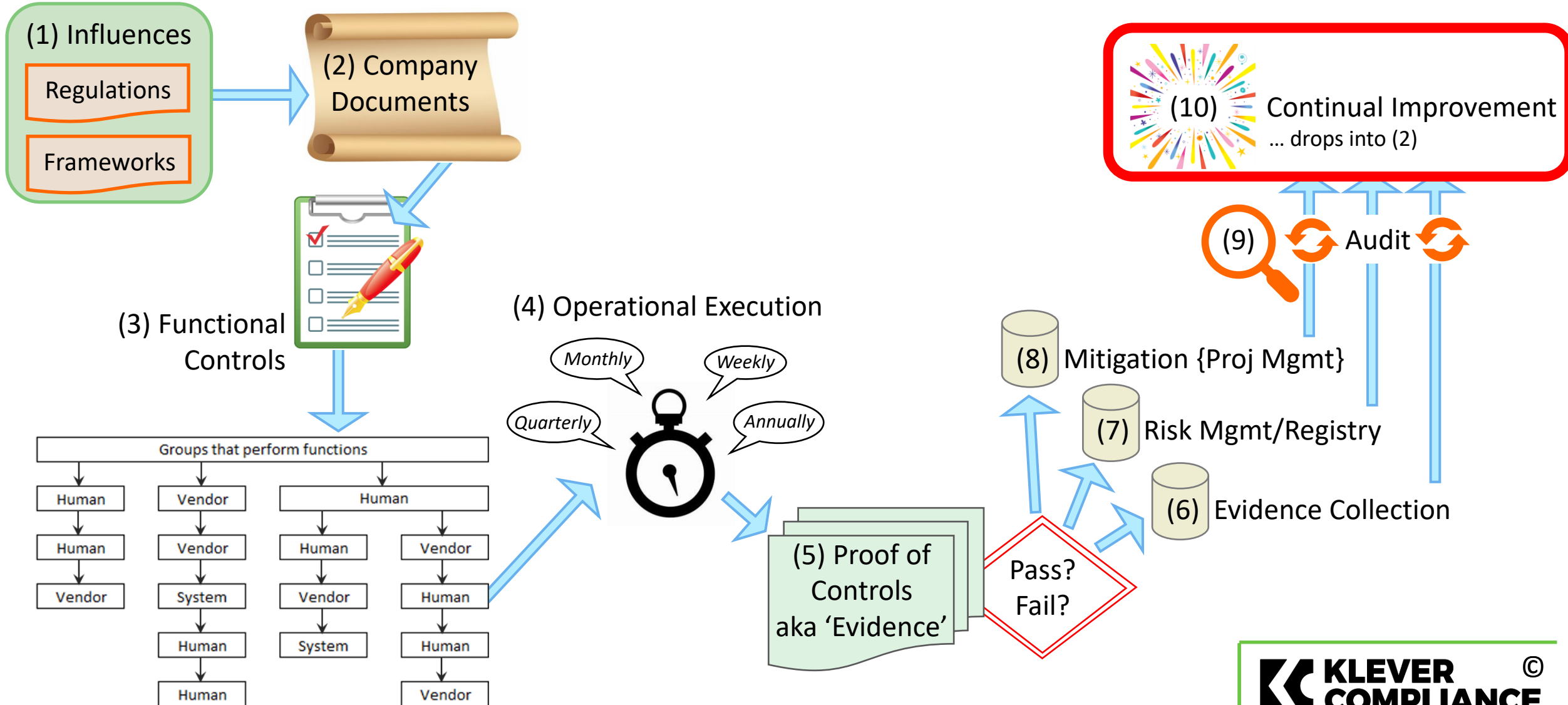
Be an active participant & engaged

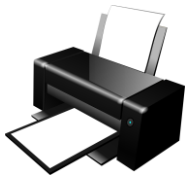
- Coordinate execution
- Monitor progress
- Internal escalation as needed
- Return cycle readiness at close of engagement

Remediate audit or certification opportunities

- Track items to completion using native project tracking mechanism
- Maintain active reporting
- Update internal & external participants (statuses & completion)

Core GRC Flow of Work





(10) Continual Improvement



(10) Continual Improvement
... drops into (2)

The entire GRC Flow of Work can, and should be, used to improve company operations and significantly elevate maturity

Give Continual Improvement focus by actively tracking opportunities derived from Functional Control (3) effectiveness, Failed Evidence (5), and prioritized Risks (7)

Actions which support continual improvement

This service maintains an active actionable ledger of lessons learned and opportunities to intelligently enact data-driven changes across the company

- Baseline current effectiveness
- Decompose targets into approachable deliverables
- Track origination and significance of each improvement opportunity
- Integrate back into GRC Flow of Work
- Measure improvements from baseline over time



Thanks for joining!

Follow Klever Compliance (LinkedIn only)

<https://www.linkedin.com/company/klevercompliance>

Karina's profile

<https://www.linkedin.com/in/karinaklever>

Calendly

<https://calendly.com/klevercompliance/intros-or-catch-ups>

Contact

Karina@KleverCompliance.com

Office: 747.800.1568

Cell: 818.326.8667

