Welcome

March 27, 2024
OWASP-LA
Welcome

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

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
   - Regulations
   - Frameworks

(2) Company Documents

(3) Functional Controls

(4) Operational Execution
   - Monthly
   - Weekly
   - Quarterly
   - Annually

(5) Proof of Controls aka ‘Evidence’
   - Pass?
   - Fail?

(6) Evidence Collection

(7) Risk Mgmt/Registry

(8) Mitigation {Proj Mgmt}

(9) Audit

(10) Continual Improvement
     ... drops into (2)
(1) Influences: Frameworks
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
Our books are balanced. 50% of our numbers are real and 50% are made up.
(1) Influences: Regulations

Timeline governing ePHI/PHI

- **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
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!

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?

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

(1) Influences
- Regulations
- Frameworks

(2) Company Documents

(3) Functional Controls
- Groups that perform functions

(4) Operational Execution
- Monthly
- Weekly
- Quarterly
- Annually

(5) Proof of Controls aka 'Evidence'
- Pass?
- Fail?

(6) Evidence Collection

(7) Risk Mgmt/Registry

(8) Mitigation {Proj Mgmt}

(9) Audit

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

---

**Warning about templates!**

- Occasionally
- Periodically
- Routinely
- From time to time
- Frequently
- Recurringly
Data Classification

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

Make sure all your types of data or information are addressed

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

Forces identification of
- The data
- The groups/systems/vendors somehow leveraging data
- Supporting information

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 requires rigid destruction practices
  - Get that confirmation!

- Which data type gets backed up & when?
  - Tiering
  - Recovery requirements
## Groups that perform functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Management</td>
<td>Asset Management</td>
</tr>
<tr>
<td>Access Management</td>
<td>Problem Management</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>Human Resources</td>
</tr>
<tr>
<td>Patch Management</td>
<td>Encryption Management</td>
</tr>
<tr>
<td>Change Management</td>
<td>Data Management</td>
</tr>
<tr>
<td>Procurement / Vendor Mgmt</td>
<td>Risk Management</td>
</tr>
</tbody>
</table>

There can be more. Maybe this is too many.
A word about access control

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 waaaaaaaaay 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

(1) Influences
- Regulations
- Frameworks

(2) Company Documents

(3) Functional Controls

(4) Operational Execution
- Monthly
- Weekly
- Quarterly
- Annually

(5) Proof of Controls aka ‘Evidence’
- Pass?
- Fail?

(6) Evidence Collection

(7) Risk Mgmt/Registry

(8) Mitigation {Proj Mgmt}

(9) Audit

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

Pass? Fail?

Don’t allow these folks to be bothered more than absolutely necessary!
Core GRC Flow of Work

(1) Influences
- Regulations
- Frameworks

(2) Company Documents

(3) Functional Controls

(4) Operational Execution
- Monthly
- Weekly
- Quarterly
- Annually

(5) Proof of Controls aka ‘Evidence’
- Pass?
- Fail?

(6) Evidence Collection
(7) Risk Mgmt/Registry
(8) Mitigation {Proj Mgmt}
(9) Audit
(10) Continual Improvement

… drops into (2)
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

Figure 8 summarizes the security and privacy control assessment process, including the activities carried out before, during, and after the assessment.
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
Identifying your own mitigation needs, shows maturity...
• Auditors love it!
• Executives love it!
• Everybody loves it!

Just be sure to track mitigation seriously!
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’
“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

(1) Influences
- Regulations
- Frameworks

(2) Company Documents

(3) Functional Controls

(4) Operational Execution
- Monthly
- Weekly
- Quarterly
- Annually

(5) Proof of Controls aka ‘Evidence’

(6) Evidence Collection

(7) Risk Mgmt/Registry

(8) Mitigation {Proj Mgmt}

(9) Audit

(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

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

Contact
Karina@KleverCompliance.com
Office: 747.800.1568
Cell: 818.326.8667

Karina’s profile
https://www.linkedin.com/in/karinaklever