How can SRE help Security Governance?

How to unstuck GRC with SRE

@madplatt
whoami

Director of Governance, Risk Management and Compliance for Security and Privacy @ LastPass

20+ years in tech, 18+ in Security. Penetration tester, Ops and Engineering, GRC and Leadership (Head of and CISO roles) and former consultant (vCISO/Interim CISO, Fractional CISO)
Project leader for “ASVS User Stories” open source project
Course instructor for “DevSecOps for Leaders” course on practical-devseccops.com
Speaker and enthusiast on Wardley Mapping, Cynefin framework, Safety Science, Resilience Engineering all applied to Security
the compliance guy?

really?
What is GRC?

“the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity” from Wikipedia

**Governance** – aligning processes and actions with organisation’s business goals

**Risk Management** – identifying and addressing organisation’s risks

**Compliance** – ensuring activities meet legal, contractual and regulatory requirements
But… we’re a bit stuck… we are
The G & the C are stuck

- Stuck in command and control and centralised governance models
- Framing of the security “problem” as one of awareness, and not goal conflicts and trade-offs (that we’re often unqualified to appreciate)
- Detached from operational realities (hierarchical information filters)
- Actually fabricating business liabilities in the name of “best practice following”. Policies largely impractical
The R…. is also a bit stuck

Risk-management-as-Imagined

Risk Management as defined in ISO 3100 and ISO 27005
Risk-management-as-Done

Work as Imagined

Risk and Compliance Managers

Risk analysis process

Controls Top Hat

Operation A
Team 1

Operation B
Team 2

Training and ingrained patterns (bias)

Accepted Industry best practices

“We see what we expect to see”
Stuck between what “oughta be” and “what actually is” and not knowing how to reconcile the difference constructively.
WHAT DOES THIS HAVE TO DO WITH SRE?
My soap-box schpiel:

The practices and structures to allow governance of technology, management of operational risk (including reliability) and enforce operational standards that SRE embeds... can be leveraged to manage security objectives, meeting and evidencing GRC goals.
The G and the C often have broken team dynamics with Engineering

Control... blah blah ..... control.... Blah.... Governance... blah... Risks.... Blah... Compliance....blah blah blah Boogey man at the door

Wall of Confusion and Despair

Features... bah blah... that looks cool.... Blah blah... Speed.... Argh can't get that function to work blah blah They won't get out of the way...

Control testing
Testing procedures
Evidence review
Checklists and spreadsheets
Compliance to
Risk analysis and uncertainty

Code
Tools
Processes and procedures
Delivery artefacts
Specifications
Sprints and Stories

@madplatt
Artefacts matter... they set the scene for collaboration (or lack thereof)

Having to ask the compliance team for feedback

Getting compliance feedback from CI/CD

@madplatt
SRE can help the G and the C

What’s already there to leverage?

- Answering “how much” through error budgets, SLIs, and SLOs
- Engineering and Ops know-how to understand constraints and trade-offs
- Levelled the playing field on Reliability concerns
- Readiness reviews and standards enforcement
- Managing toil
- Codification of policies in process
Between the C and the R - automated governance

Stage 1: Source Code Repository

Figure 4 shows a generalized overview of what an automated governance model might look like during the source code repository stage.

<table>
<thead>
<tr>
<th>Risks</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Unapproved changes</td>
<td>1. Peer review</td>
</tr>
<tr>
<td>2. Untested changes</td>
<td>2. Unit test coverage</td>
</tr>
<tr>
<td>3. Unapproved 3rd party dependency</td>
<td>3. Clean dependency</td>
</tr>
<tr>
<td>4. Information (secrets) leakage</td>
<td>4. Scan for sensitive information</td>
</tr>
<tr>
<td>5. Low quality code sent to production</td>
<td>5. Static code analysis/linting</td>
</tr>
</tbody>
</table>

Figure 4: Governance during the Source Code Repository Stage

DevOps Automated Governance Reference Architecture

Attestation of the Integrity of Assets in the Delivery Pipeline

John Willis - https://jfrog.com/user-conference/devops-automated-governance/
Governance and Compliance

- Oversight of metrics management
- Oversight of standards enforcement
- Negotiation of policy statements
- Influence prioritisation of codification of policies in process
- Define security standards to comply with
- Collaborate on artefact creation

SRE (Security)

- Report on security metrics and trends (error budgets)
- Report on policy enforcement and compliance
- Request or review policy exemptions
- Report on readiness reviews
- Input into strategy and security programme roadmap

Engineering & Operations

- Collaborate on automated governance deployment
- Support in deploying / planning compliance automation and tagging against security standards
- Ensure suitability of artefacts

- Request support in operationalising security compliance and automation
- Report on user experience of compliance

Observability of actions (feedback loops)

@madplatt
Work as planned vs. work in practice

“Workers are masters of the blue line.”

- Conklin/Edwards

On managing (operational) risk

Figure 3. Under the presence of strong gradients behaviour will very likely migrate toward the boundary of acceptable performance.


@madplatt
On managing (operational) risk

Adapted from Jens Rasmussen

@madplatt
On modelling product risk

Hierarchically-aligned model

Product-oriented model
Managing risk requires multiple strategies

Figure 7. Hazard source characteristics and risk management strategies.
(Vulnerability) Error budgets

Security Chaos Engineering

https://www.usenix.org/conference/srecon19americas/presentation/thomson
On Learning

Learning from (security) incidents

Learning from normal work

Howie, https://www.jeli.io/howie/welcome

“Learning organisations become graduate studies in the skills they require to be successful” @littleidea

https://www.learningteamscommunity.com/
Key Take-aways

- Traditional GRC functions are stuck. We’re largely bringing spreadsheets to a declarative fight.
- Work as imagined by “gatekeepers” and work as done by practitioners isn’t the same.
- SRE metrics embed good governance of competing goals. Why not Security?
- SRE Readiness practices can be leveraged to ensure a pragmatic level of capability in the teams to manage their own product components. Why not Security?
- SRE community is years ahead in (actual) learning from incidents. Why not Security?
- SRE’s conception (and therefore management) of risk is more aligned to the dynamic reality of operations and how surprises happen. Why not Security?
Thanks.
Questions ?
Comments ?