RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: CSV-T09

One Approach to Rule Them All—Global Privacy and Security

Bill Burns
VP & Chief Information Security Officer
Informatica
@x509v3

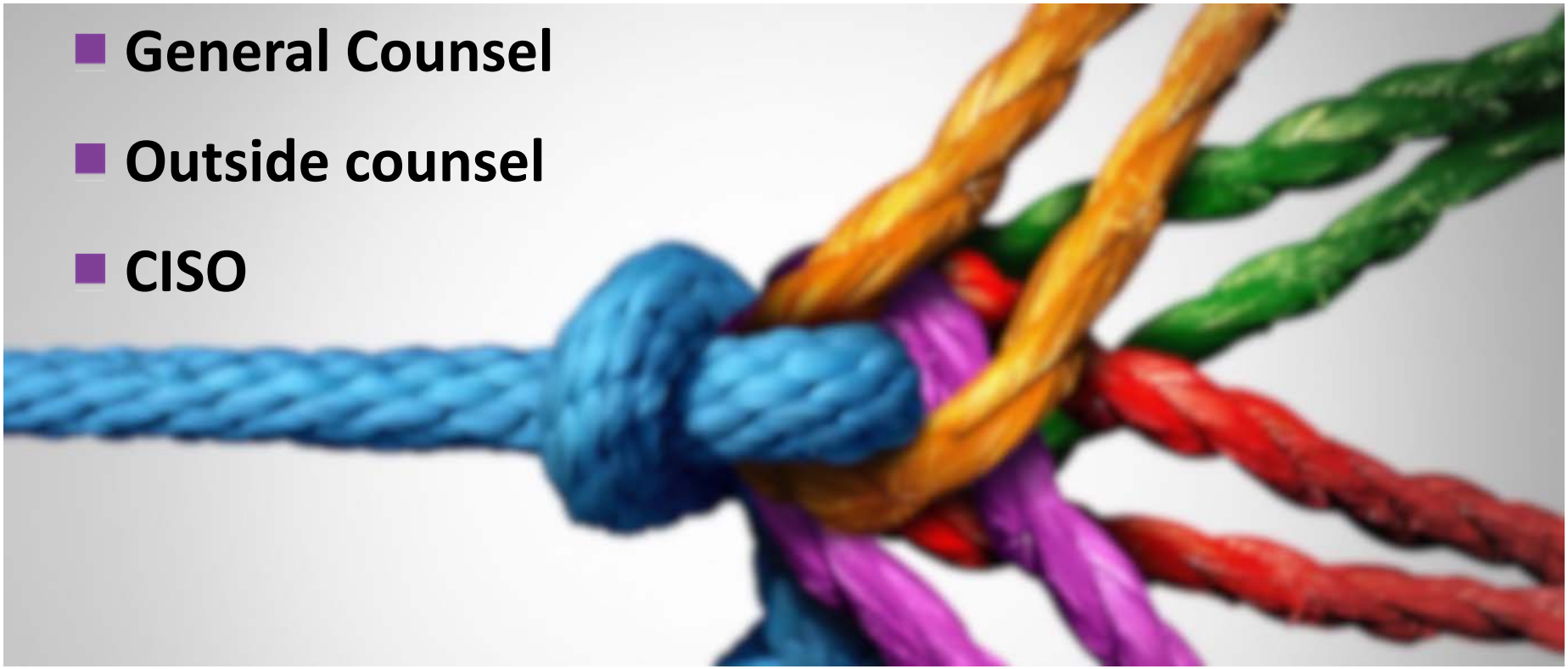
Katherine Haar
General Counsel
Informatica
@kikihaar

Todd Hinnen
Partner
Perkins Coie LLP

What is your Frame of Reference?

Three perspectives … and a plan

- General Counsel
- Outside counsel
- CISO



Context: Who is Informatica?

- Global, multi-national enterprise software company focused on all things data
  - Originally founded 1993, IPO 1999, taken private 2015
  - Over $1B in annual revenue
  - Over 5,800 enterprises in more than 80 countries depend on INFA
  - Nearly 3,600 employees in over 25 countries
- Subject to many different security and privacy regulations

Informatica: What's Changed? Why Now?

- Customer-driven:
  - Was: On-premise products & orchestrating cloud workloads
  - Now: Trusted cloud service provider handling data directly
- Workforce-driven:
  - Evolving concerns and questions
  - Security and privacy controls, regulations
- Supplier-driven:
  - Protecting our employees' data
  - Growth of our infrastructure globally
  - Proliferation of SaaS applications

Evolving Global Privacy, Security Focus

- Increasing attention to privacy globally
- New laws and regional frameworks
- More transnational data flows
- Enforcement authorities more active, aggressive
- Significant changes in laws and frameworks
  - US EU Safe Harbor unlawful by ECJ (Oct 2015)
  - US EU Privacy Shield(?!)

Outside counsel perspective

- Help understand and avoid legal risk.
- Help dedicate appropriate resources.
- Help organization communicate among different stakeholders, components.
- Help translate law into tech, into sales.
- Help develop policies and procedures consistent with client's culture, business objectives.

informatica PERKINSCOIE COUNSEL TO GREAT COMPANIES

Privacy Governance 101

- Good privacy and data security begin with understanding the data you have, and what you do with it.
  - Collect, store, secure, use, share, and dispose of it.
- Privacy and data security are company-wide endeavors
  - Oversight of the Board of C-Suite
  - Company-wide program managed by relevant stakeholders
- Policies, procedures, training, and enforcement
- FIPPs, EU Data Protection Directive, APEC Privacy Framework, FTC Publications & Guidance

Global Privacy Challenges & Opportunities

- Meeting the idiosyncratic requirements of particular jurisdictions
- Creating a global program that accommodates cultural, legal differences
- Developing tailored, “novel” approaches (?)
- Striking a balance between
  - security / privacy
  - US law / foreign laws
  - Innovation / organizational tradition, culture

Alternatives – Data Transfer

- EU to non-EU
  - Standard / Model Contract Clauses
  - Binding Corporate Rules
  - Safe Harbor (now "US-EU Privacy Shield")* cy
- APEC, Australia, etc . . .
- Take a global approach
- Factors: cost, complexity, scalability, up front investment

* EU to US only

Alternatives and Options

- What options are available to US companies?
  - Standard / Model Contract Clauses
  - Binding Corporate Rules
  - Safe Harbor (now “US-EU Privacy Shield”)
- Outside EU and US options
- Cost, complexity, timing differences

CISO Perspective

- Most CISOs: tech, risk background
  - Embrace ambiguity, risk, contradictions
- Fundamental rights vs. best practices vs. good ideas
- Start with a solid data security policy foundation
  - Know your data, data flows, stakeholders, context
- 3rd party and intermediary risk

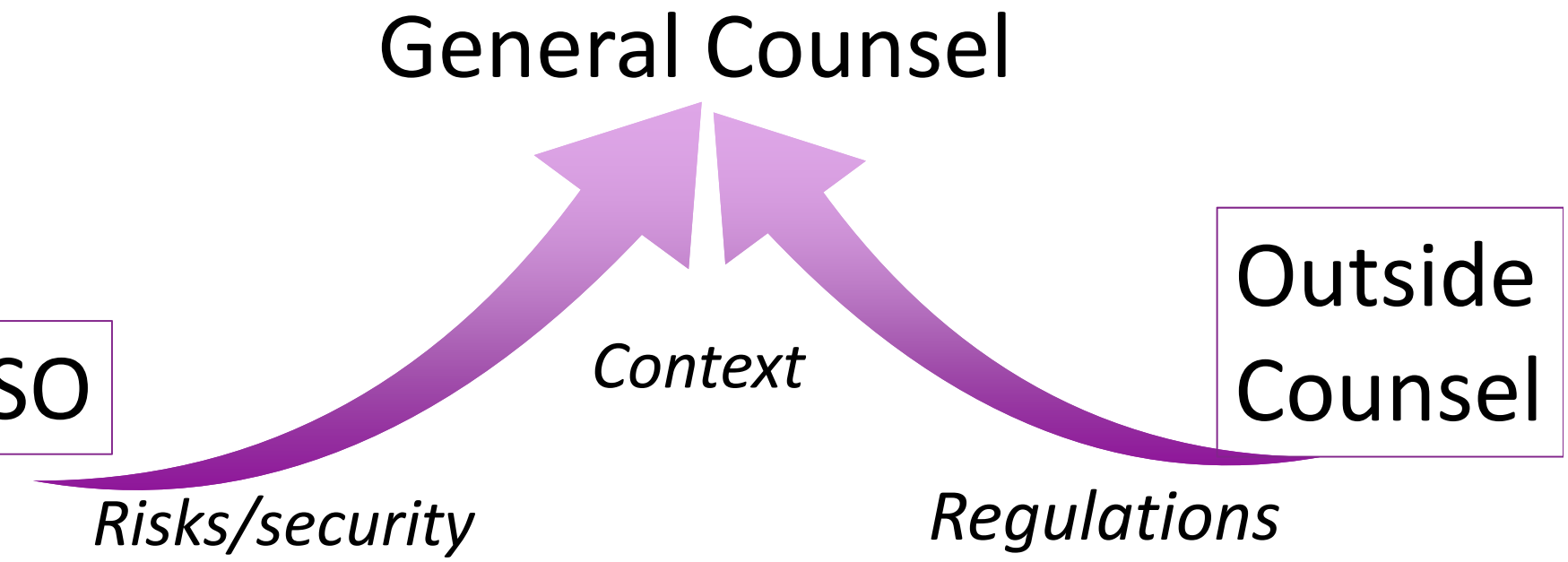
What it felt like

- Competing interests, priorities
- Conflicting guidance
- Out of date tech
- High stakes
- No standards

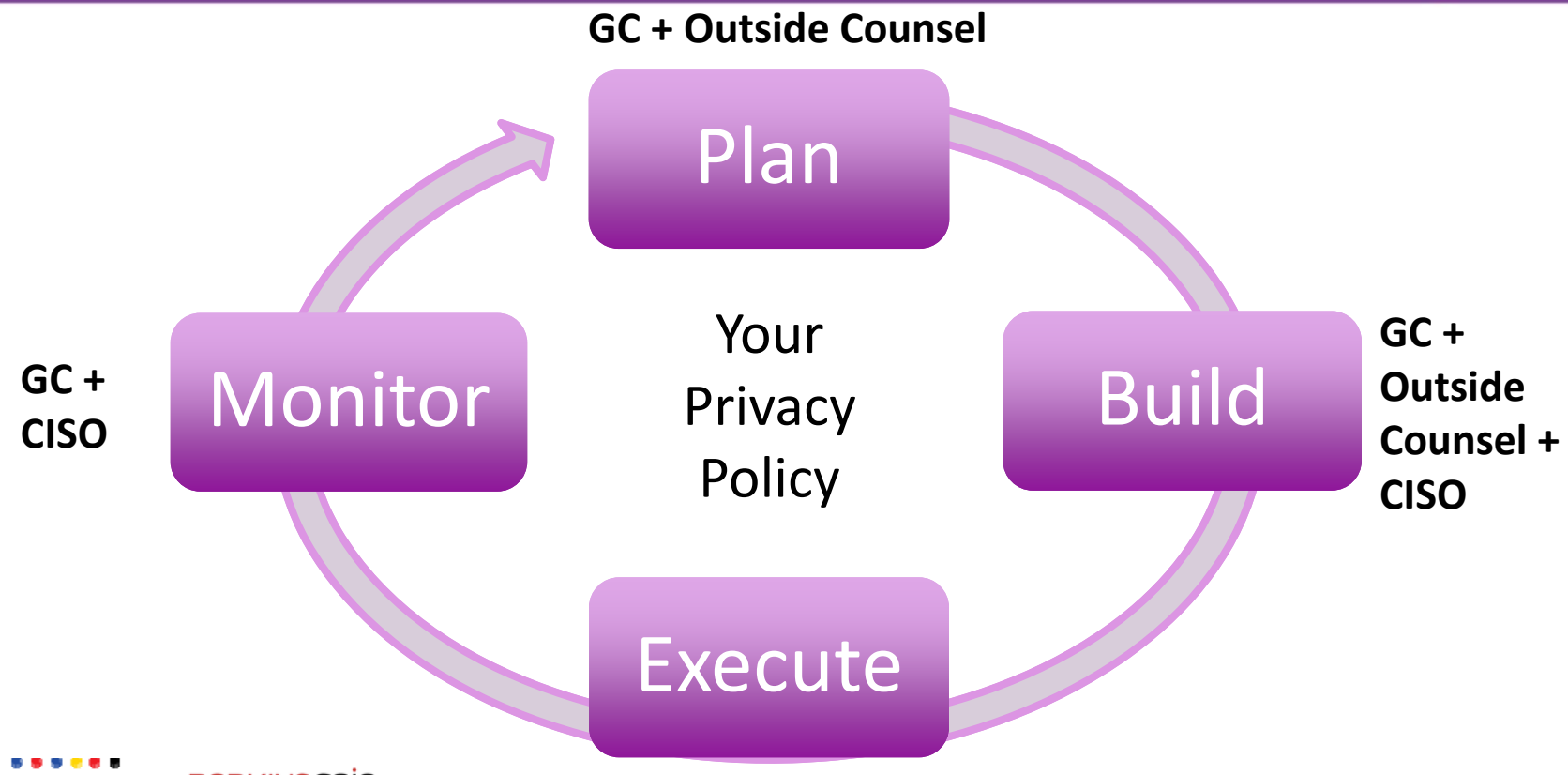
General Counsel Perspective

- GC is the Art of Balance, mediating between:
  - Outside counsel: external privacy regulations, laws
  - CISO: Internal security considerations, our context and needs
- My primary role is risk management
  - I rely on technical experts to translate the technical
  - CISO and I intersect on risk management
  - Outside counsel and I intersect on policy
- Plan → Build → Execute → Monitor metaphor

GC Is the Art of Balance & Mediation



Privacy Policy: Living Document



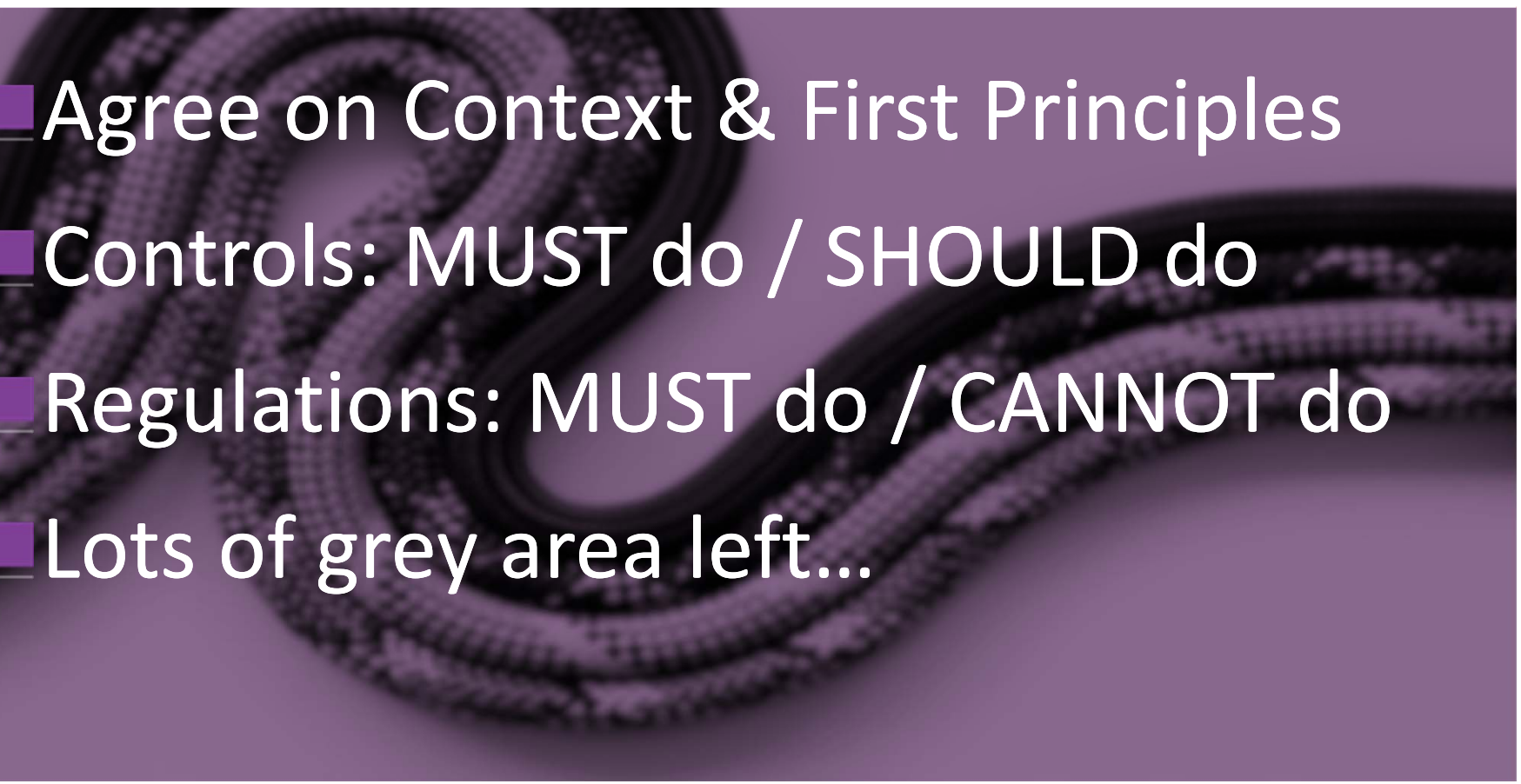
General Counsel Perspective

- My primary role is risk management
  - I rely on technical experts to translate the technical
  - CISO and I intersect on risk management, security
  - Outside counsel and I intersect on policy, regulations
- Plan → Build → Execute and Monitor metaphor
  - Plan: GC + Outside Counsel
  - Build: GC + CISO + Outside Counsel
  - Execute and Monitor: GC + CISO

Our Journey

- Started small, grew organically
- Decided to take holistic, global approach
- What we found successful
  - Business perspective and drivers
  - Executive sponsorship
  - Cross-functional engagement
  - Risk-scoping

Building The Matrix

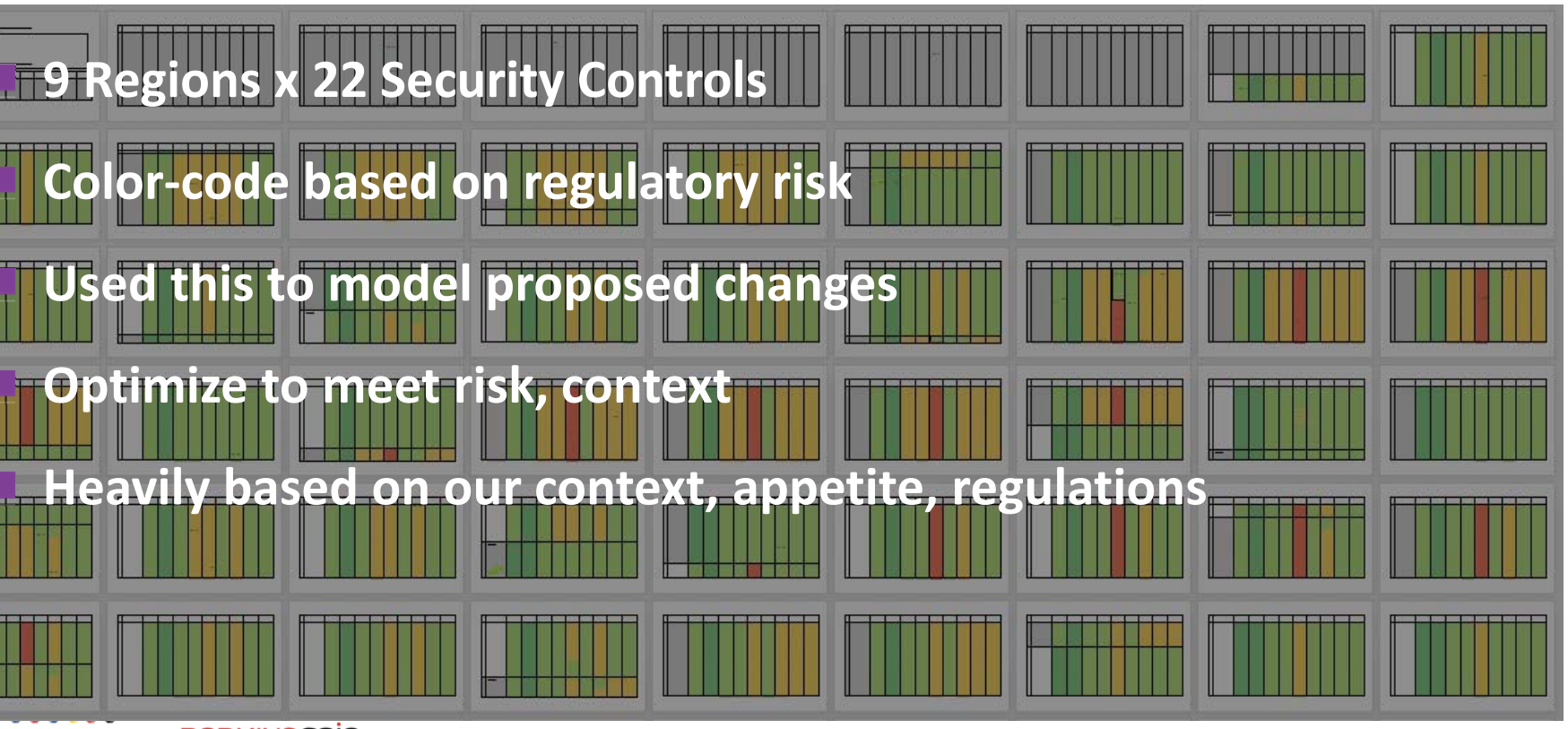


- Agree on Context & First Principles
- Controls: MUST do / SHOULD do
- Regulations: MUST do / CANNOT do
- Lots of grey area left…

What we did

- Outside expertise, opinion, case law
- Modeled use cases
- Residual risk

Our solution: The Matrix



- 9 Regions x 22 Security Controls
- Color-code based on regulatory risk
- Used this to model proposed changes
- Optimize to meet risk, context
- Heavily based on our context, appetite, regulations

The Matrix (sample)

Employee Data Security Control	Country1	Country2	Country3	Country4	Country5
Remote systems administration. Perform system administration remotely and access files on managed computers. Remote system administration and file access is only performed on company-owned laptops and desktops.	Notice and consent. Inform employees that their use of Company Devices, including files stored on Company	Notice and consent. Inform employees that their use of Company Devices, including files stored on Company	Notice and consent. Inf em tha use Cor De inc file on De	Notice and consent. l es, e, r use any files	No issue if nc If employee - Access to e - Access mus Notice to em Cross border If employee - the recipien

Key:

- Best Practice
- Low Risk
- Practical Risk or Law Unclear
- Not Permitted Under Local Law

What's Next for us: Monitor and Improve

- Matrix was helpful, we're evolving it
- Post-Safe Harbor world
- Need a mix of controls
  - More than one solution, based on your needs and context
  - Refer back to business drivers,

Apply: How Do I Get Started?

- Next week you should:
  - Take your CISO / GC out to lunch!
  - Discuss your company's context
  - Ice breaker: How does Privacy Shield affect us?

Apply: How Do I Get Started?

- In the next three months you should:
  - Sample some of your sensitive data and workflows
  - Describe the controls and int'l regulations involved
  - Partner with your GC / CISO, build the executive case
  - Seek executive sponsorship and budget
  - Do not proceed without this!

Apply: How Do I Get Started?

- Within six months you should:
  - Form your multi-stakeholder committee
  - Document your data, flows, stakeholder risk
  - Build your own region – controls matrix
  - Prioritize and address against the GDPR standard
  - Lather, rinse, repeat.