RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

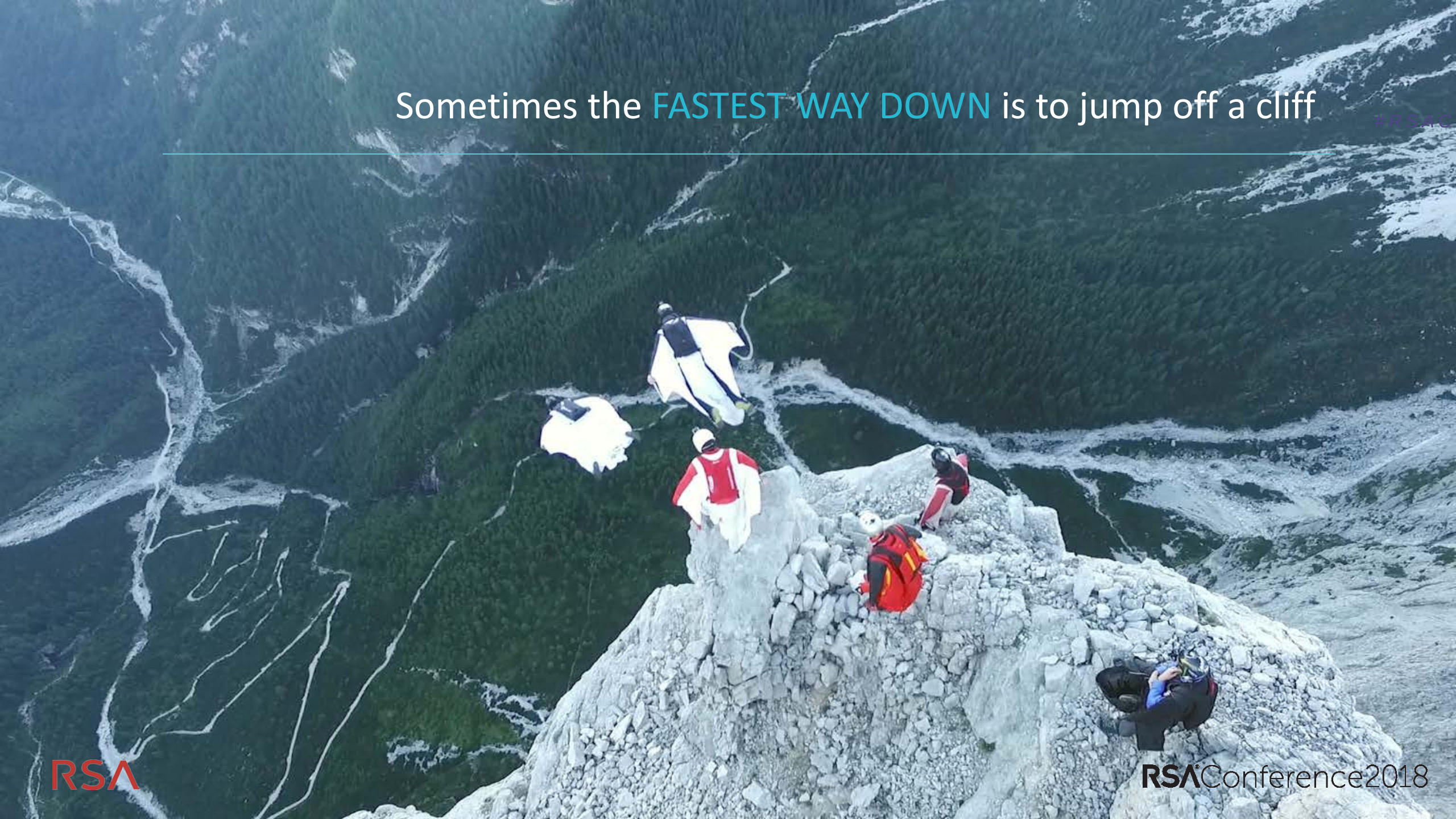
SESSION ID: SEM-M01

GET UP TO SPEED ON GDPR FAST

Rashmi Knowles CISSP

Field CTO EMEA
RSA

Sometimes the FASTEST WAY DOWN is to jump off a cliff



What is the EU General Data Protection Regulation (GDPR) & what impact will it have?

What is it?

- **Replaces EU's Data Protection Directive** with one EU regulation and is **effective 25 May 2018**
- **Significantly increases penalties** for violations– potential fines of up to **Euro 20M** or **4% annual turnover**
- **Definition of personal data –** is broader, includes online identifiers for example
- Much of what is included was in former Directive but some new requirements

Scope

GDPR applies to controllers & processors established **within** the EU & **outside** the EU where:

- they offer goods & services to individuals in the EU or
- their processing includes the monitoring of individuals' behavior within the EU, **thus substantially increasing those who are covered**
- Processors will have additional obligations that were previously reserved for controllers

Companies Must Also…

1 Tell individuals how their personal data will be used

2 Grant individuals access to correct or erase their personal data upon request

3 Comply with requests from individuals to stop using their personal data for marketing

4 Keep personal data secure

5 Make sure staff are appropriately trained in the care and handling of personal data

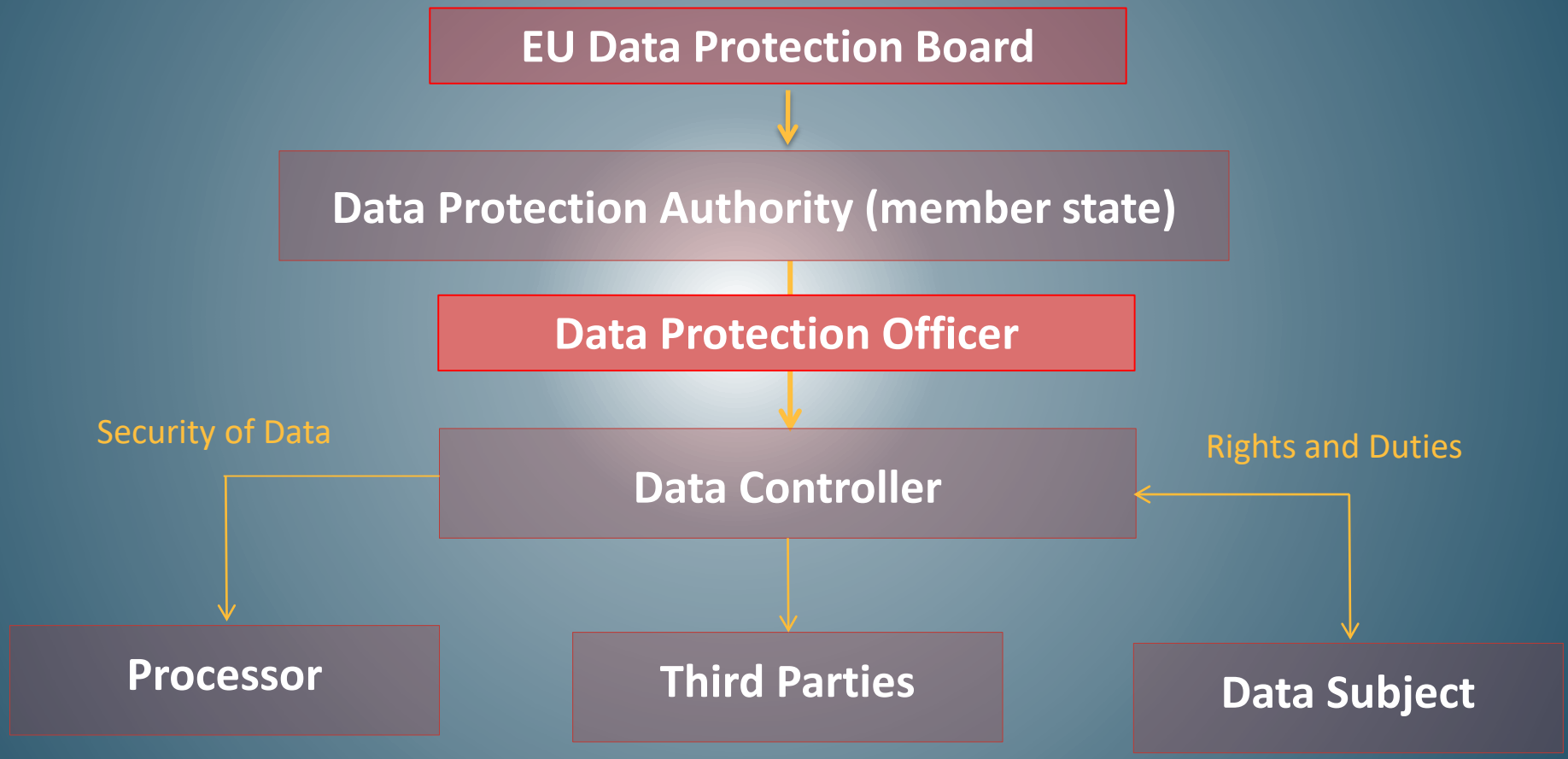
6 Put data processing agreements in place to ensure third party vendors follow the same protective rules

7 Notify regulators and/or affected individuals in the event of a serious data breach (usually within 72 hours)

8 Limit transfers of personal data out of the European Economic Area to only those that comply with EU international data transfer rules

9 Build privacy compliance into product, software and services design, processing tools and system development

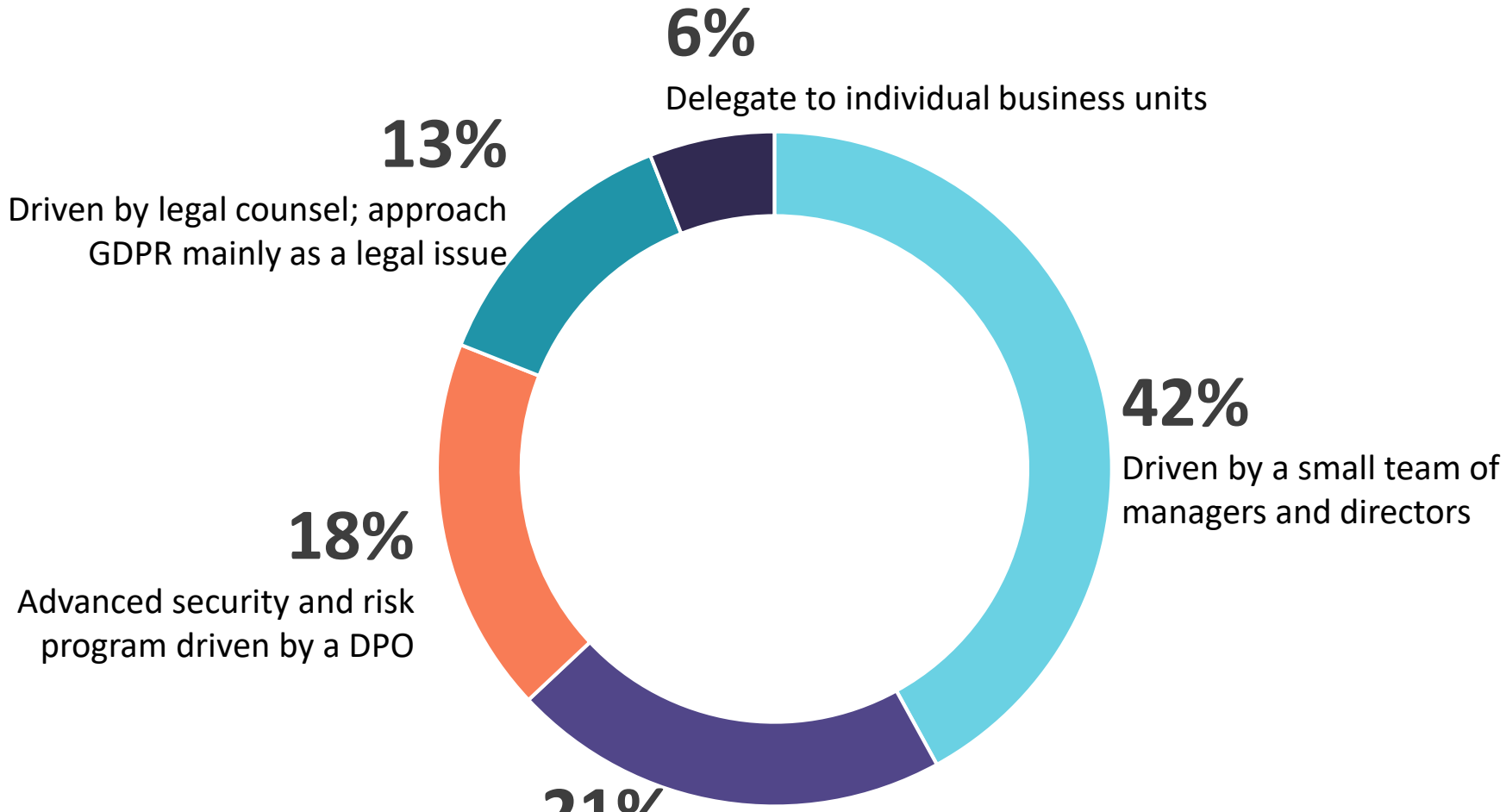
Who's who in GDPR



Where Are We Today?

RSA

Which of the following statements best describes the current state of GDPR compliance operations in your organization?



Source: A commissioned study conducted by Forrester Consulting on behalf of RSA, October 2017

Polling Question #1

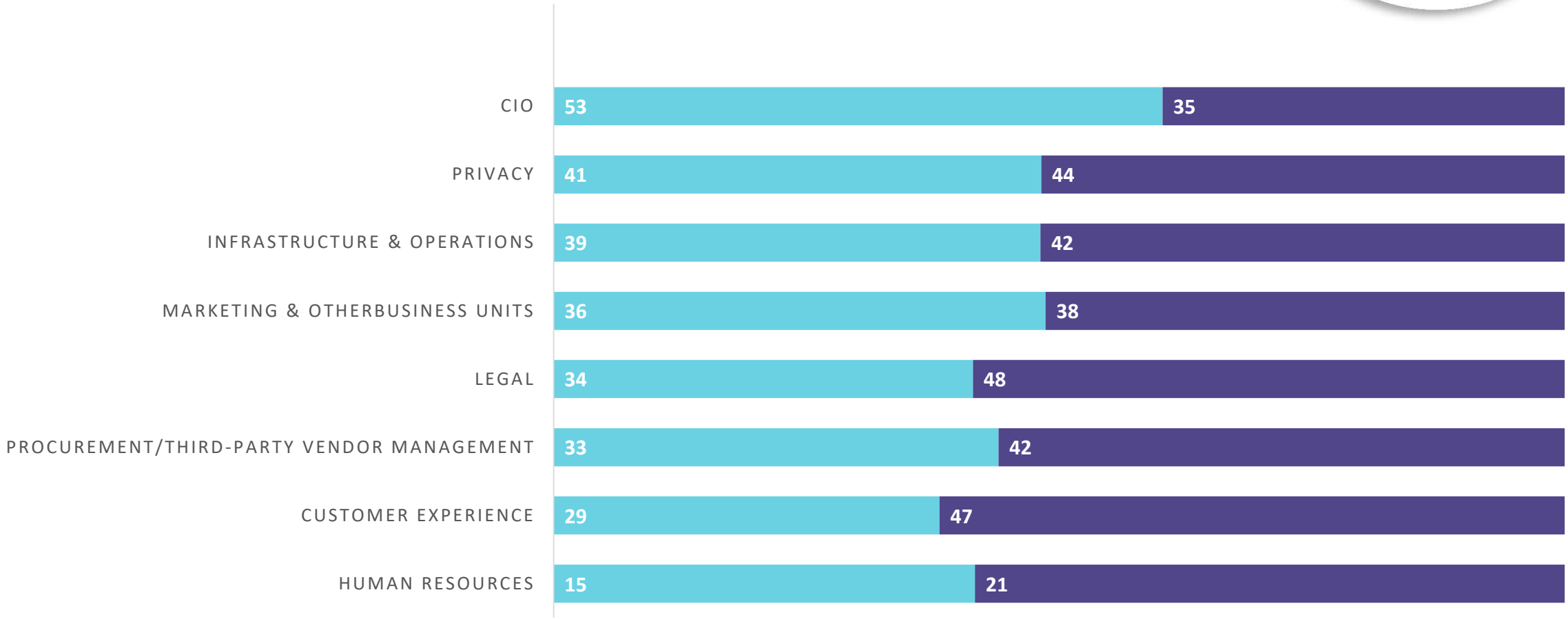
Who is driving your organization towards GDPR?

CISO
CIO

Compliance
Team

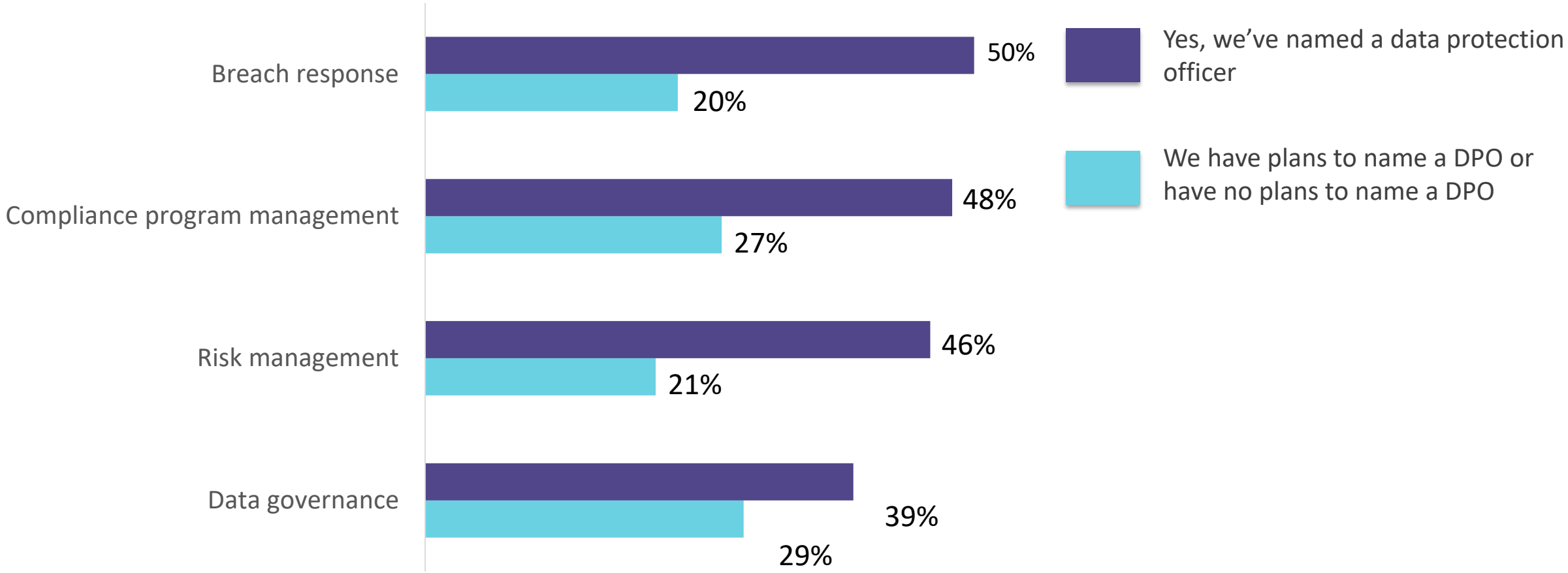
Other

How involved are the following teams in driving your organization toward GDPR compliance?



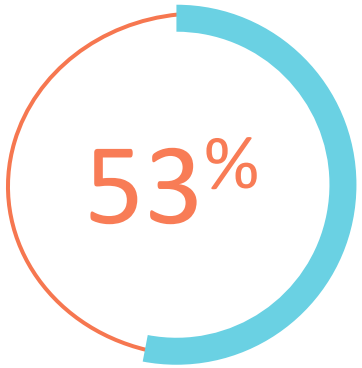
Source: A commissioned study conducted by Forrester Consulting on behalf of RSA, October 2017

What is your organization's timeline for achieving full GDPR compliance across the following requirements?

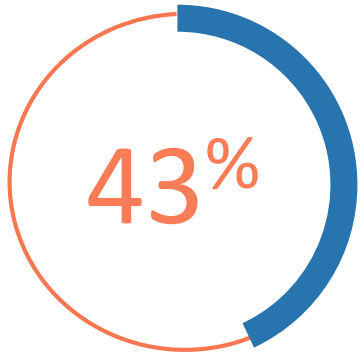


Source: A commissioned study conducted by Forrester Consulting on behalf of RSA, October 2017

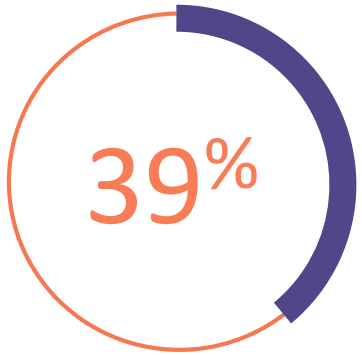
Percent of those very confident about what the company has in place to comply with GDPR requirements



Technologies



Processes

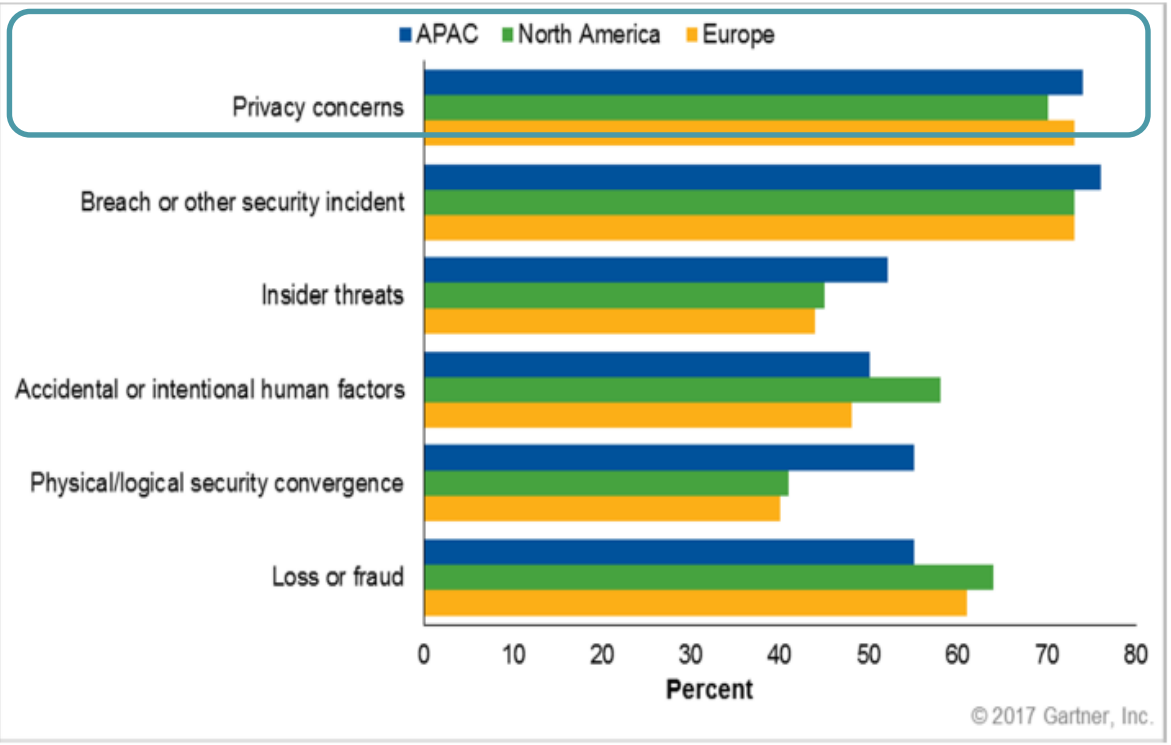


Policies

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA, October 2017

It’s not just an EU Issue…

Figure 1. Risks Influencing Security Spending by Region



Source: Gartner (March 2017)

A recent **PwC pulse survey** asked C-suite executives from large American multinationals about the state of their plans for GDPR. The “pulse” revealed:

- Over half of US multinationals say GDPR is their top data-protection priority
- Information security enhancement is a top GDPR initiative
- 77% of survey respondents plan to spend $1M or more on GDPR

Source: “GDPR Prepardness Pulse Survey” published by PwC – January 2017

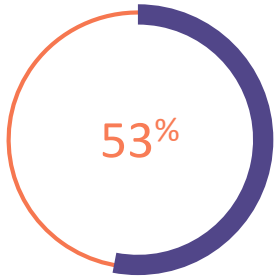
40% of organizations will be in violation of the GDPR by 2020; this is expected to be near zero by 2023.

Gartner

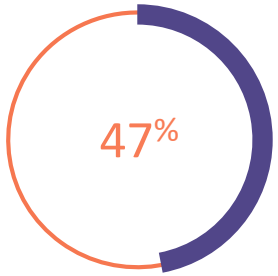
GDPR is an Opportunity

- Drive real value from your data
- Come to grips with Consent!
- Create new Governance Models
  - Data Management Policies
  - Data processes
- Build trust with customers/consumers
- Revisit security
- Employee skills, access management

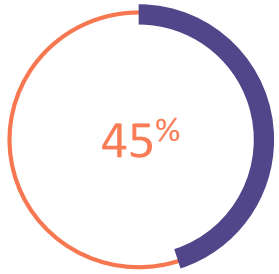
Beyond compliance benefits, what do you see as the business advantages of becoming GDPR-compliant?



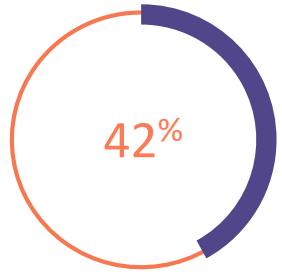
Improved customer experience



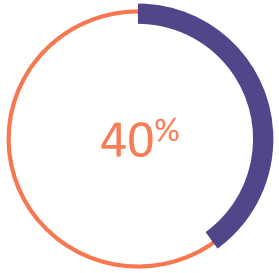
Improved data strategies



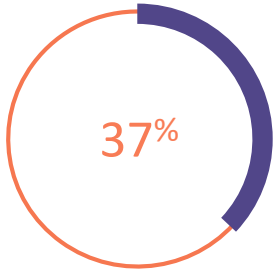
Better privacy policy management



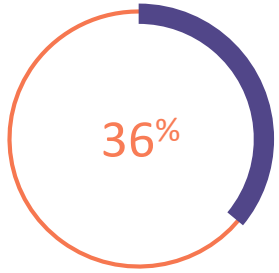
Efficient practices for data governance and privacy



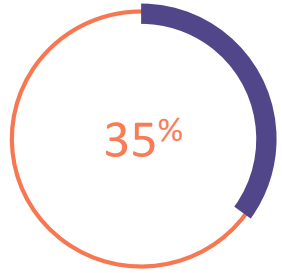
Greater operational efficiency



Better KPIs and metrics for data security and privacy



Enhanced design of analytics projects



Address growing customer expectations for privacy

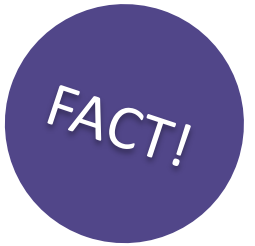
Biggest Concerns in Achieving Compliance

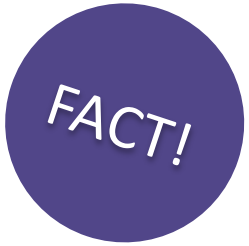
- Business Process Change
- Detecting, protecting and responding to….
- Implementation costs
- Infrastructure change
- Loss of customer confidence/productivity
- Policy Complexity
- Revealing sensitive data/protecting data
- Possible fines...

GDPR: Fact or Fiction ?

RSA

Record Keeping & Demonstrating GDPR Compliance – Who cares





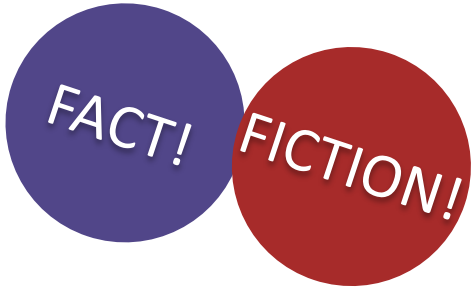
Rights of the Data Subject – Does this matter?

To comply with GDPR we should encrypt everything…

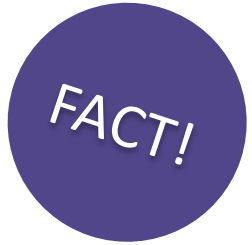
GDPR Compliance – Is this optional?

Data Location is irrelevant

A DPIA must always be conducted…



All Personal Data Breaches Results in a Fine



You Must Notify the Supervisory Authority of a Personal Data Breach Within 72 Hours

Four Key Areas to get Started

RSA

Four Steps to GDPR Planning

Primary objective:
Detect and respond to the threat *before* a breach occurs but if a breach *does* occur, you need to know the details and exact impact.

Primary objective:
Establish a risk assessment process to ensure controls are appropriately designed and implemented.

Primary objective:
Know where data is in the enterprise and who has access and implement controls in data processing activities.

Primary objective:
Establish a compliance program to ensure controls are effective and operational.

Polling Question #2

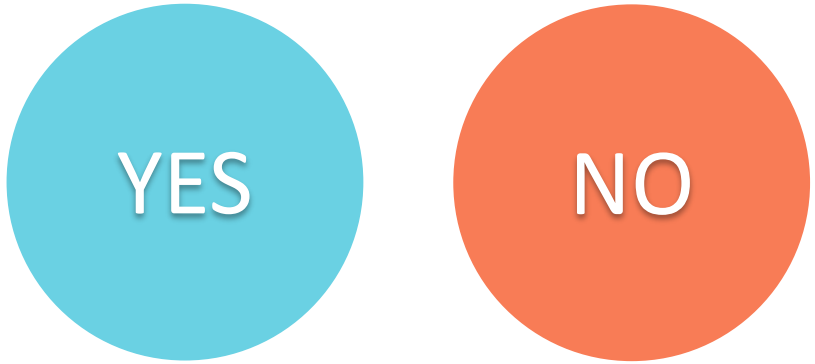
Considering these four requirements – How is your organization prioritizing each?

Working to a Plan

DON'T FORGET ABOUT THIRD PARTIES…

Polling Question #3

Do you use Third Parties to process or store EU resident data?

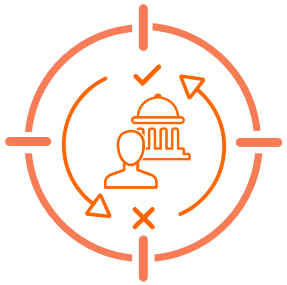


KEY INGREDIENTS

Breach Readiness

Risk Assessment

Data Governance

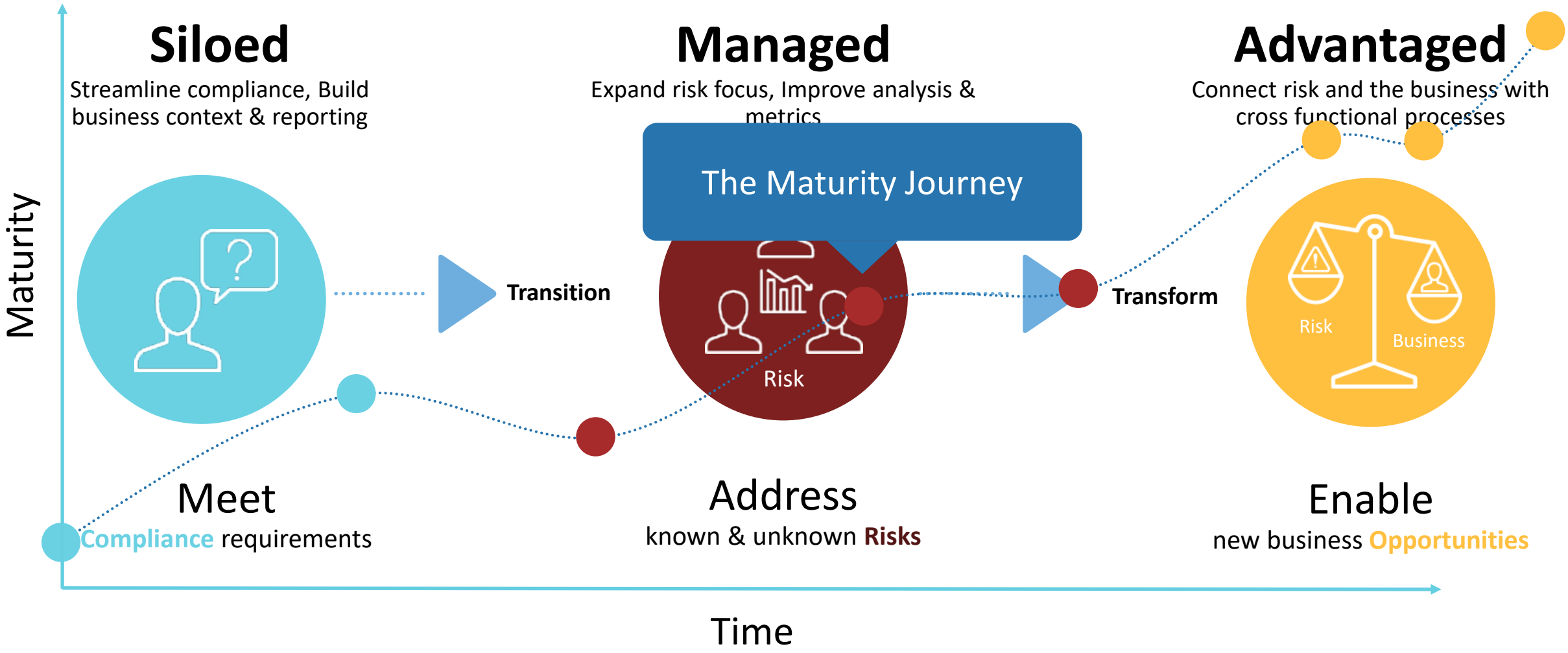


Compliance Management

The Journey Forward

RSA

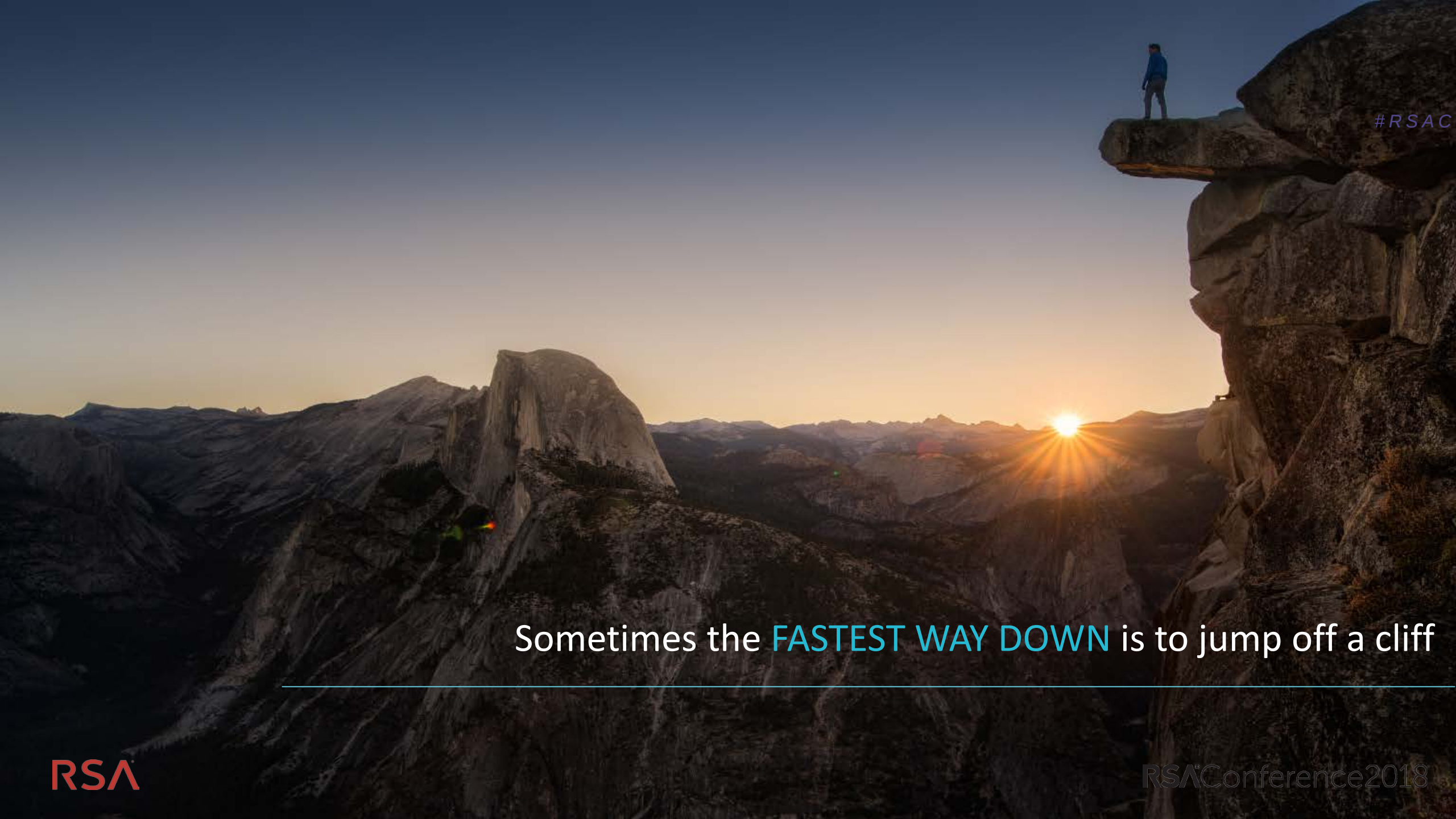
Take Command of your Journey



Steps to Take Now

1. RAISE AWARENESS
2. UNDERSTAND PERSONAL DATA
3. COMMUNICATING PRIVACY INFO
4. INDIVIDUAL'S RIGHTS
5. SUBJECT ACCESS REQUESTS
6. LEGAL BASIS FOR PROCESSING DATA

Steps to Take Now


#RSAC
Sometimes the FASTEST WAY DOWN is to jump off a cliff

THANK YOU