ISO 27001
A competitive Advantage

Sean Griffin, CTO
Who is Poppulo?

HQ in Cork
US Office - Boston
160+ employees
Growing by 40%
B2B
55% New Sales in US
38% New Sales in UK
SaaS Model
ISO 27001
A competitive Advantage

Data centers

EU: Cork (CIX)
EU: London
US: Boston
US: Chicago

Cloud Deployments in Progress
ISO 27001
A competitive Advantage

Manage IC communications

- Email
  Newsletters & Flyers

- Events

- Employee Data
  PII Data

- Pulse Surveys

- Cross Channel Analytics

- Data Processor
ISO 27001 at Poppulo

Started implementing ISO 27001 over 6 Years ago
Company size ~40 people
Identified a rise in security audits
Slowing the sales process

Certified for over 5 years
Scope of ISMS is all operations worldwide
It does not eliminate security audits

2017 ISMS Phase 2
Incorporating GDPR compliance

2 Years ago went to ISO 27001:2013
ISO 27001
A competitive Advantage

Implementing ISO 27001 at Poppulo

Hired Brian Honan as Consultant
“Ok at security but useless at documentation”

Based on existing work practises
Document what you do; Implement changes for identify gaps;
It’s daunting but not hard

9 months to first audit
Implementation team had day jobs
ISO 27001
A competitive Advantage

Importance of ISO 27001 to Poppulo

95% of new customers perform a security audit as part of onboarding. We have never failed a security audit.

GDPR is mentioned once a day in sales calls, customers assume that we as compliant as a result of ISO 27001.
ISO 27001
A competitive Advantage

Poppulo’s initial misconceptions

What ISO 27001 covers?

Anything that can damage the company:
Company Brand, Hurricanes

- Surely we can copy an ISO 27001 implementation
  - Unique for each company
- Everything needs to be perfect
- Auditor is out to get you!
ISO 27001
A competitive Advantage

ISO 27001/GDPR in US

**ISO 27001**
Not as widely implemented in US.

SSAE 16/18, common in US.

ISO 27001 is accepted by US customers as better.

Globally recognised

**PII/GDPR Laws**
Data Privacy Laws in Various States

Most large companies hold data on EU citizens

**Large US companies**
Will look for Cyber Insurance

Some will decide to store their data in the EU
ISO 27001: Continuous Improvement

- Company has grown in 6 years
- Now implementing: ISMS Phase 2
- Distribute security around the organisation
- Assets, risks and controls
- Influenced by GDPR and PII laws
  - Privacy by design
- Security by design
Org Structure of ISMS Phase 2

Auditors
Alice
Emma
Tony
Julian
Ryan
Beatrice
Carl
David L

Senior MGT Team
CEO
CFO
CTO
DPO

ISMS Manager

ISMS Operations Team
Marketing
Danielle G
IT
Tom
Sales
Dan
Cust Ops
Ruth
Engineering
Daryl
People OPS
Danielle H
Finance
Robin
US Office
Melinda
Product Mgt
Petra
## Assets, risks and controls

### Assets
- What is the Asset?
- Has it Material Value
  - Pens
  - Laptops
- PII data
- Who Owns Asset?
- Identify Risks

### Risks
- Basic Types
  - Loss
  - Unauthorised Use
  - Unauthorised Access
- Impact
- Probability
- Risk Acceptance
- Identify the Controls

### Controls
- Mitigate Risks
- Simple as possible
  - Paper disposal
- Too many controls
- Automate
- Owner
- Executor
ISO 27001
A competitive Advantage

ISMS - Software

Speadsheets

Atlassian
Jira & Confluence

Internal
PAsset
ISO 27001
A competitive Advantage

Jira - Evidence of compliance
ISO 27001
A competitive Advantage

Confluence - Documentation of ISMS
ISO 27001
A competitive Advantage

PAsset - Assets, Risks and Controls
Thank you!

Sean Griffin, CTO