UBS

Public

The CEO gets it.
Now you have to deliver!

Defining, Implementing and Executing a Contemporary Information Security Strategy

Stephan Pfirter
Information Security Officer of UBS Group IT

23 June, 2015

SIGS Technology Summit
Security Interest Group Switzerland

ISF Information Security Forum

One fine day…

"Are we ready to face the challenges of Cyber Security?"

Executive board

"Are we secure?"

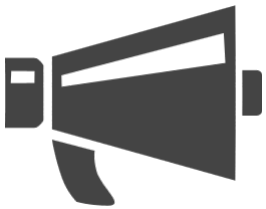
CEO

LogJam

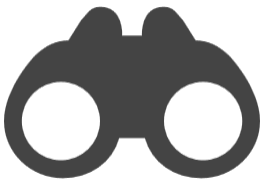
"The CEO gets it. Now you have to deliver!"

ISF Threat Horizon 2016

On the board's radar

New target audience 

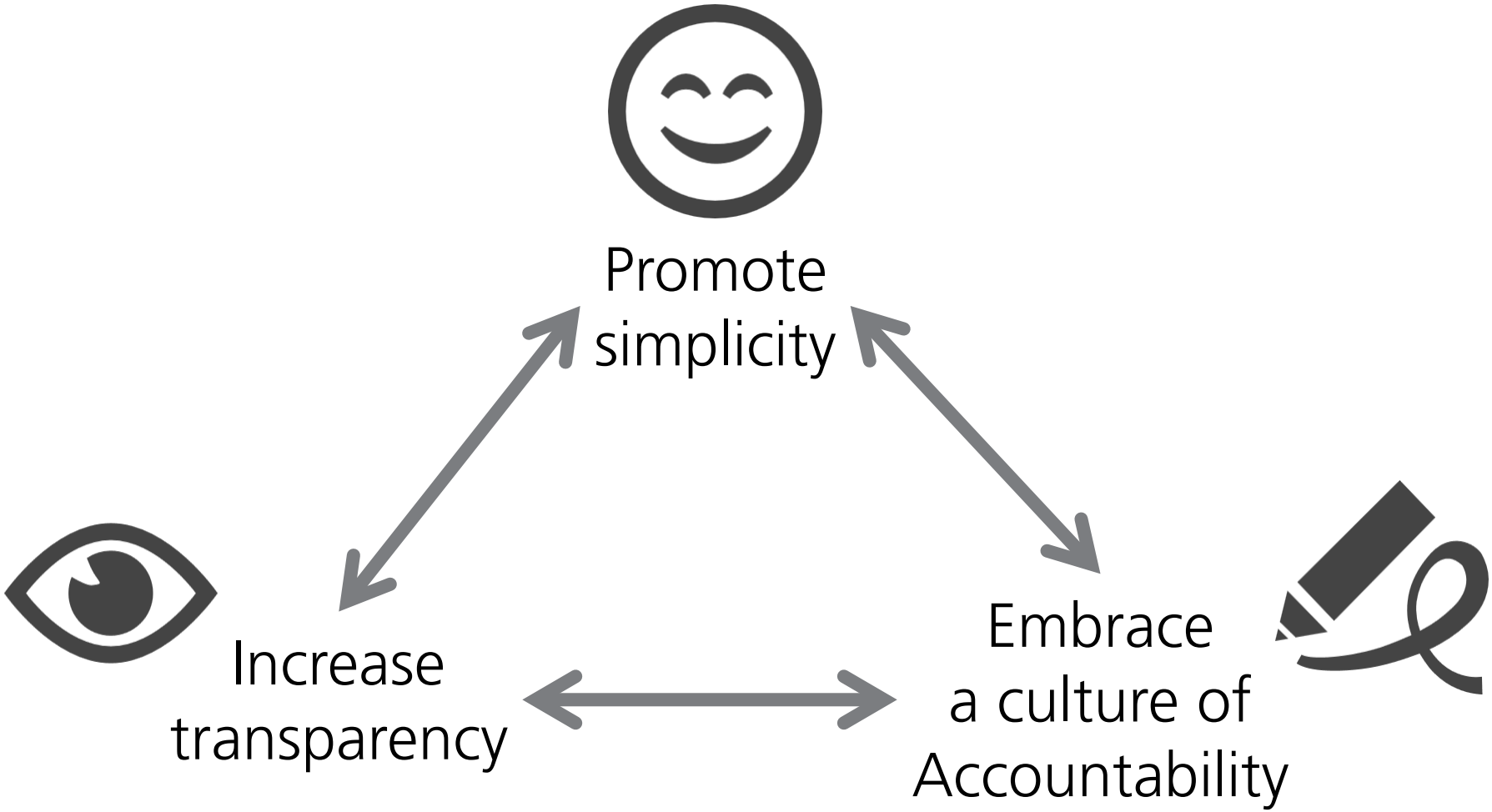
Increased visibility … and exposure!



Answers instead of questions –
Solutions instead of problems

Where to start?

A set of guiding principles – to life, the universe and everything

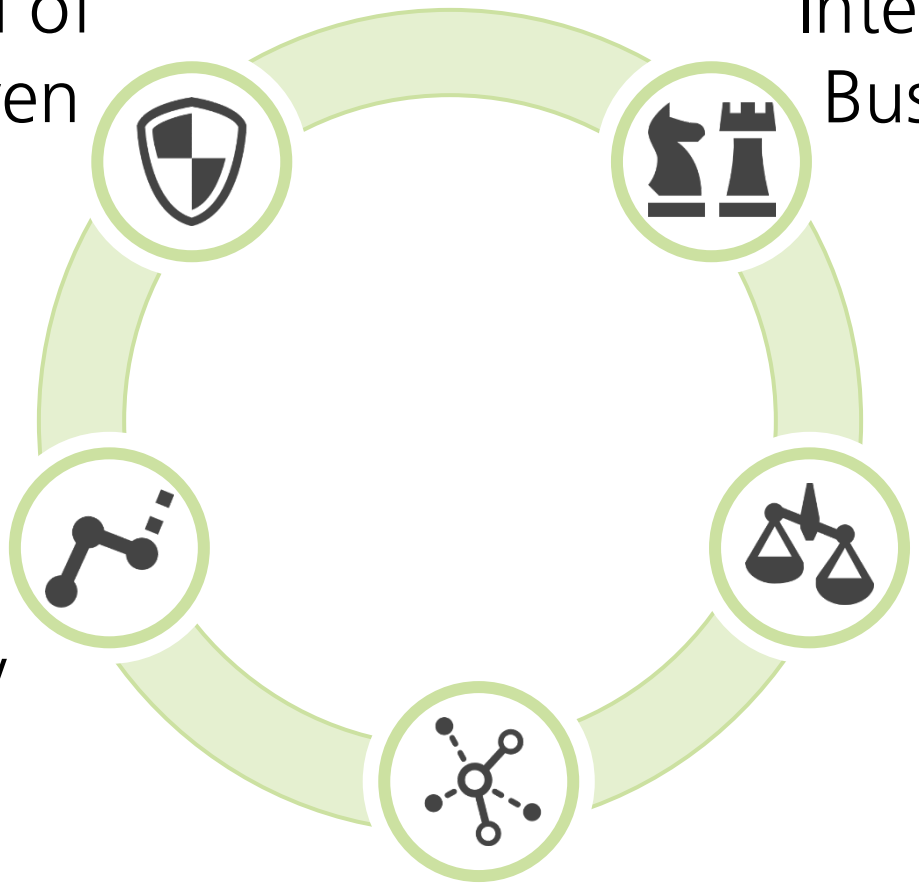


A Contemporary Information Security Strategy

Characteristics

Security- instead of compliance-driven

Integrated into the Business Strategy



Active and anticipatory

Risk-based

Pragmatic

A Contemporary Information Security Strategy

Integrated into the Business Strategy

- Digitalisation: Business Products/Services become S.M.A.R.T.
  - Dependency on Information Security increases
- Sound understanding of firm's business, and context it is operating in (P.E.S.T.L.E)
- Derive:
  - Key valuable information assets
  - Business services/products depending on these

A Contemporary Information Security Strategy

Risk-based

- Information security incident: Not "if" but "when"
- You cannot afford 100 % security
- Residual risk = risk appetite?
  - Adjust risk response
  - Adjust business product/service
  - Adjust risk appetite
- Residual Risk Response: R^3 – Repellence, Resilience, Recovery!
- Information security risk = simply another type of risk

A Contemporary Information Security Strategy

Pragmatic

- World is inherently complex
- Perfect = "good enough"
- Focus on standard cases
- Robust and resilient exception management

A Contemporary Information Security Strategy

Active and anticipatory

- "Everything changes, nothing stands still" Heraclitus, Greek Philosopher, 535 – 475 BC
  - Business environment
  - Threat landscape
- Collect, Relate, Create, Disseminate

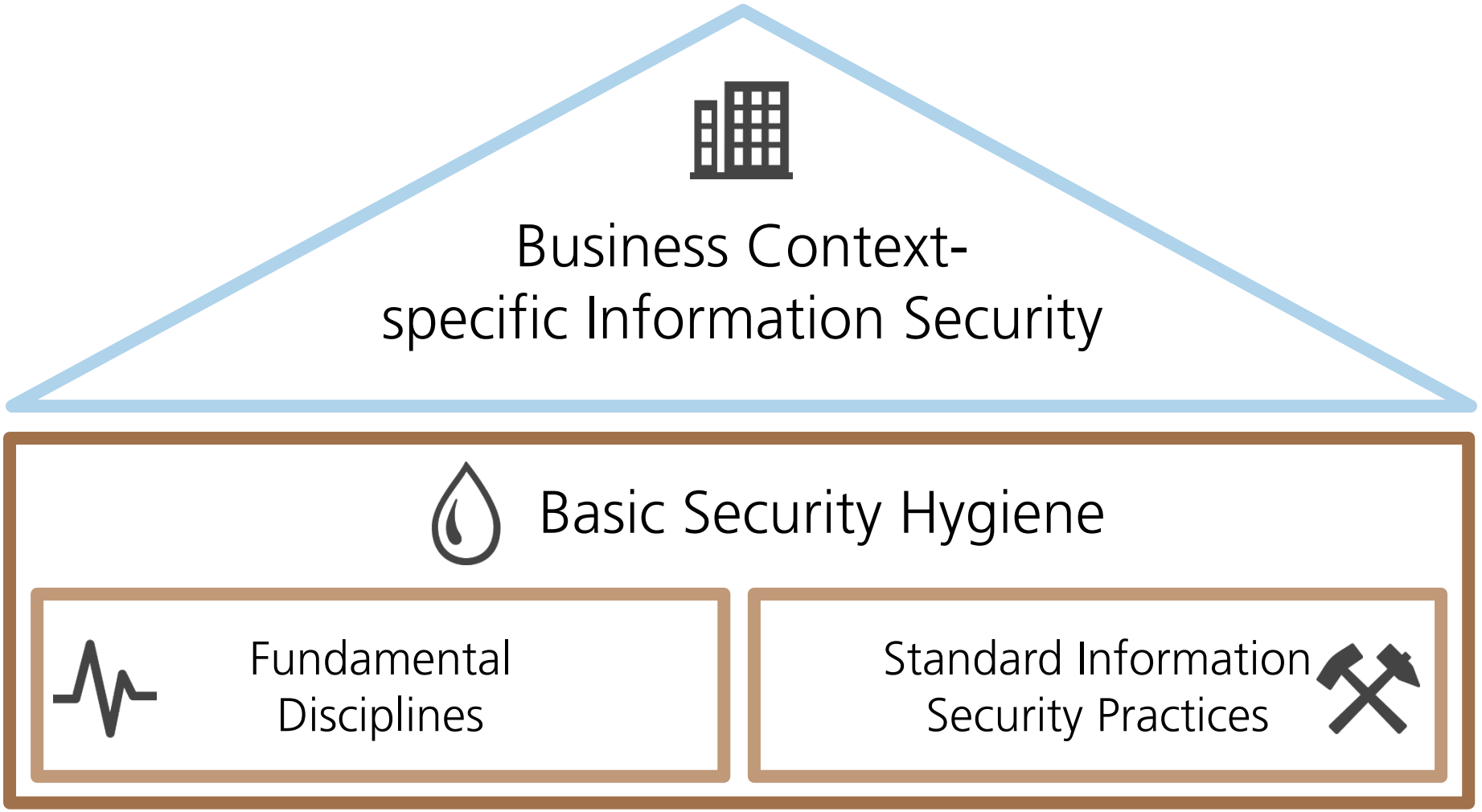
A Contemporary Information Security Strategy

Security- instead of compliance-driven

- It is called Information Security (not Compliance) Strategy
- Relationship: "Security" and "Compliance" ≠ causal!

A Contemporary Information Security Strategy

Two-pronged approach



A Contemporary Information Security Strategy

Basic Security Hygiene

Fundamental Disciplines

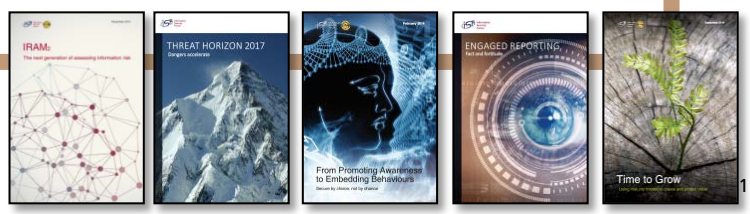
Organisation & Governance
Set-up, Operating Model, Policies, Roles, RACI, etc.

Risk Management
Enable a sensible risk dialogue

Information Security Intelligence
Collect, relate, create, disseminate

Information Security Awareness
From promoting awareness to changing behaviours

Quality & Performance Management
Efficiency, effectiveness, maturity, benchmarking



UBS SIGS Technology Summit Security Interest Group Switzerland ISF Information Security Forum

A Contemporary Information Security Strategy

Basic Security Hygiene

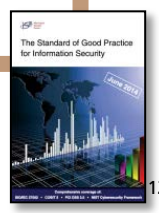
Standard Information Security Practices

Secure Operations
Recommended priority 1 topics

- Incident management
- Vulnerability & Patch Management
- Configuration management
- Privileged access management

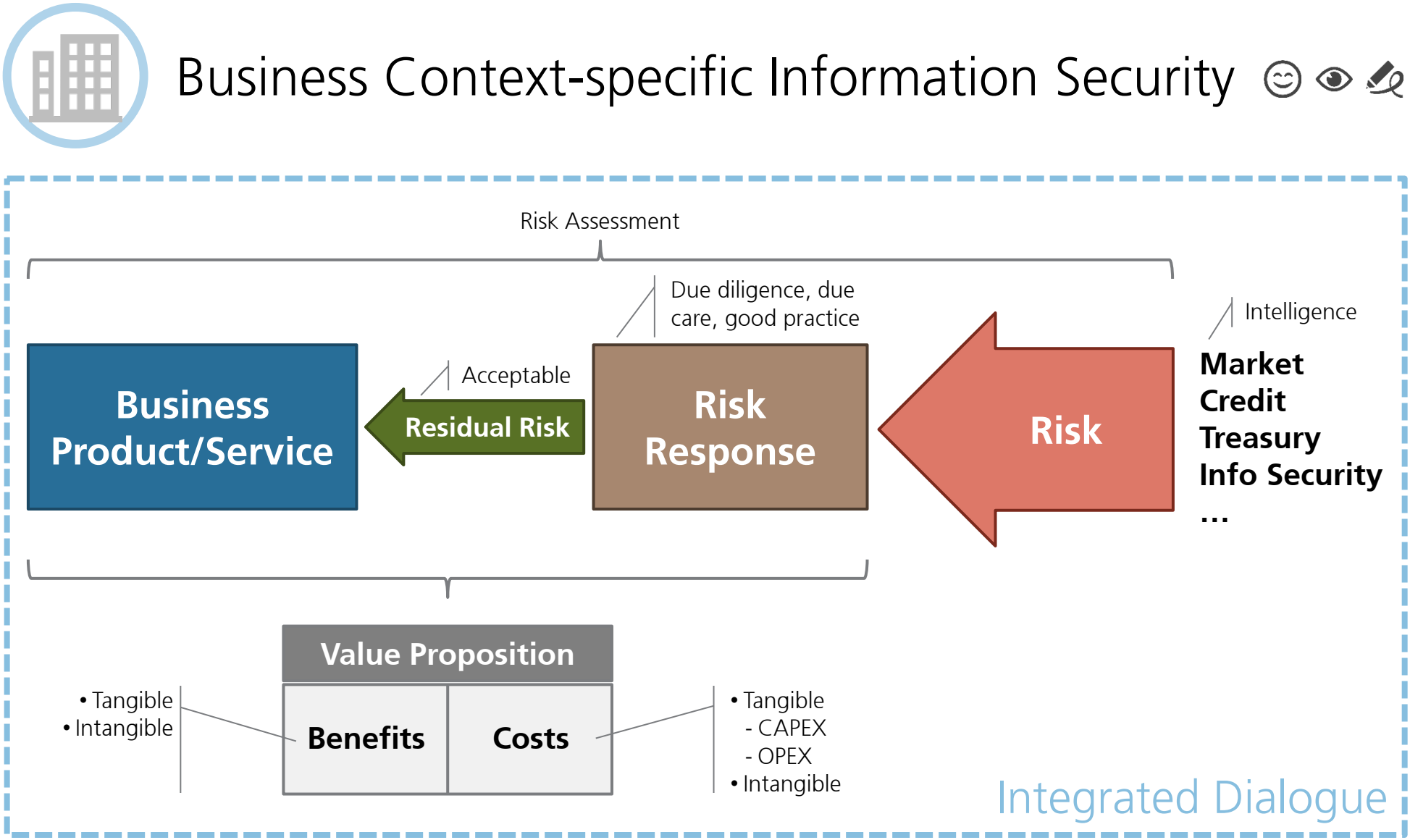
Secure Development
Recommended priority 1 topics

- Security requirements management
- Vulnerability Scanning
- Penetration testing



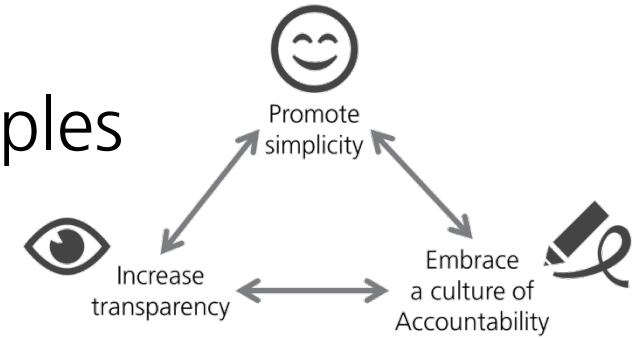
A Contemporary Information Security Strategy

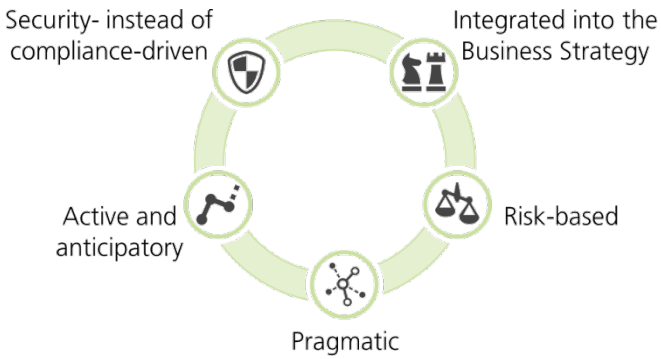
Business Context-specific Information Security



[TL;DR]

Define your guiding principles and stick to them!





Ensure your Information Security Strategy addresses the important characteristics!

Follow a two-pronged Approach – start lean and grow!