

Practical Risk Management in a Complex Supply Chain

Alison Tetley

Business Assurance Manager - Xerox Global Services

Institute of Risk Management North West with ALARM
2009

28 October

Introduction



- < Business Assurance Manager – Xerox Global Services
- < iON senior management team
- < Main focus – iON, an association of companies providing services to a major government department; this contract is seen as a partnership between iON and the department concerned
- < My role is about managing risk – governance, internal controls (SOX), information security, business continuity
- < Outward facing role – to the client, partners, the extended supply chain, wider Xerox (UK, Europe, worldwide)

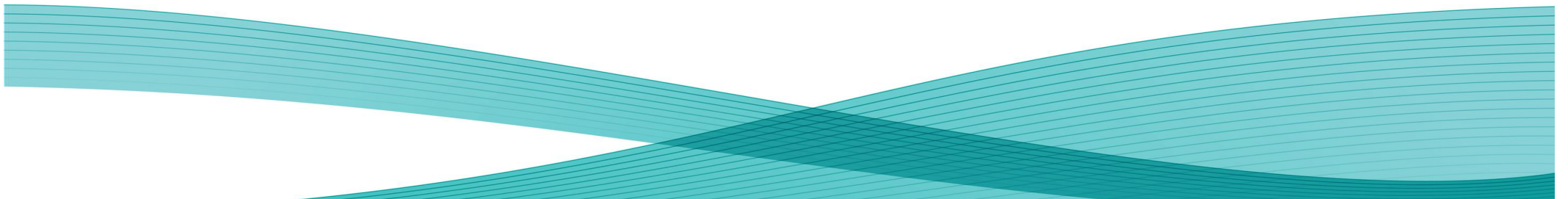
My main challenge:

Service Delivery team – fixes problems when they arise

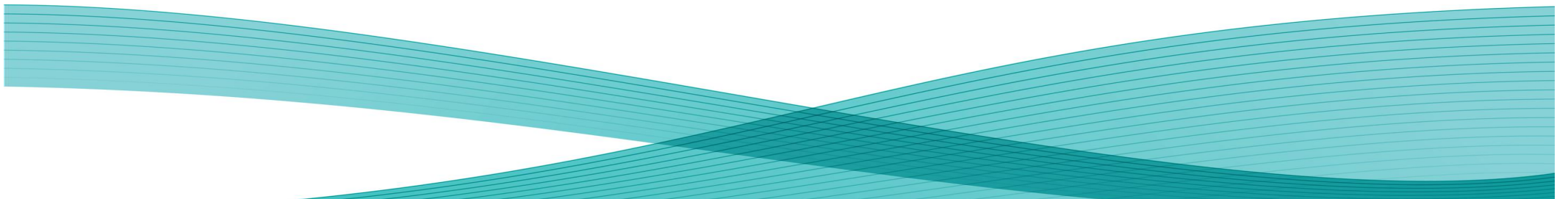
Business Assurance – my objective is to STOP THOSE PROBLEMS OCCURRING in the first place or minimise the impact if they do occur!

Overview

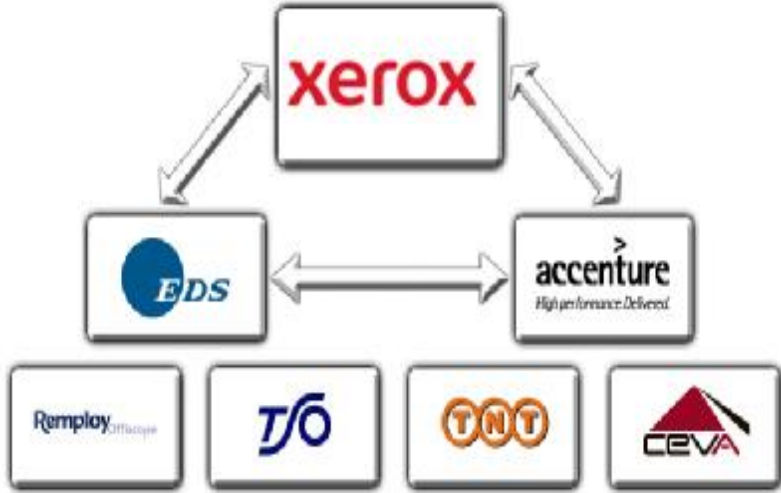
- The iON Association
- The services we provide
- How we manage risk
- Some practical examples
- Conclusions



The iON Association

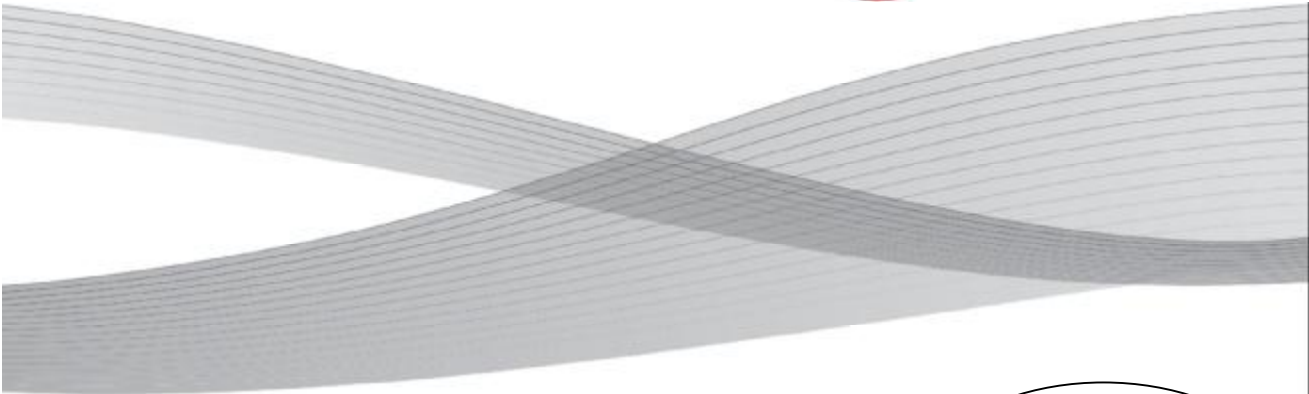


iON Association – what is it? Why do it?

Partner & Workshare	Why Partner
<p>XEROX</p> <ul style="list-style-type: none"> < Prime Contractor <p>EDS (also a customer of the service)</p> <ul style="list-style-type: none"> < Provision of Secure Print/ Office desktop print & transactional print, & IT systems <p>CEVA</p> <ul style="list-style-type: none"> < Warehousing <p>Accenture</p> <ul style="list-style-type: none"> < Change Management / transformation <p>The Stationery Office</p> <ul style="list-style-type: none"> < Digital Asset Management <p>Remploy</p> <ul style="list-style-type: none"> < Employment diversity < Provision of some Direct Mail services <p>TNT (outside Association)</p> <ul style="list-style-type: none"> < Distribution <p>Oracle on Demand</p> <ul style="list-style-type: none"> < IT systems 	<ul style="list-style-type: none"> < Presence in the sector, established incumbents < Expertise in niche areas < Risk Sharing < Portfolio alignment gaps, needed an Enterprise view < Bench strength, resources, expertise, process & methods <div data-bbox="1249 774 2027 1268" data-label="Diagram">  <pre> graph TD Xerox[Xerox] <--> EDS[EDS] Xerox <--> Accenture[Accenture] EDS <--> Accenture Remploy[Remploy] TSO[TSO] TNT[TNT] CEVA[CEVA] </pre> </div>



Position in the Xerox Corporation



- § Xerox is the prime contractor
- § “Partners” are in reality sub-contractors – iON is not a legal entity in its own right
- § Capable of leveraging infrastructure to support cross government shared service model
- § Leverages other Xerox offerings – XGS / XOS – and complex supply chain

Production

Specialist equipment for production customers

Office (XOS)

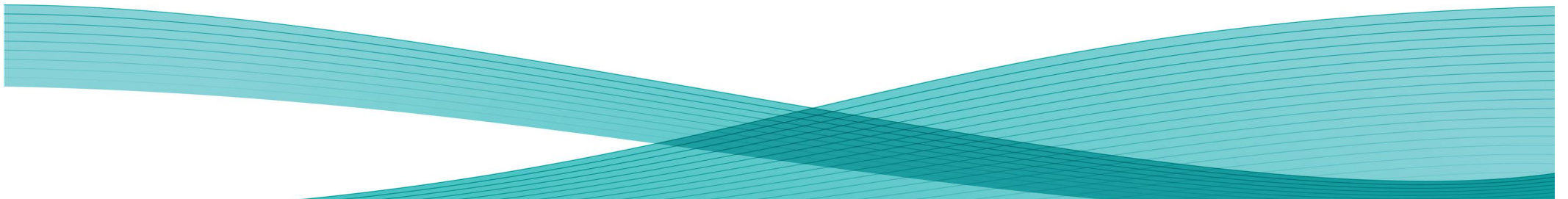
Multi-function devices (MFDs) for offices

Services (XGS)

Outsourced services for businesses



The services we provide



Service Delivery Model



Transformation

Core Business Print
Marketing & Publicity
Direct Mail
Secure Print
Configurable Print
Ordering
Reprographics
Stationery Products
Scanning

Warehouse
Catalogue Cleanse
Catalogue Realms
Product Rationalisation
Product Sourcing
Digital Asset Management
Product Sponsor Relations
Internal Mailings
Service Launch

**Future: ECM, XOS,
Paper reduction, Creative**

**Product Rationalisation &
Consolidation**
Local Stores
Reprographics Transformation
Ordering Transformation
Demand Management
Publicity Register
Citizen Ordering

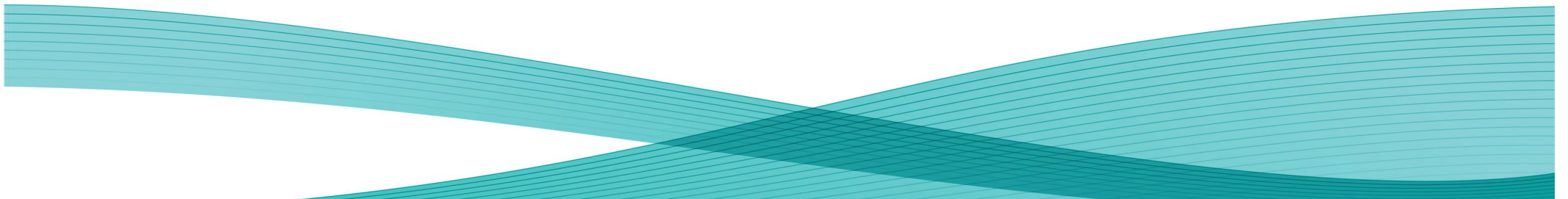
Take On

Consolidate

Transform

Governance, Business Continuity, Risk Management
Communications, feedback & learning

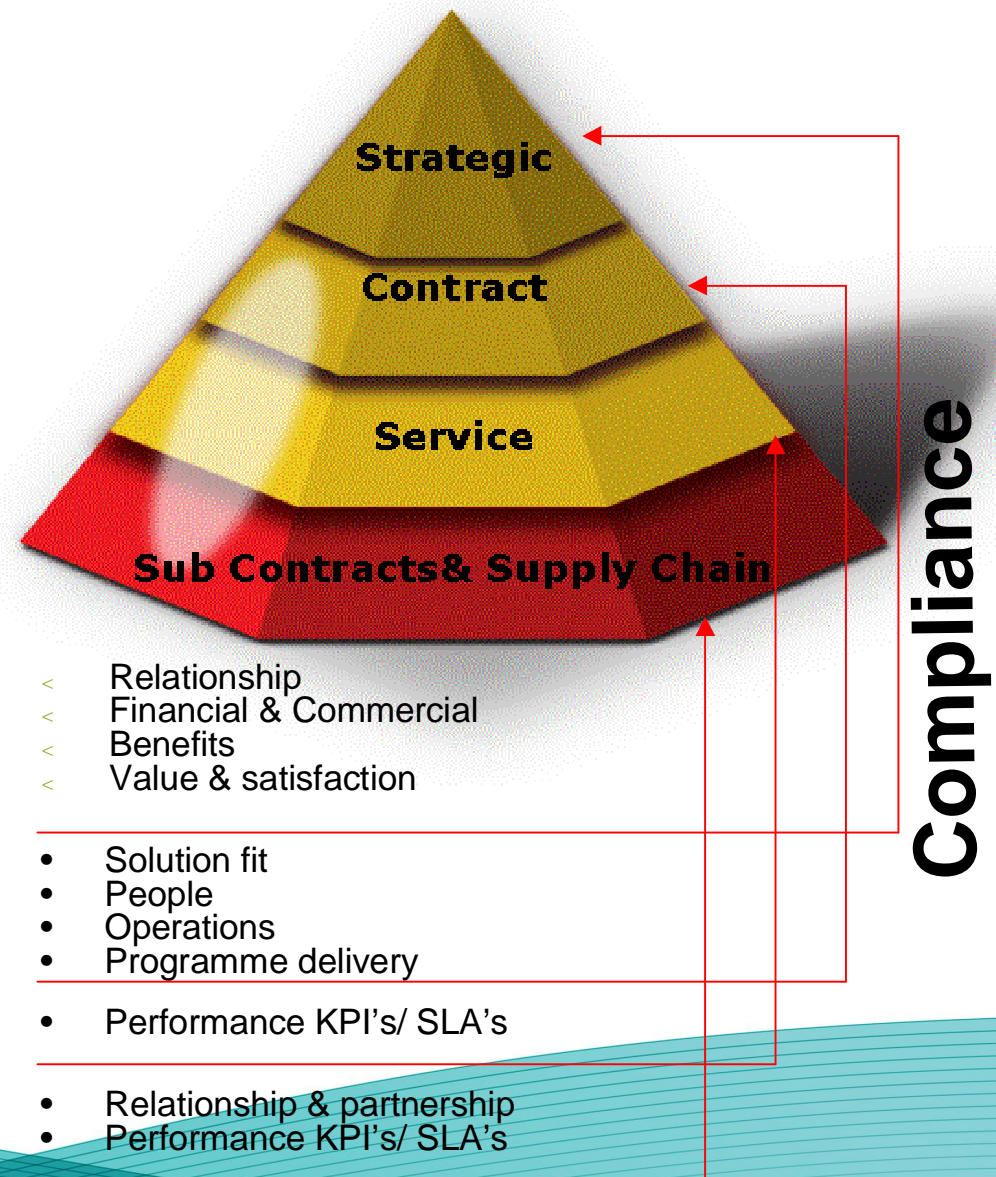
How we manage risk



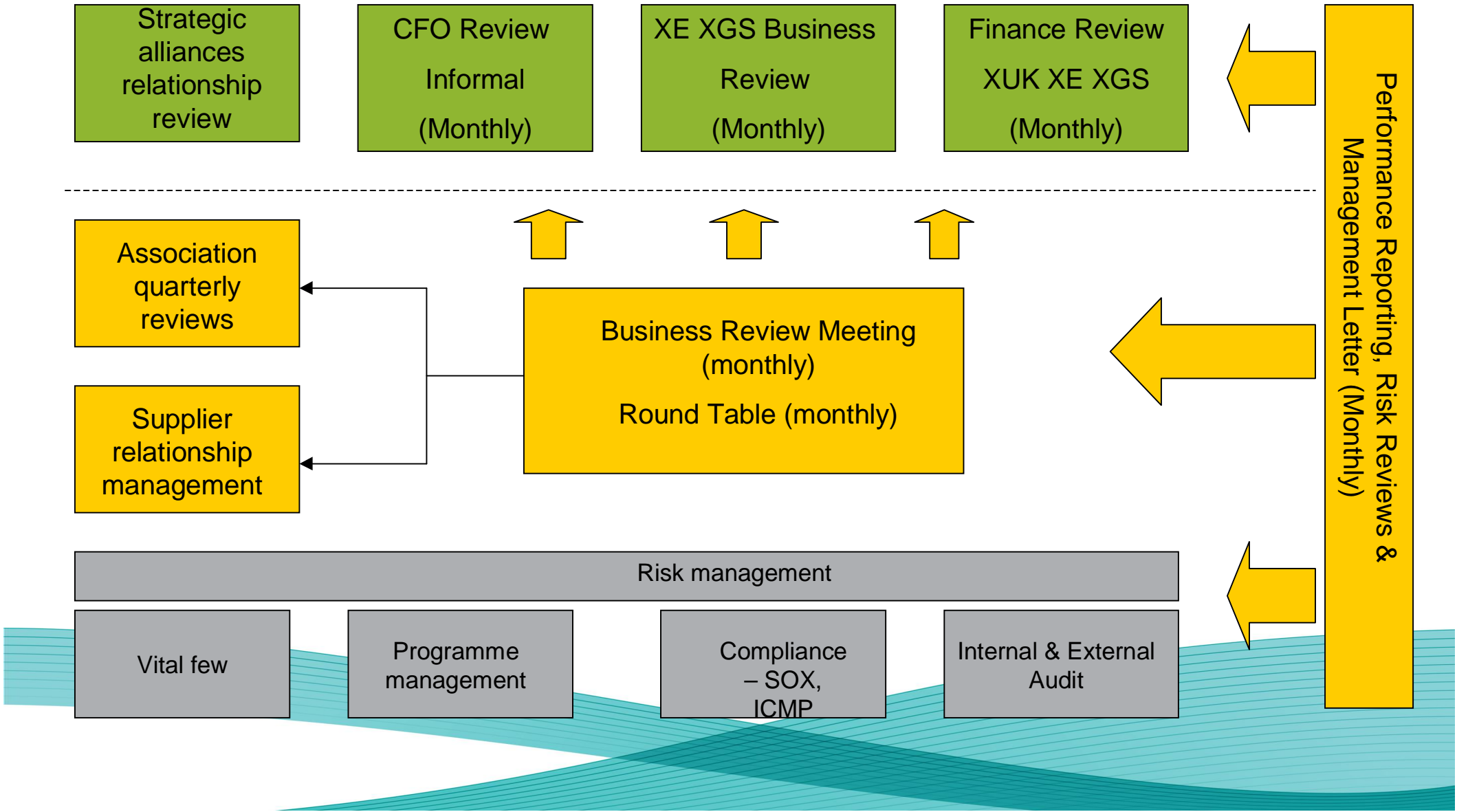
Drivers for sound risk management



- Contractual requirement to manage risk jointly using client methodology
- Need to manage both internal risk and risk shared with client – 2 separate registers
- Governance arrangements – Xerox and client facing
- Partners and suppliers – strategic relationships and extended supply chain
- Performance management
- Transformational change agenda
- Data handling and transfer – Government data
- Sarbanes Oxley, internal and external audit requirements



Internal Governance



Risk Management Methodology



Joint (Client) Risk

- Contractual commitment to jointly manage shared risk
- All risks have owner and action manager from client and from iON
- Measure inherent and residual risk – impact x likelihood (3 x 4)
- No financial values attributed

Internal (Xerox) Risk

- Requirement to report to XGS Europe in accordance with XGS approach
- $\text{Impact} \times \text{Probability} = \text{Inherent risk} \times \text{Controls effectiveness (\%)} = \text{Residual risk}$
- $\text{Gross financial impact (\$)} \times \text{controls effectiveness \%} = \text{net financial exposure}$
- Higher degree of granularity - scoring out of 9 x 9 (or 10 if risk crystallises)
- Measuring financial exposure v cost of implementing controls

Underpinned by active risk review on weekly basis by risk owners and action managers.

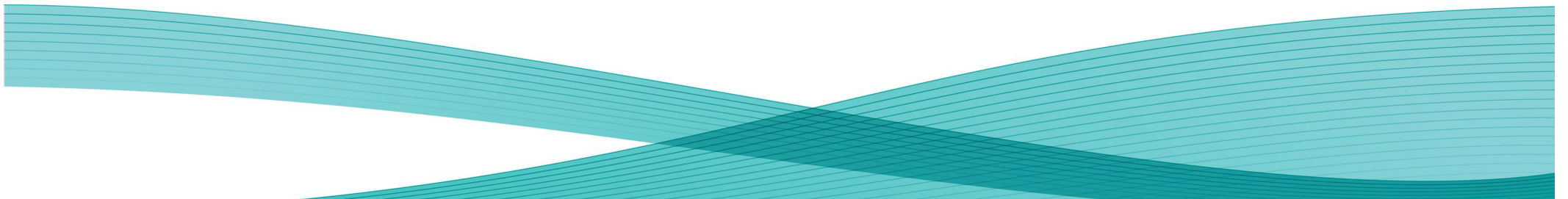
Joint red risks reported weekly in client facing portfolio update.

Monthly review and challenge by Business Assurance Manager (internal) and risk review board (joint)

Quarterly internal risk review board by iON senior management team.

A decorative graphic at the bottom of the slide consisting of several overlapping, wavy, teal-colored bands that create a sense of movement and depth.

Risk management in practice – examples and lessons learned

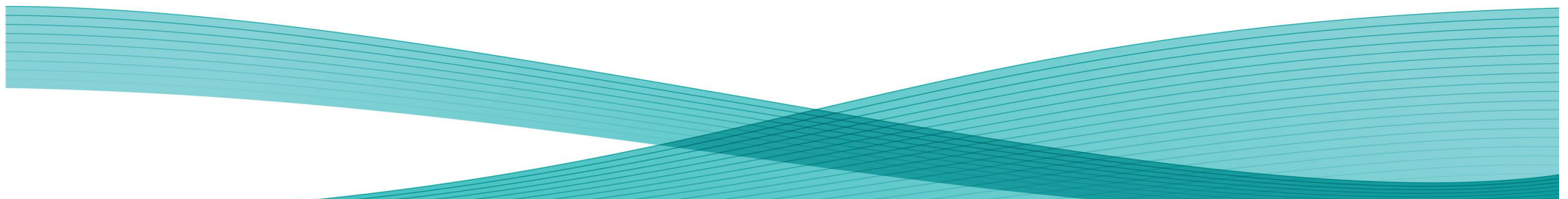


Example 1 – loss of intellectual property

Contract Ts & Cs placed requirement on client to provide digital assets for production of print products to iON.

- At commencement of contract client was unable to supply artwork and specifications for @6500 core business print products
- Cause – loss of ownership of asset to incumbent supply chain (not an uncommon problem!)
- Consequence – unable to replenish stock at cutover into the iON warehouse. Potential loss of supply of business critical product and adverse impact on front line services

The client believed that it had transferred the risk around version control and accuracy to iON as supplier



Example 1 – loss of intellectual property

Management actions

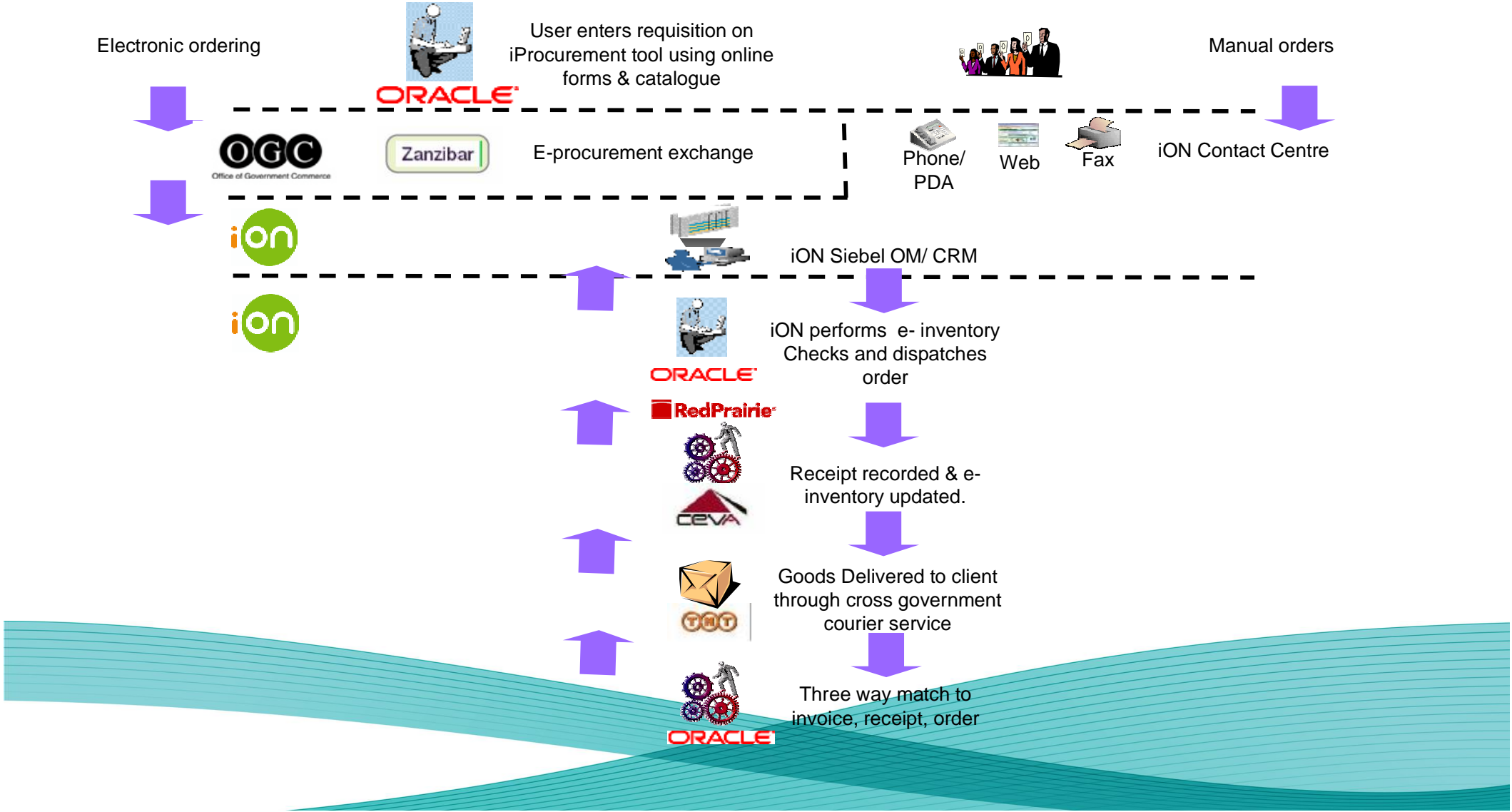
- < Continuous escalation of risk to client as business continuity risk to aid understanding of impact – did not understand whose risk this really was!
- < Establish “Tiger Team” – LSS Black Belt in lead
- < Daily meeting / call each morning to review progress and identify next actions and process improvement
- < Full use of relationships with suppliers to obtain by back door
- < Full log of all actions and outcomes
- < Daily dashboard to track
- < Provide as much transparency of position at any time as possible – complete openness
- < Continuous communications – internally and with client

Outcomes

- Closed gap to @2500 missing items
- But o/s gap included critical product
- Obtained client resource to assist – too late to avoid stock outs and inability to supply; business seriously impacted
- Requested to supply unvalidated product – potential £m loss to client if wrong version supplied
- Daily reporting to client business units on status and gap.
- Alternative solutions provided – digital Print on Demand for low usage items
- 6 months intensive work to significantly resolve the issue - limited loss to @£60K

Example 2 - Order to Cash complexity in process

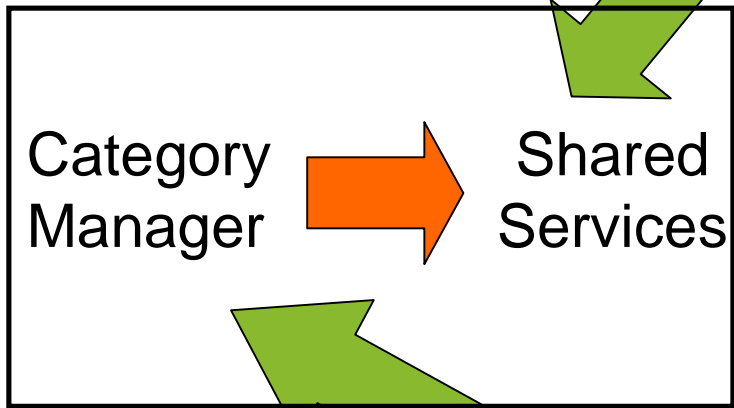
- *iON hosted e-Procurement tools linked to OGC Zanzibar & client's Oracle iProcurement to enable users to raise and track orders from electronic catalogue. Contact Centre for OGD's & non catalogue -*



Example 2 - Complexity in processes and relationships



Office of Government Commerce

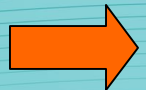
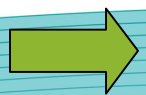


Key:

Contractual

Relationship / SLA

No formal relationship



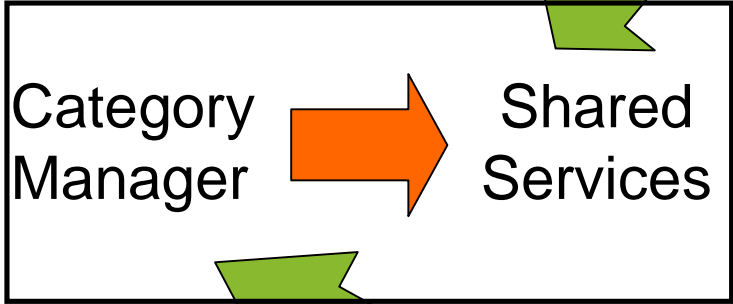
Example 2 - Complexity in processes and relationships



Office of Government Commerce

Agreement to provide service

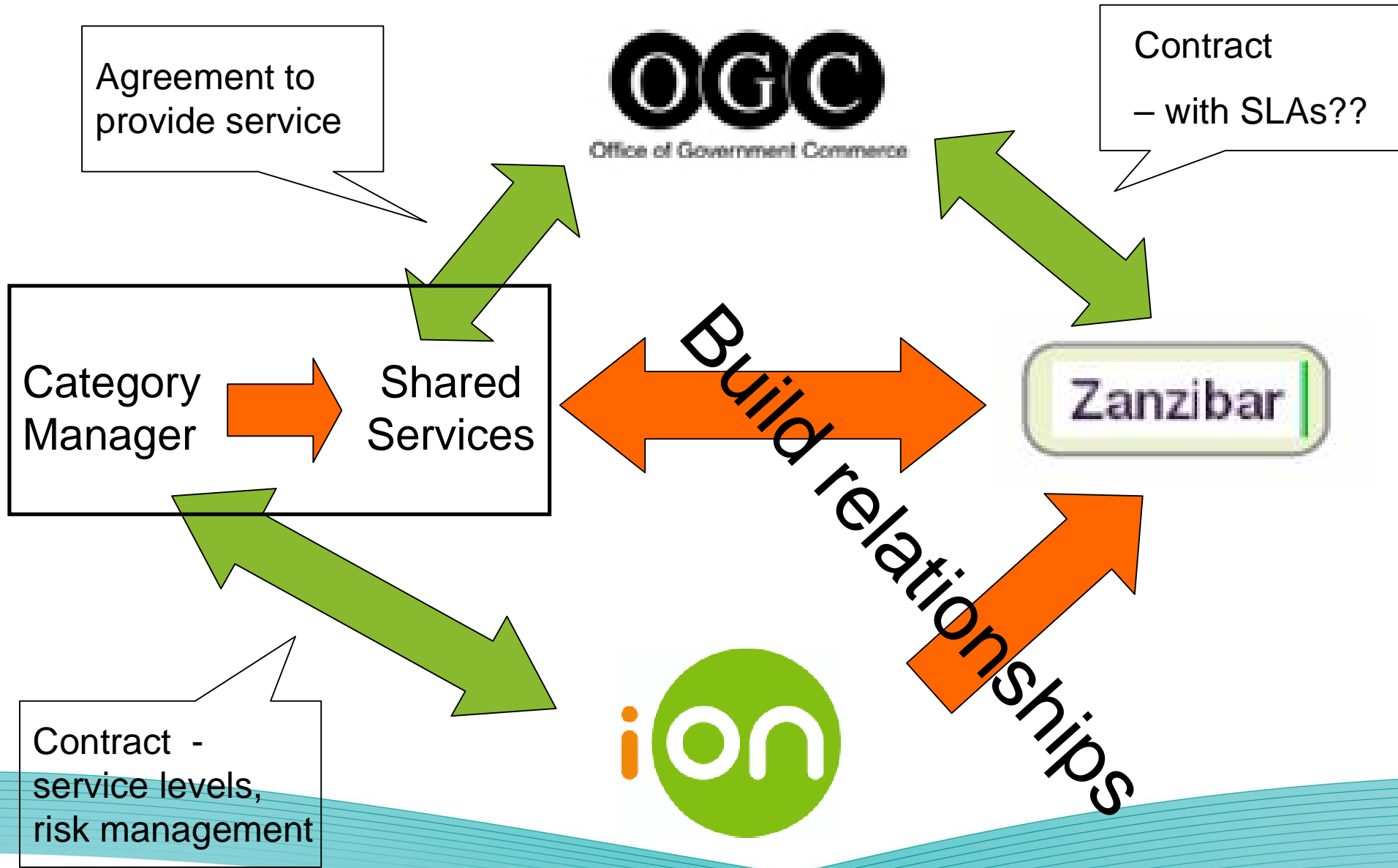
Contract
- with SLAs??



Contract - service levels, risk management



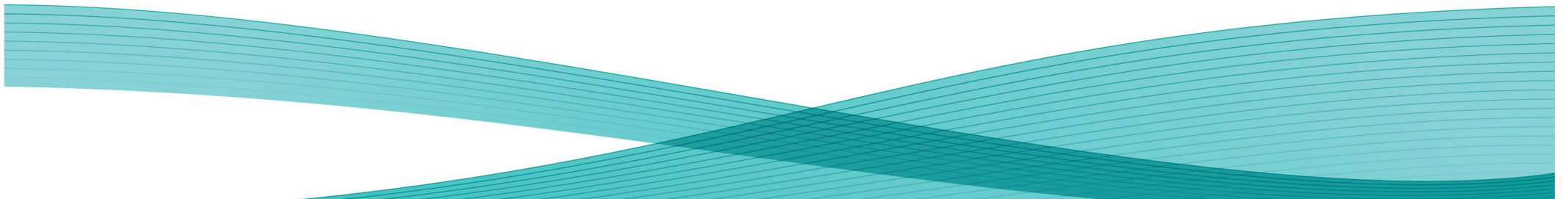
Example 2 - Complexity in processes and relationships



Example 2 - Complexity in processes and relationships; lessons learned



- < Risk managed through formal and informal arrangements – use every means available
- < Use contractual tools and SLAs where possible
- < Where no contract / SLA exists build and maintain relationships
- < Communicate - with all stakeholders at all times
- < Maintain robust change management
- < Test interfaces and infrastructure regularly (change and business continuity) – builds confidence where you can do this, causes concern if you can't!
- < Understand impacts - what they are, on whom do they fall and timing of them
- < RACI – clear accountabilities and responsibilities must be established and understood by all parties
- < Understand what risk is, and where it resides - has risk really been transferred?



Example 3 – risk management in silos

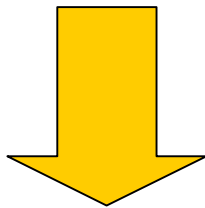


An information security risk assessment was undertaken on a small web-hosted IT solution to support security accreditation:

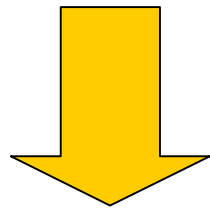
- u The solution is designed to bring control over a disparate set of digital assets.
- u These assets are in the public domain, and have no confidentiality issues.
- u The current manual process has a high risk of loss of the asset, and use of the incorrect (out of date) version.
- u The risk assessment focused solely on the IT security risks and not the existing business risk – even if there were no security features whatsoever risk would be reduced.
- u Data integrity is the key risk – can be mitigated whilst asset resides on the system but not once in the public domain (i.e. when it is printed!)
- u The system is prevented from going live because one security feature has not been tested to the satisfaction of the accreditor. The risk to which it relates exists in the current process and cannot be mitigated. It will remain exactly the same even after accreditation and go-live.

Example 3 – risk management in silos

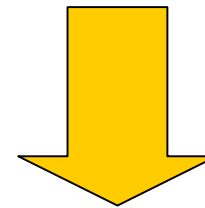
- < Risk assessment overstated – resulting in significantly greater cost to mitigate, cost that is disproportionate to the solution being offered
- < Risk assessment undertaken by wrong people – did not understand the business impact or risks the is solution designed to mitigate
- < Risk assessment did not take into account the actual business risk – only the risks around using an IT solution instead of a manual process



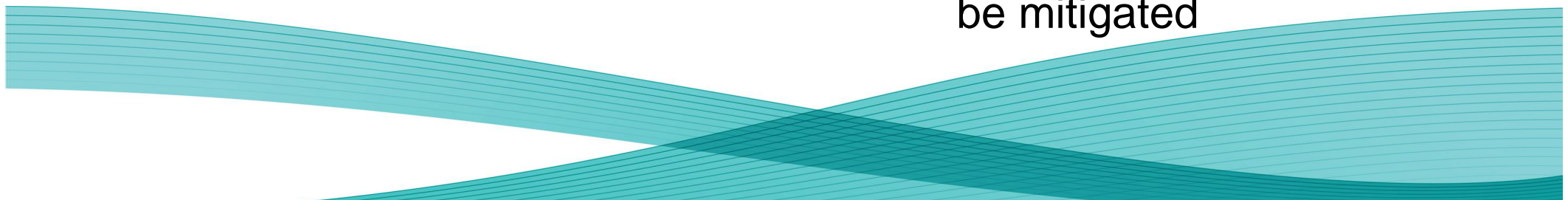
Increased cost



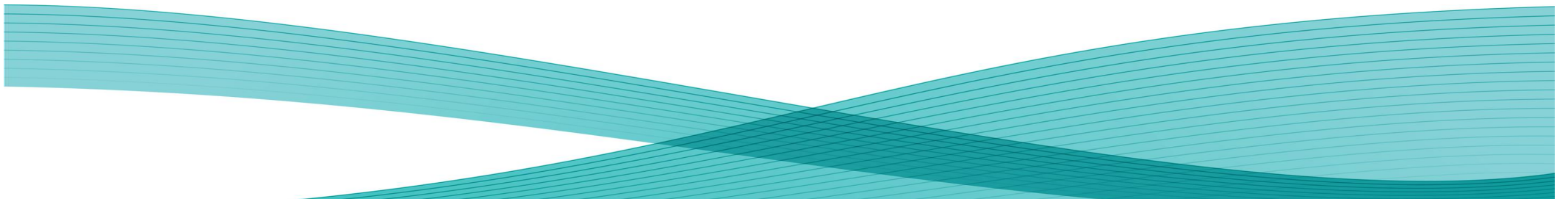
Delay



High risk profile
remains, cannot
be mitigated



Conclusions



Conclusions

- < Know your contracts and your responsibilities
- < Openness and transparency – at all times
- < Trust – good risk management is difficult without it in partnering arrangements
- < Relationships – build strong relationships, manage those relationships to death
- < Must not assess any specific risk in isolation from the wider business risk or those impacted – NO SILOS
- < Overstating impact of risk will result in disproportionate cost to mitigate
- < Risk transfer - understand whose risk it really is!
- < **Communicate, communicate, communicate**

