Digital Sovereignty

DANW Meeting
8 April 2025

Raymond Slot
Utrecht University of Applied Sciences
Strategy Alliance Consulting

Raymond Slot

- Lector Cybersecurity
- Partner Strategy Alliance

Opleidingen

- PhD, Business Waarde van Enterprise Architectuur, 2010
- Master of Business Administration, TSM Business School, 1995
- Elektrotechnisch Ingenieur, Universiteit Twente, 1984

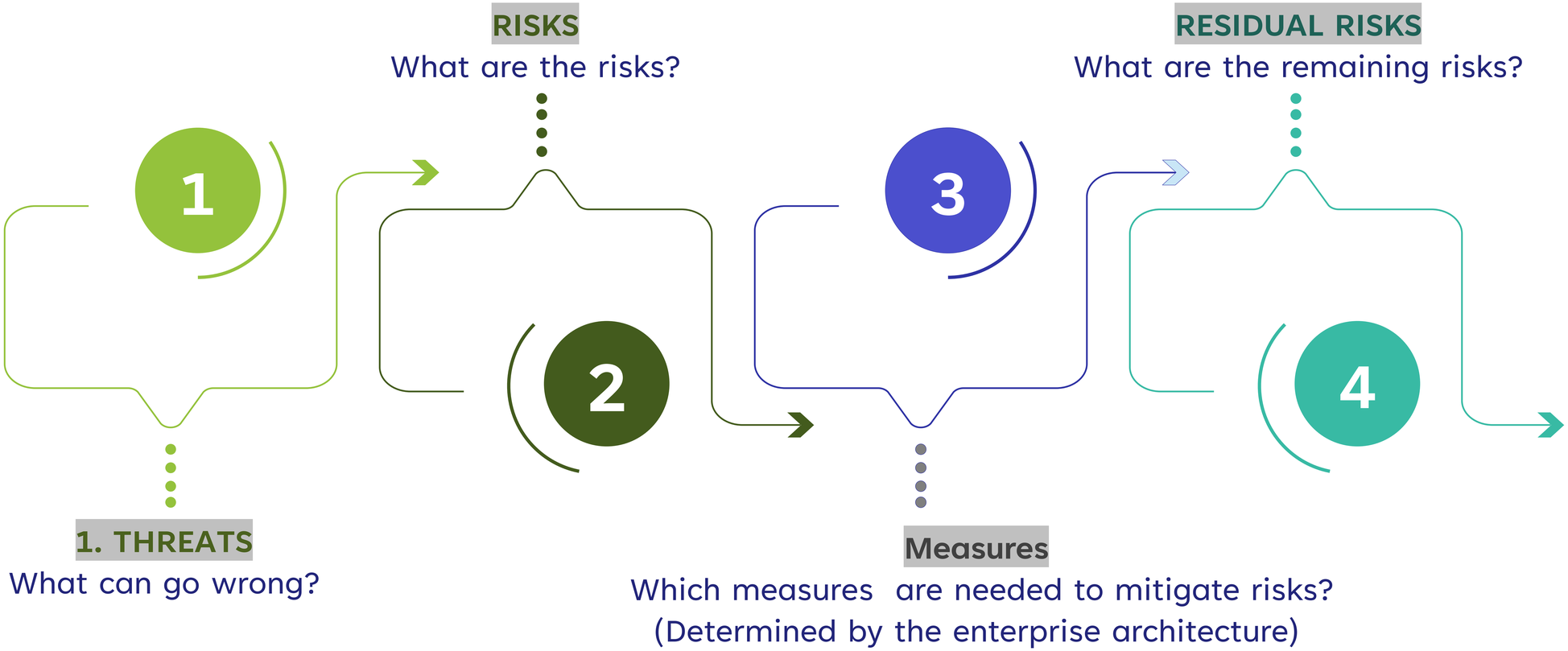
Contactinformatie

www.hu.nl/onderzoek/cyber-security

raymond.slot@hu.nl

Digital Sovereignty

Sovereignty Resilience Chain



Example Digital Sovereignty Threats

- **Tech Monopolies**: Reliance on major tech companies (e.g., from the U.S. or China) for cloud services, hardware, software, and social platforms can limit a nation's autonomy.
- **Supply Chain Vulnerabilities**: Foreign control over key hardware components (chips, networking equipment) can be a vector for espionage or disruption.

1. Foreign Dependence on Technology

- **Data Storage Abroad**: Sensitive data stored on foreign servers may be subject to foreign surveillance laws (e.g., U.S. CLOUD Act).
- **Cross-Border Data Flows**: Inadequate control over how personal and corporate data flows across borders undermines national regulatory power.

2. Data Sovereignty Issues

- **State-Sponsored Cyberattacks**: Espionage, infrastructure disruption, and information warfare conducted by foreign states.
- **Ransomware and Cybercrime**: Attacks by criminal groups can weaken trust in digital infrastructure and require international cooperation to resolve.
- **Zero-Day Exploits and Backdoors**: Unpatched software or hidden vulnerabilities can be exploited by hostile actors.

3. Cybersecurity Threats

- **Information Control by Foreign Platforms**: Social media and search engines controlled by foreign companies influence public opinion and policy debate.
- **Misinformation and Disinformation Campaigns**: Coordinated influence operations by foreign actors can destabilize democratic processes.

4. Platform Governance and Misinformation

- **AI Model and Infrastructure Control**: If large language models, foundational AI tools, or quantum computing are dominated by foreign entities, nations may lose control over key technologies.
- **Algorithmic Governance**: Foreign-developed algorithms affecting domestic decisions (e.g., in finance, health, or justice) may reflect external biases or interests.

5. AI and Emerging Tech Dominance

- **Extraterritorial Laws**: Foreign laws with global reach (e.g., export controls, sanctions, IP laws) can constrain domestic use of technology.
- **Lack of Digital Jurisdiction**: Inability to enforce national laws in cyberspace weakens sovereignty.

6. Legal and Regulatory Constraints

- **Digital Infrastructure Imposition**: Investment in local digital infrastructure by foreign governments or corporations (e.g., smart cities, 5G) can create dependency.
- **Surveillance Infrastructure**: Export of surveillance tech and norms may undermine local rights and institutions.

7. Technological Colonization

Potential Threats and Consequences

Threats

Full data Access

- US Government has access to all data, anywhere in the world

Weakening of privacy

- Conflicts between the GDPR and US legislation

Geopolitical Weapon

- Access to Trade or Governmental Secret Information

Nationalization of Data

- Data available to US Competitors

Business Consequences

1. Unpredictability in Regulations
2. Loss of Customer Trust
3. Compliance and Complexity Costs
4. Market Access Restrictions or Sanctions
5. Influencing Business Decisions (e.g., DEI policy)

Risk Impact Categories

Reputation and Credibility

- Declining customer loyalty and sales
- Falling stock prices
- Reduced investor confidence

Operational Delivery

- Revenue loss
- Operational inefficiencies
- Supply chain descriptions

Financials

- Increase costs
- Loss of financial information, i.e., invoices, etc.
- Decreased innovation budgets

Compliance, Legal and Regulatory

- Risk of Noncompliance
- Misreporting Regulatory Information
- Data, Privacy and Security violations

Levels of Risk Appetite

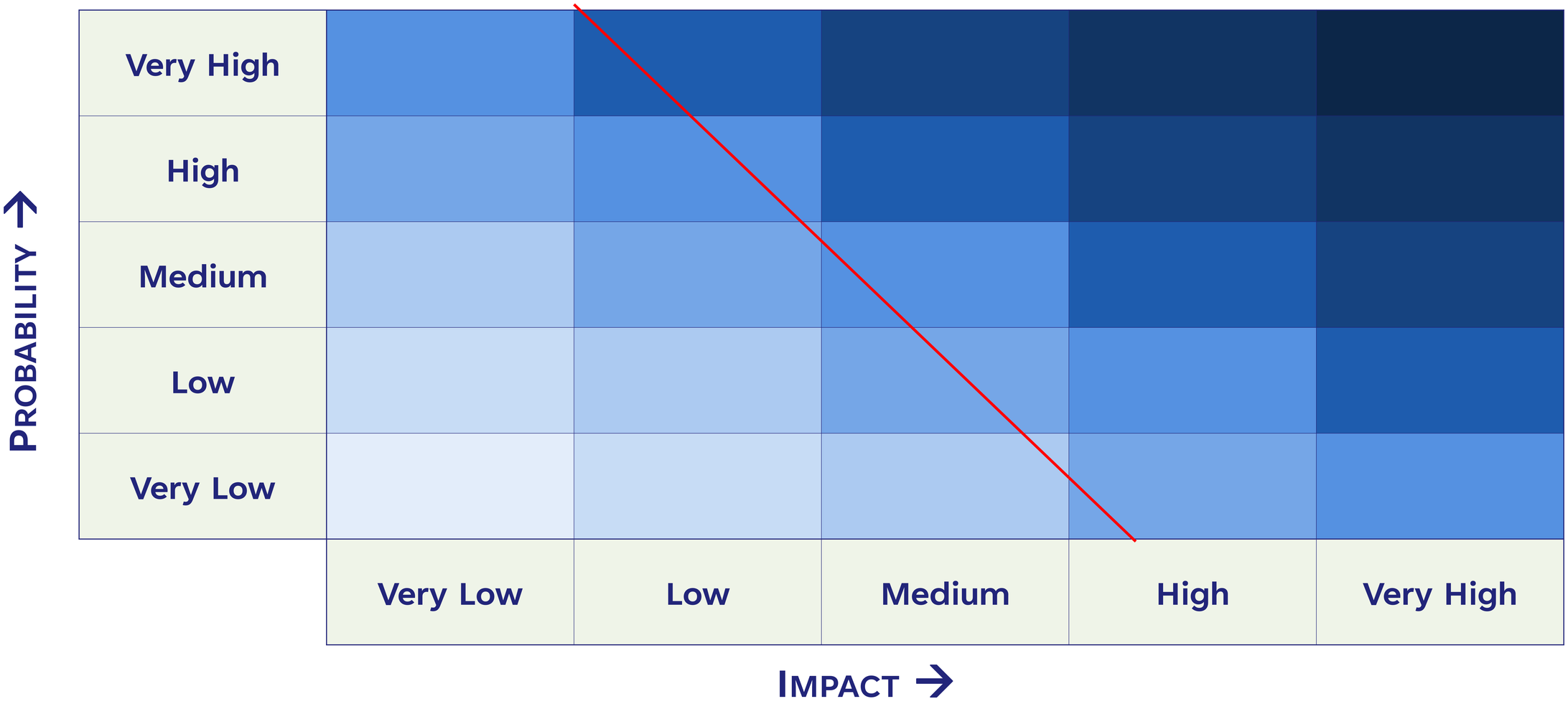
1. Averse	Avoidance of risk and uncertainty is a key organizational objective.
2. Minimalist	Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have the potential for limited reward.
3. Cautious	Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.
4. Open	Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery, while also providing an acceptable level of reward (and value for money, etc.).
5. Hungry	Eager to be innovative and to choose options offering potentially higher business rewards (this despite greater inherent risk).

Risk Appetite Level Definitions

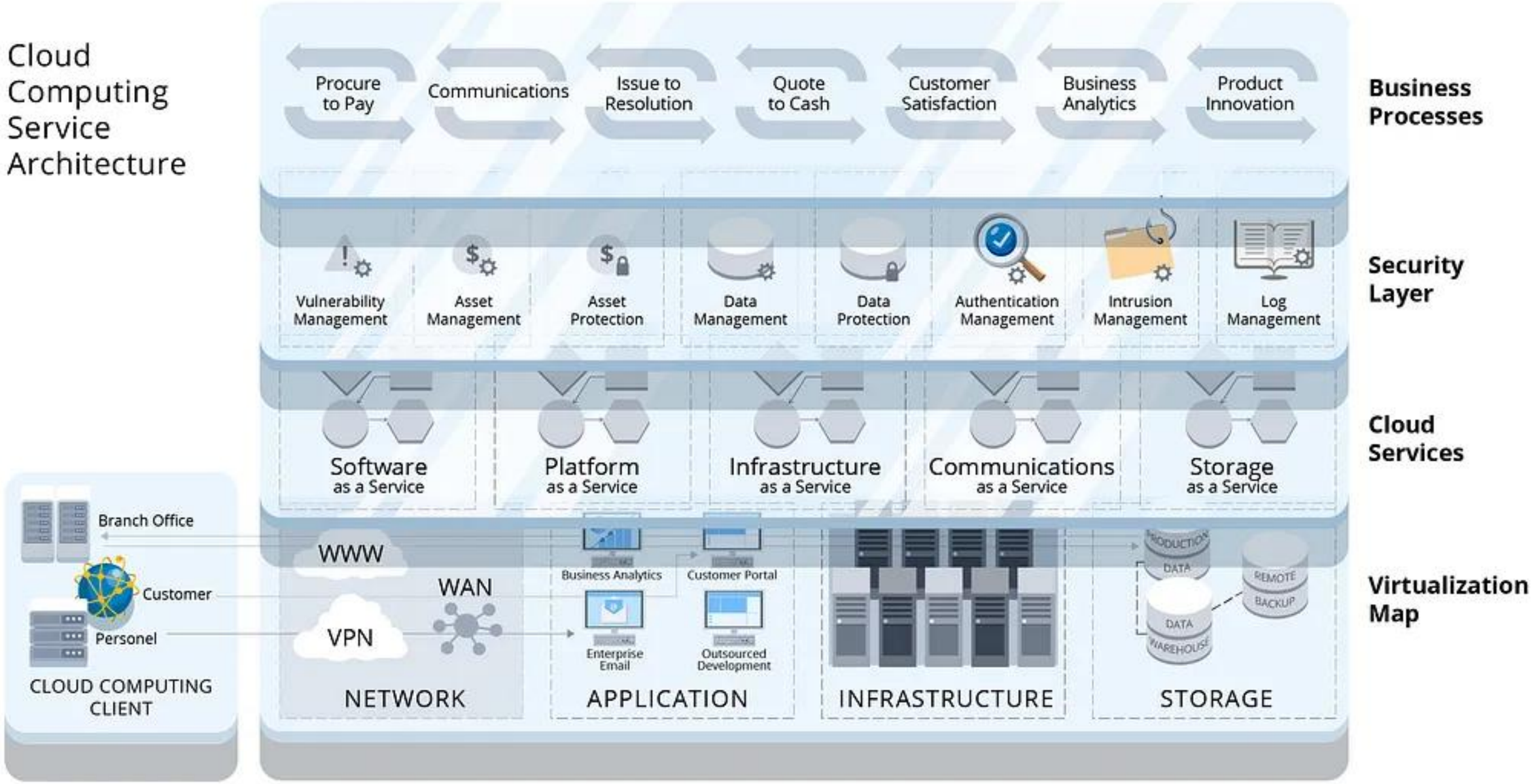
	1 Averse	2 Minimalist	3 Cautious	4 Open	5 Hungry
	Avoidance of risk and uncertainty is a key Organisational objective	**Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have a potential for limited reward.**	**Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.**	**Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward (and value for money etc.).**	**Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk).**
Category of Risk	**Example behaviours when taking key decisions…**				
Reputation and credibility	• Minimal tolerance for any decisions that could lead to scrutiny of the Government or the Department.	• Tolerance for risk taking limited to those events where there is no chance of any significant repercussion for the Government or the Department.	• Tolerance for risk taking limited to those events where there is little chance of any significant repercussion for the Government or the Department should there be a failure.	• Appetite to take decisions with potential to expose the Government or Department to additional scrutiny but only where appropriate steps have been taken to minimise any exposure.	• Appetite to take decisions that are likely to bring scrutiny of the Government or Department but where potential benefits outweigh the risks.
Operational and policy delivery	• Defensive approach to objectives – aim to maintain or protect, rather than to create or innovate. • Priority for tight management controls and oversight with limited devolved decision making authority. • General avoidance of systems / technology developments.	• Innovations always avoided unless essential. • Decision making authority held by senior management. • Only essential systems / technology developments to protect current operations.	• Tendency to stick to the status quo, innovations generally avoided unless necessary. • Decision making authority generally held by senior management. • Systems / technology developments limited to improvements to protection of current operations.	• Innovation supported, with demonstration of commensurate improvements in management control. • Systems / technology developments considered to enable operational delivery. • Responsibility for non-critical decisions may be devolved.	• Innovation pursued – desire to 'break the mould' and challenge current working practices. • New technologies viewed as a key enabler of operational delivery. • High levels of devolved authority – management by trust rather than tight control.
Financial/VFM	• Avoidance of financial loss is a key objective. • Only willing to accept the low cost option. • Resources withdrawn from non-essential activities.	• Only prepared to accept the possibility of very limited financial loss if essential. • VfM is the primary concern.	• Prepared to accept the possibility of some limited financial loss. • VfM still the primary concern but willing to also consider the benefits. • Resources generally restricted to core operational targets.	• Prepared to invest for reward and minimise the possibility of financial loss by managing the risks to a tolerable level. • Value and benefits considered (not just cheapest price). • Resources allocated in order to capitalise on potential opportunities.	• Prepared to invest for the best possible reward and accept the possibility of financial loss (although controls may be in place). • Resources allocated without firm guarantee of return – 'investment capital' type approach.
Compliance – legal / regulatory	• Avoid anything which could be challenged, even unsuccessfully • Play safe.	• Want to be very sure we would win any challenge.	• Limited tolerance for sticking our neck out. Want to be reasonably sure we would win any challenge.	• Challenge will be problematic but we are likely to win it and the gain will outweigh the adverse consequences.	• Chances or losing are high and consequences serious. But a win would be seen as a great coup.

Risks Matrix (probability × impact)

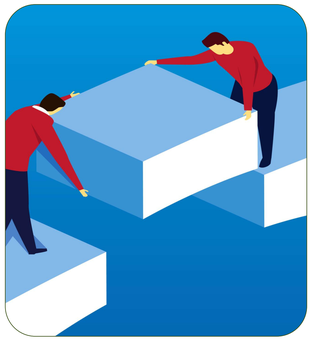
← Acceptable Unacceptable →



Create cloud architecture – indicating interdependencies and vulnerabilities



Sovereignty Risk Management Process Overview



1. Identify Initial Risks

- Threat assessment
- Risk assessment
- Risk appetite

2. Create Architecture

- End-to-End Models

3. Identify gap criticality

- Assess current controls and measures
- Identify gaps architecture ←→ current situation
- Assign gap criticality level

4. Calculate Residual Risk

- Calculate the residual risks
- Consolidate across gap criticality

5. Evaluate Acceptability

- Compare residual risk levels and risk appetite
- Acceptable Risk: Residual risk within defined limits.
- Unacceptable Risk: Requires additional controls or a change in strategy.

6. Roadmap

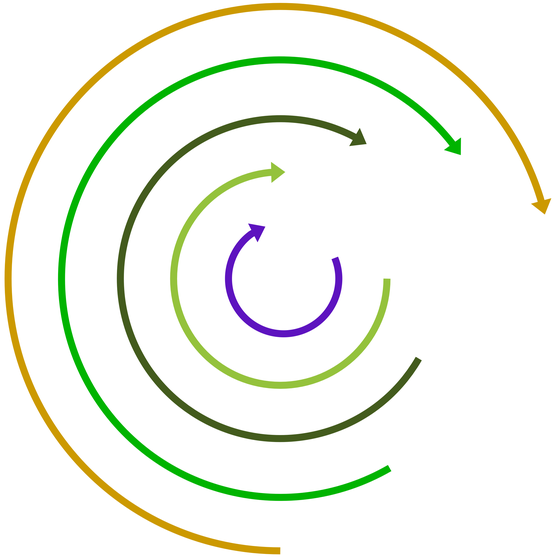
- Reevaluate architecture
- IT project
- Insure risks

7. Document and Monitor

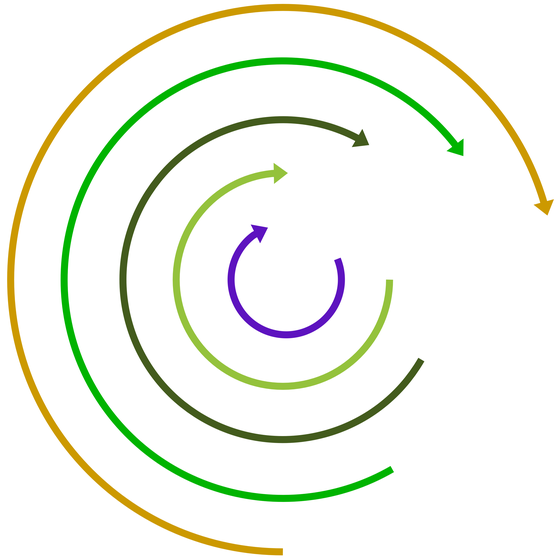
- Record the residual risks
- Continuously monitor risks

Considerations

Control Effectiveness
- How well do the implemented measures address the risks?



Compensating Controls
- Are there secondary processes that provide additional protection if primary processes fail?



Emerging Threats
- Does the residual risk assessment consider new and evolving developments?

Business Impact
- What are the consequences of residual risks on business operations, compliance, and reputation?

Cost-Benefit Analysis
- Are additional mitigations justifiable based on cost versus reduction in risk?


Thank you!