POWED – The Economics of Standardization and Certification

POWED – Economics of Standardization and Certification

Typically the argument against a standard goes like this:

P it's prescriptive!

O others are better!

W it assumes a waterfall model!

E it's expensive to use!

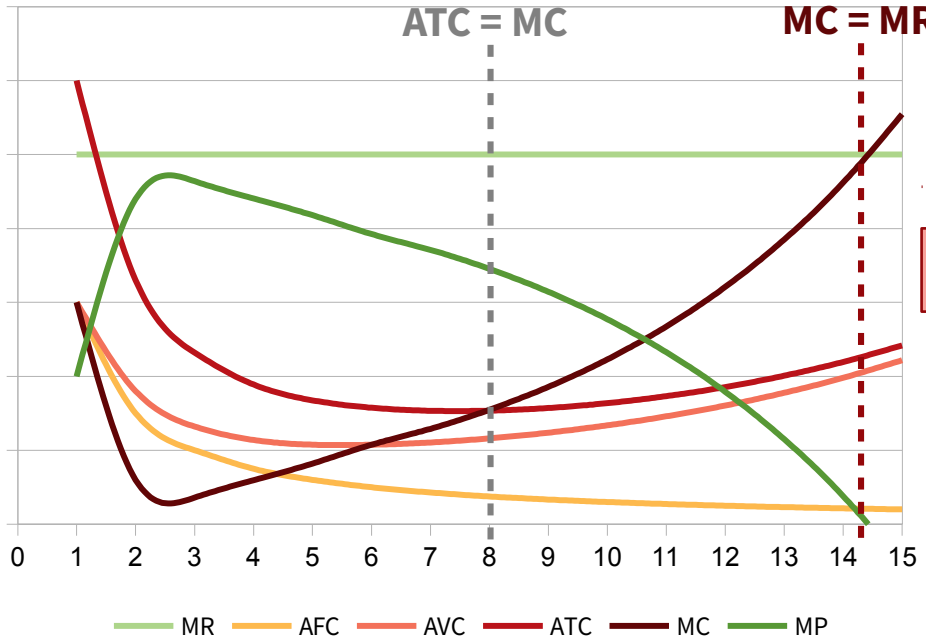
D it's document-laden!

Outline

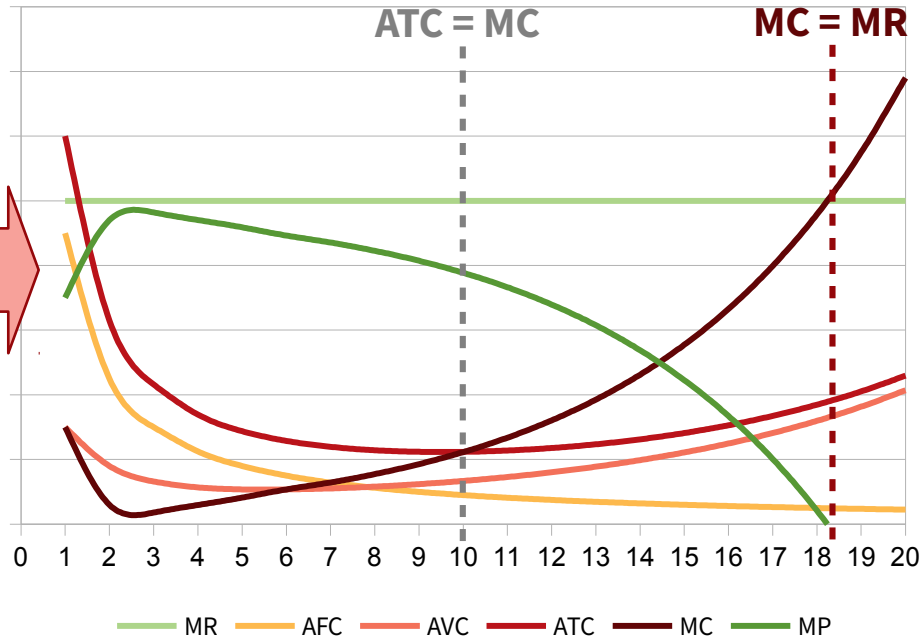
- **Economies of Scale and Scope**
- Utility in the Digital World
- Risk Management and this Clumsy Gut Feeling
- The Case for Standardization and Certification
- Outlook

Economics Briefing: The Traditional Manufacturer

Marginal Revenue, Costs and Profit of a Traditional Manufacturer



Marginal Revenue, Costs and Profit of a Traditional Manufacturer with Capacity Extension

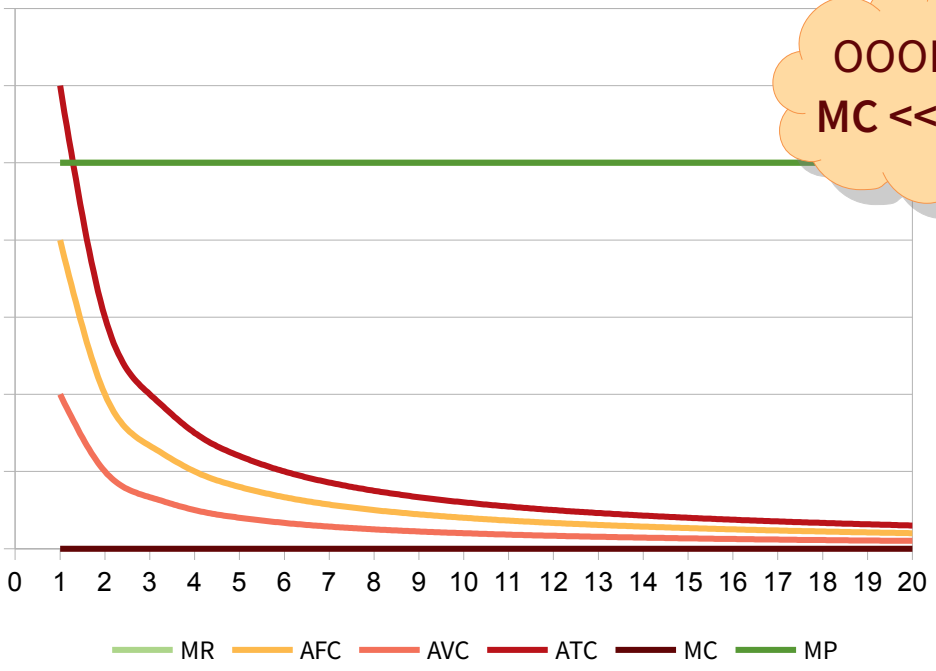


Economics Briefing: Lessons

- **Economies of Scale:** average total costs decline with increased output.
- **Diseconomies of Scale:** average total costs grow when they meet the marginal costs schedule, thus, marginal profits decline.
- **Constant Return to Scale:** average total costs are zero.
- When marginal profits turn negative (MC=MR ↔ 0 = MR – MC) the producer's cost schedule limits its production.
- Producers escape Diseconomies by capacity extension, either by increased investment in capital and labour or by advances in production (e.g. automation).
  → Note: Overcrowding effect affects costs.
- Plus: the marginal profit schedule indicates the producer's expected utility.

Economics Briefing: The Software Company

Marginal Revenue, Costs and Profit of a Software Producer



Marginal Revenue, Costs and Profit of a Software Producer with A New Hire

Economics Briefing: Lessons from Software

- The company enjoys increasing returns to scale since average total costs converge to zero.
- While such companies mainly face uncertainty in customer adoption and new competition, the strongest and unlimited entrepreneurial incentives are rendered by buyer's utility, supply, and weak regulation.
- The ability to enjoy returns from transactions with other customers, suppliers, or products is called a **network effect**. And it calls for coordination.
- By looking at the marginal profit schedule we find perfect elasticity which assigns strong bargaining power to the producer (price setting, discrimination).

Some Notes

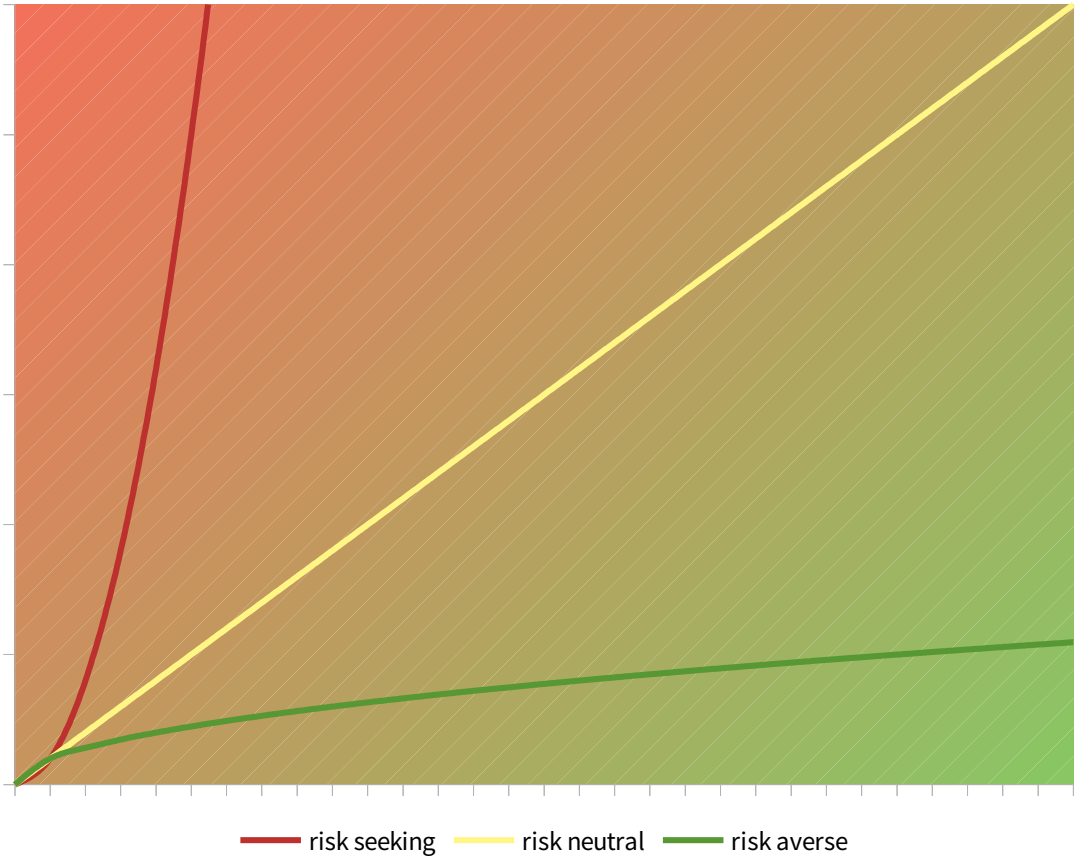
- Is an attacker any different from the software company?
- Do software companies actually enjoy increasing returns to scale?
- Or do software companies walk on a very long path from economies of scale through constant returns to scale until diseconomies of scale when the network gets saturated?
- Might it help to tax away the network effect on each sale of a new software item: $$software\ unit\ tax = \frac{software\ unit\ count\ (software\ unit\ count - 1)}{2} * tax$$?

  (Consider, the tax affects marginal returns and reimposes a natural limit to the unlimited connectability.)

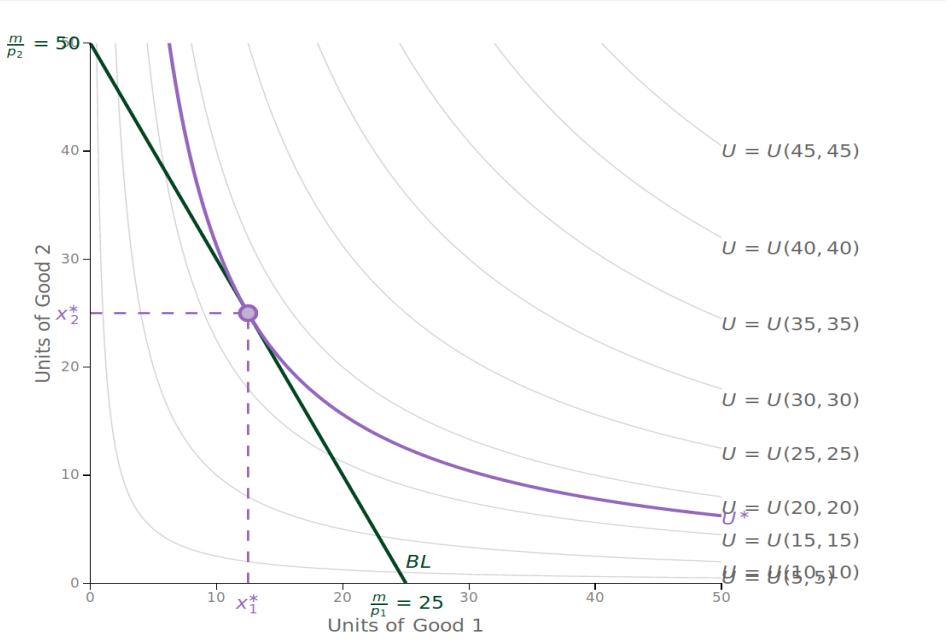
Outline

- Economies of Scale and Scope
- **Utility in the Digital World**
- Risk Management and this Clumsy Gut Feeling
- The Case for Standardization and Certification
- Outlook

Utility and Risk Bias



Utility Theory



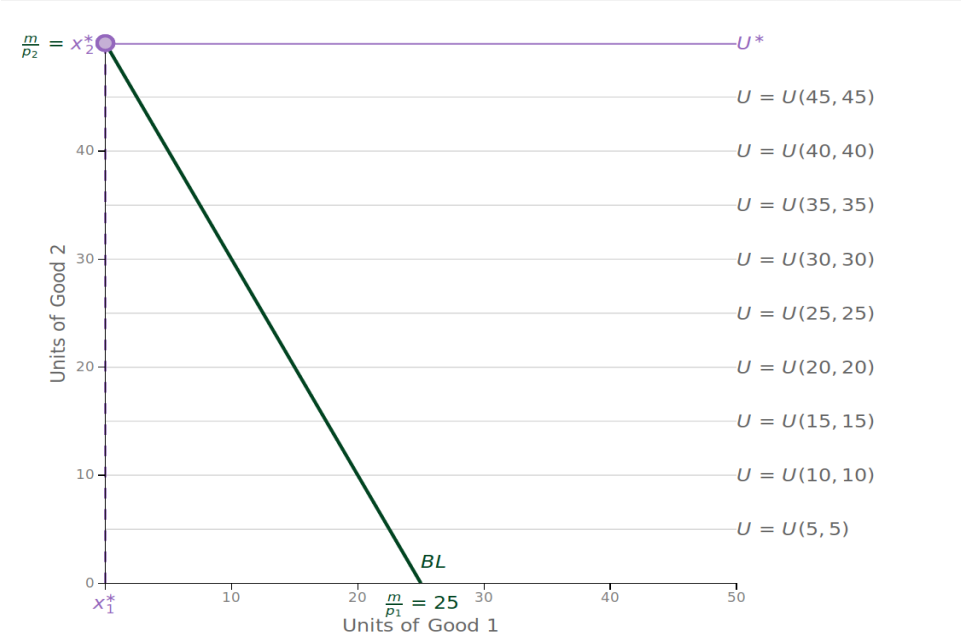
What can be changed?

- The preferences, i.e rules of the game
- The pricing parity, i.e. pay-off

Utility Function $U(x_1, x_2) = x_1^n * x_2^{(1-n)}; p_1 = 2 * p_2; n = 0.5; m = 50$

Note: concave graph, such as in the risk-averse case

Utility Theory: Preference Change



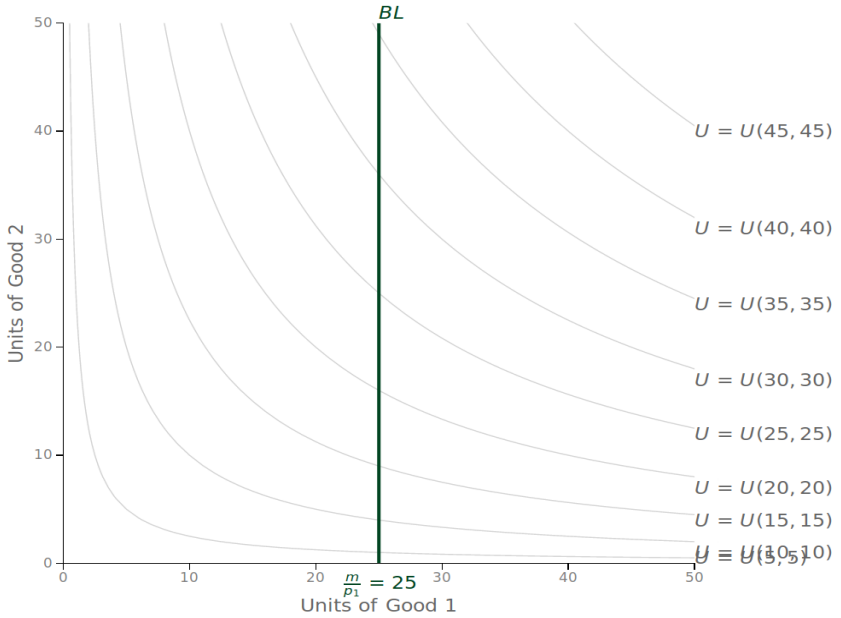
How to change?

- Nudging: behaviour change
- Market segmentation and fragmentation: hand-crafted vs. mass market goods, good ingredients

Utility Function $U(x_1, x_2) = x_1^n * x_2^{(1-n)}; p_1 = 2 * p_2; n = 0; m = 50$

Note: $U(x_1)=1$; $U(x_2)=x_2$, such as in the risk neutral case

Utility Theory: Payoff Change



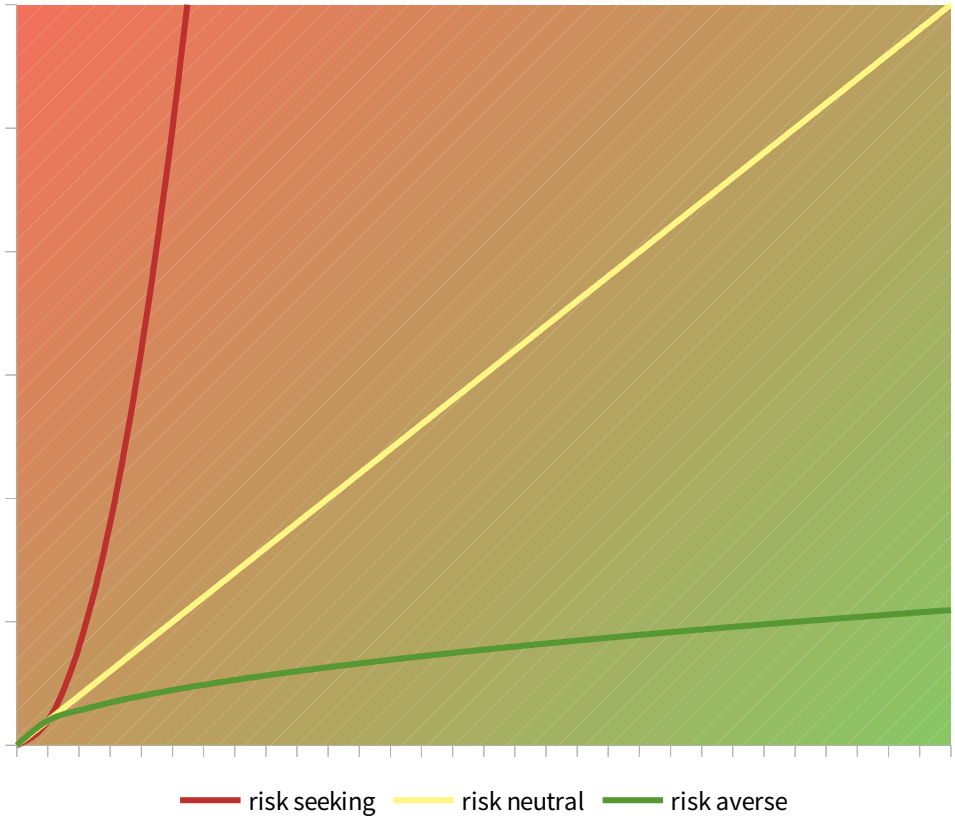
How to change?

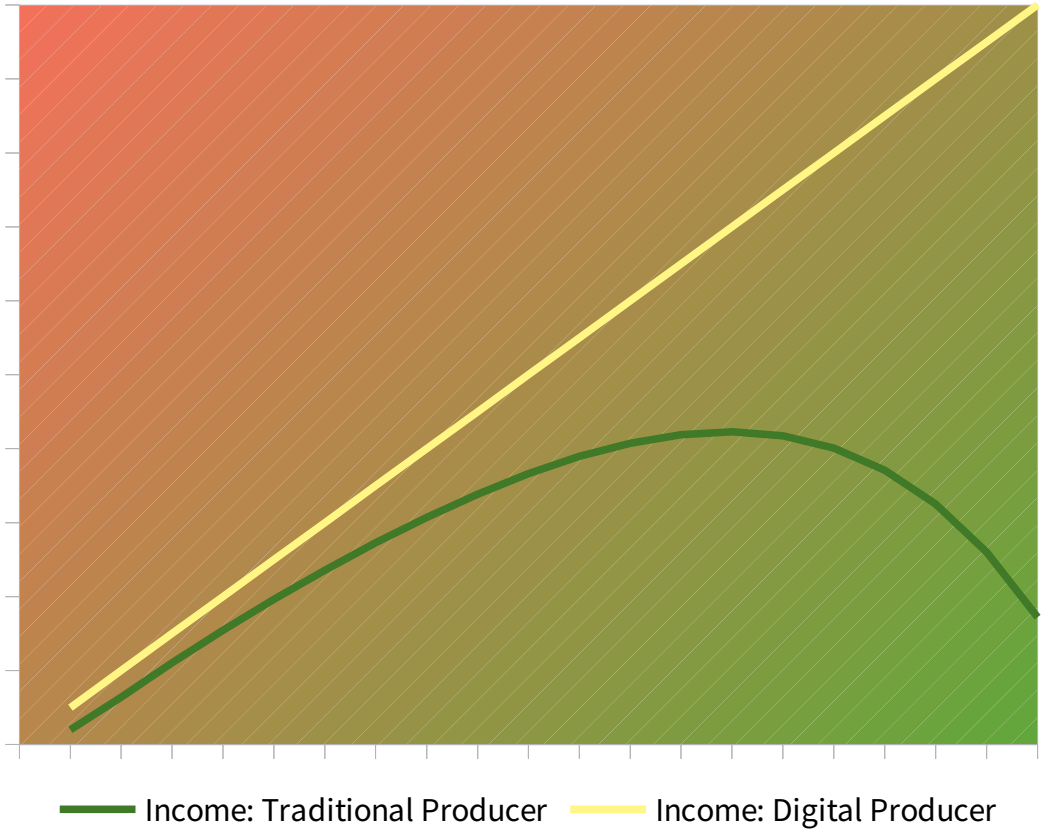
- Taxation: price adjustments
- Market segmentation and fragmentation: pricing of luxury and perennial goods

Utility Function $U(x_1, x_2) = x_1^n * x_2^{(1-n)}; p_1 = 2; p_2 = 0; n = 0.5; m = 50$

Note: no change in preference, demand for good 2 has become perfectly elastic

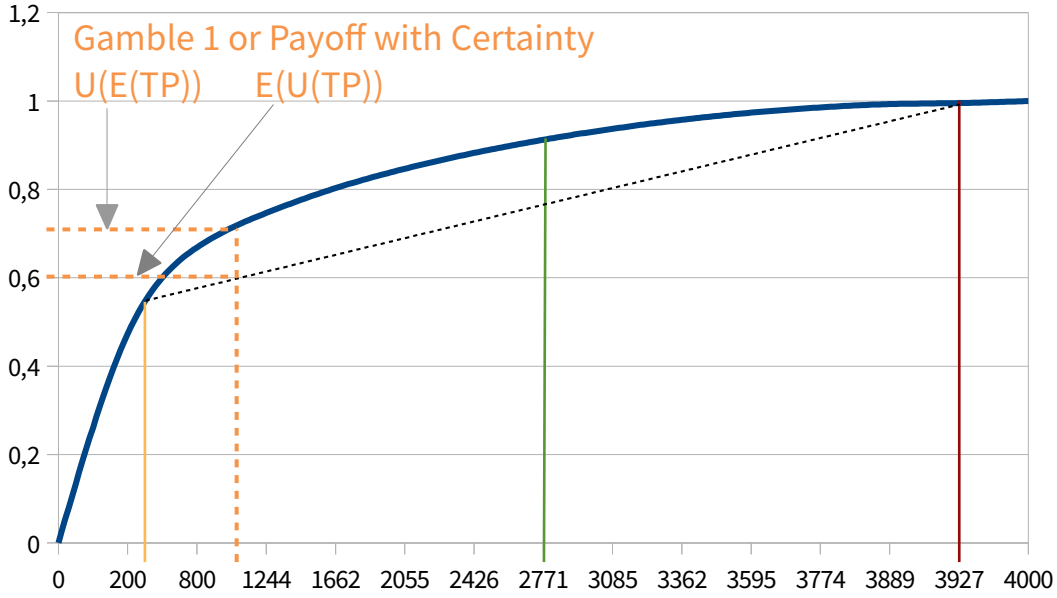
Introducing the Risk Bias





Hedging the producer's sales expectations

Our traditional producer likes to sell 8 items (2,771C) in any case, never less than 2 (340C) and never more than 14 (3,927C).



- The required cardinal utility curve is given by $U(TP)=\sqrt[4]{\frac{TP}{4{,}000}}\,;TP<4{,}000\,;TP:=total\ profit$
- Expected utility $E(U(TP))=p*U(tp_1)+(1-p)*U(tp_2)$
-

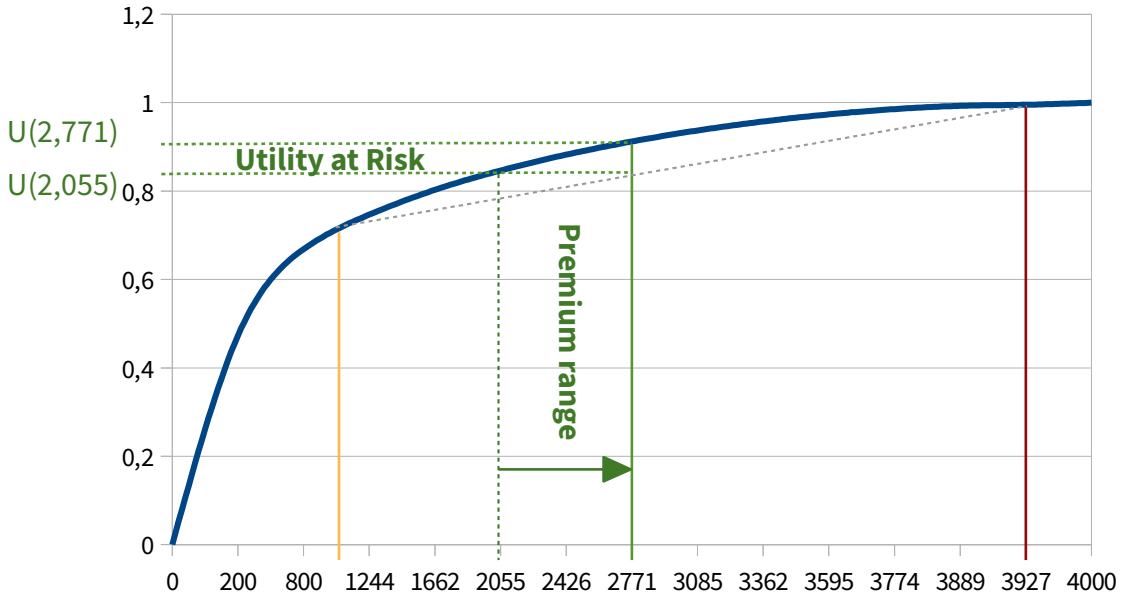
Gamble	E(TP)	U(E(TP))	E(U(TP))
1: $p_{tp1=340}$=0.82	986.66C	0.705	0.622
2: $p_{tp1=340}$=0.50	2,133.50C	0.855	0.768
3: $p_{tp1=340}$=0.18	3,281.34C	0.952	0.913

- What about our risk bias?
  We need a reference U(2,771)=0.912.

Lessons from the Neoclassical Utility Theory

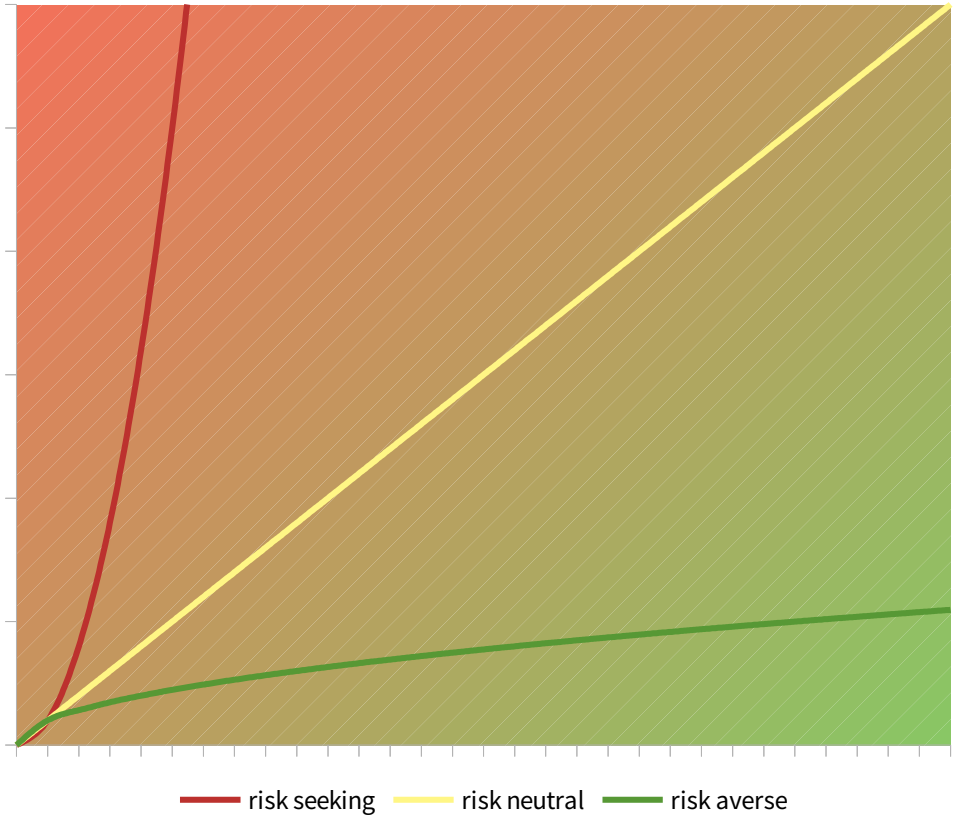
- The utility and probabilities shape the **rules of the game**.
- The reference value (or certain pay-off) and rules of the game impose the **risk bias**.
- Insurance is not available on incomplete data and for risk neutral players.

- **Hedging risks** means covering the difference between a gamble's expected utility and utility of a certain pay-off.



The Risk Bias Revisited

- Constant returns to scale (from software or data sales) make our digital producer risk neutral.
- **A zero-priced app lets the user identity dissociate**
  - **As a data consumer she becomes risk loving** since the app's utility unfolds only in a sizeable network.
  - **As a data producer she stays risk averse**.
- Such cases cannot be insured since the app vendor commands the risk bias.
- The network effect impose a lock-in, e.g. for a Whatsapp user the switching costs come up to 3-10$ (1.5bln users, 5 to 15 bln $ revenue)



Free Chocolate For All?

- By accepting the **free offer we bought ourselves into the utility curve of the vendor and her risk appetite**.
- Awareness campaigns? *Nice try, thank you.*
- Sandboxing? Virus scanners? *What for?*
- Example:
  - Facebook's Announcement for using Encryption in my words: "your data is secure in our environment … that parametrizes security commensurate to our risk appetite and business model."

Outline

- Economies of Scale and Scope
- Utility in the Digital World
- **Risk Management and this Clumsy Gut Feeling**
- The Case for Standardization and Certification
- Outlook

This Clumsy Feeling Again

- In safety, the environment is protected from a subject/object according to rules.
- In safety, we enjoy simple models with direct causation and a few hazards that can be easily parametrized.
- In security, some subject/object seeks protection from its environment that suffices its/owners individual risk appetite.
- In security, we often figure threats or actions by an uncharacterised attacker:
  - Do we know *all causes, i.e. possible vulnerabilities*?
  - Can we *estimate its probabilities*?
  - What about a *threat's impact?*
  - How do we know our *model is complete, undistorted, not exaggerated*?

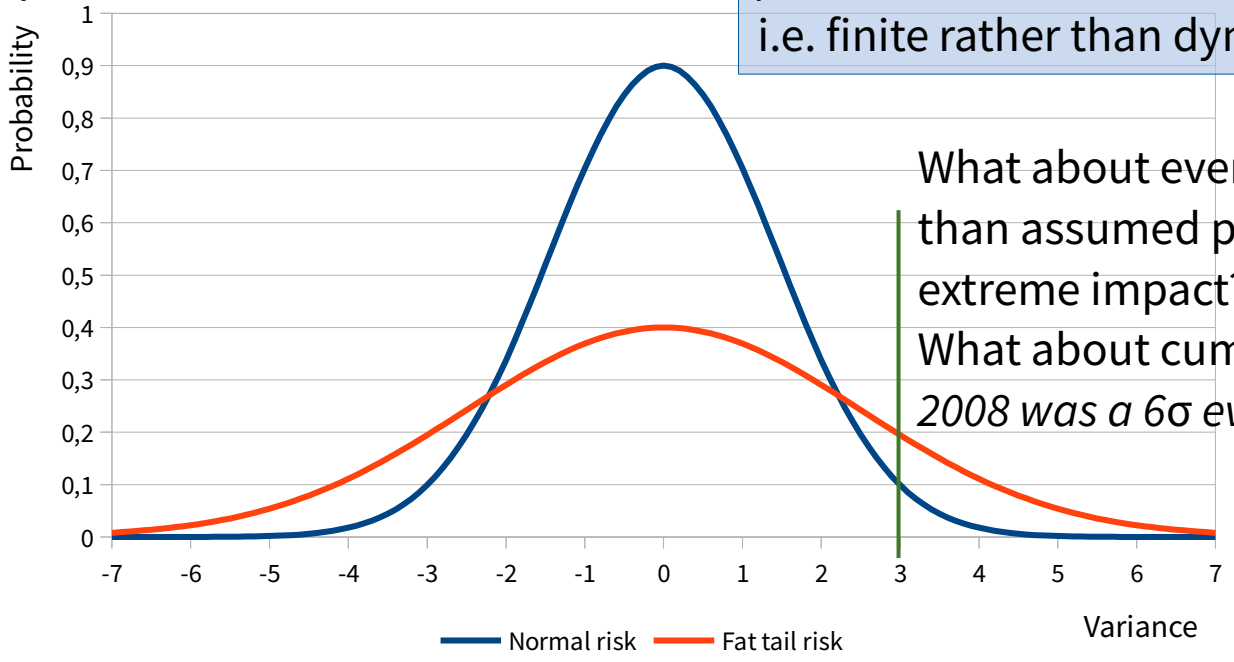
Risk Modelling Issues

- **Unavailability of Referencing Anchor** – the risk free asset
- **Parameter uncertainty:**
  - Stochastic: randomness or natural variability (causation)
  - Epistemic: imprecision, vagueness or ignorance (depth of problem)
- **Model uncertainty:** analyst's bias towards abundance, transposition, exaggeration, simplification/elimination
- **Completeness Uncertainty:** risk inducing environment, life span, and contributors are not fully absorbed

Problematic Risk Perception

How can a vulnerability be stochastically defined?
How to compensate for a vulnerability?
How to score compensation measures?

In Security we consider risks as *single* and un*correlated* events with *semi-objective probabilities* and *limited impact*, i.e. finite rather than dynamic games.



What about events with higher than assumed probability and extreme impact?
What about cumulative losses?
2008 was a 6σ event.

Security Metrics?

- $ROSI = Savings - Tool\ Costs$?
- Famous Gordon-Loeb Model on Security Investment (GL):
  Expected Net Benefits from an Investment in Information Security

$$ENBIS(z) = \{v - S(v,z)\}L - z\,;\, S^{I}(z,v) = \frac{v}{(\alpha z+1)^{\beta}}\,;\, \boxed{S^{II}(z,v) = v^{\alpha z+1}}$$

$v := conditional\ probability\ of\ a\ successful\ vulnerability\ exploitation\,;\, 0 \leqslant v \leqslant 1$

$z := Investment$

$L := \lambda t\,;\, \lambda := Loss\,;\, t := threat\ probability\,;\, 0 \leqslant t \leqslant 1$

$\boxed{\alpha, \beta := productivity\ of\ a\ security\ investment\,;\, \alpha > 0\,;\, \beta \in \mathbb{R}}$

→ Finding by maximizing *ENBIS(z)*: **never invest more than 37% of your loss!**

- Remember the risk bias induced by our zero-priced app?
- The GL model works for small figures, but not in real world applications.
  For $z \in \mathbb{R} \to \infty$ and $0 \leq v < 1$ we get $v^{\alpha z+1} = 0$ and thus $ENBIS(z) = vL - z$ irrespective of the investment's productivity α!
  To compensate for $z \in \mathbb{R} \to \infty$, we need an unproductive investment **α=n/z** ($n \in \mathbb{N}$), that gives us $(v - v^{n+1})L - z$ though we should get $-(L + z)$.

Intermediate Wrap Up

- We learned
  - Productivity in scale economies
  - Incentives in constant returns to scale
  - Utility in networks and flipped preferences
  - Uncertainty, risk bias, the need for a risk free value (at least systemic risk)
- Can Game Theory help us?

Get your Terminology Straight!

- A (negative) positive **externality** is the (cost) benefit that affects a party who did not choose to incur that (cost) benefit.
- **Asymmetric information:** imperfect and/or incomplete information
  - Incomplete (rules of the game): Adverse Selection
  - Imperfect (state of the game): Moral Hazard
- **Uncertainty:** expected value predictable, not its probability or timing.
- **Risk:** stochastic insecurity regarding moral hazard, i.e. an ex-post expected value and its probability is known but not its timing.

Game Theory

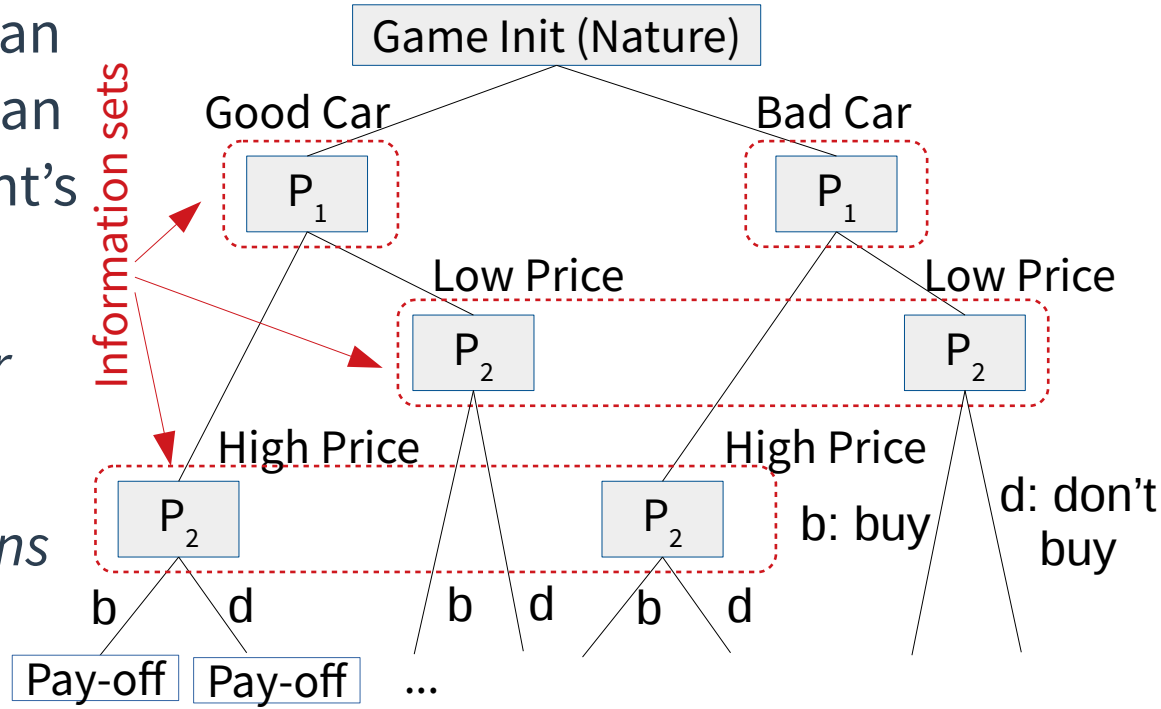
- **Game Theory: study of strategic interdependence**
- **Availability of common knowledge about participants** – *Which game are we in?*
  (In)Complete Information: players **do (not) know game's rules (possible actions*, pay-offs).**
  → in incomplete games the pay-off is determined by the opponent's type and the player's common prior beliefs
- **Observability of Actions** – *Where are we at?*
  (Im)Perfect Information: players **can (not) observe (at least some of) their opponents' actions***.
  → imperfect information appears in simultaneous games**.
- **Since incomplete information games have no solution, risk management means transforming such a game into a game with imperfect information by assuming a player type whose actions are predictable but unobservable (moral hazard).**

* Strategy: complete action plan by which each player's decisions are predetermined for each set of information.
** Imperfect information games are therefore incomplete information games but not vice versa.

Solving Games with Incomplete Information

- **Bayes' Solution:** from an outcome B correlated to an event E with an estimated probability P(E) we can draw the probability of the event's occurrence P(E|B)
- For each iteration: *updating our current probabilities* (beliefs)
- Ideally, we have *infinite iterations*

- Building an extensive game



Problematic Risk Perception

- Risk: $Expected\ Value = Event * Probability\ ;\ Event \ni (Threat\ , Opportunity\ , Efforts\ for\ Attack \wedge Defense\ , Impact)\ ;\ Impact = Loss - Recovered\ Loss$
- A viable risk model should:
  - Assume security as an infinite game, since the finite game of securitization is lost.
  - Internalize negative externalities to reflect costs and benefits of risk decisions.
  - Profile attacker and defender behaviour as well as estimate their efforts and adaptability.
  - Establish intelligence from reliable incident data (cause, impact, mediation).
  - Offer models for expressing and parametrizing incidents (loss, probabilty).
  - Align securitization incentives and efforts properly.
  - Stackelberg and Green Security Games promise solutions for adaptive utility models of human preferences.

Outline

- Economies of Scale and Scope
- Utility in the Digital World
- Risk Management and this Clumsy Gut Feeling
- **The Case for Standardization and Certification**
- Outlook

Why Standardize or Certify?

- Coordination: setting the game rules (voluntary, dirigisme, from the fringe)
- Interoperability: setting the pay-off structure
- Externalities: network effects

Requires *sponsored* networks and coordination

- Key Motivation
  - Market leadership
  - Intellectual property
  - Capability to invent
  - Lead time (First Mover)
  - Production capabilities
  - Abilities for complements and extensions
  - Image and brand
  - **Ideology: „Not Invented Here“**

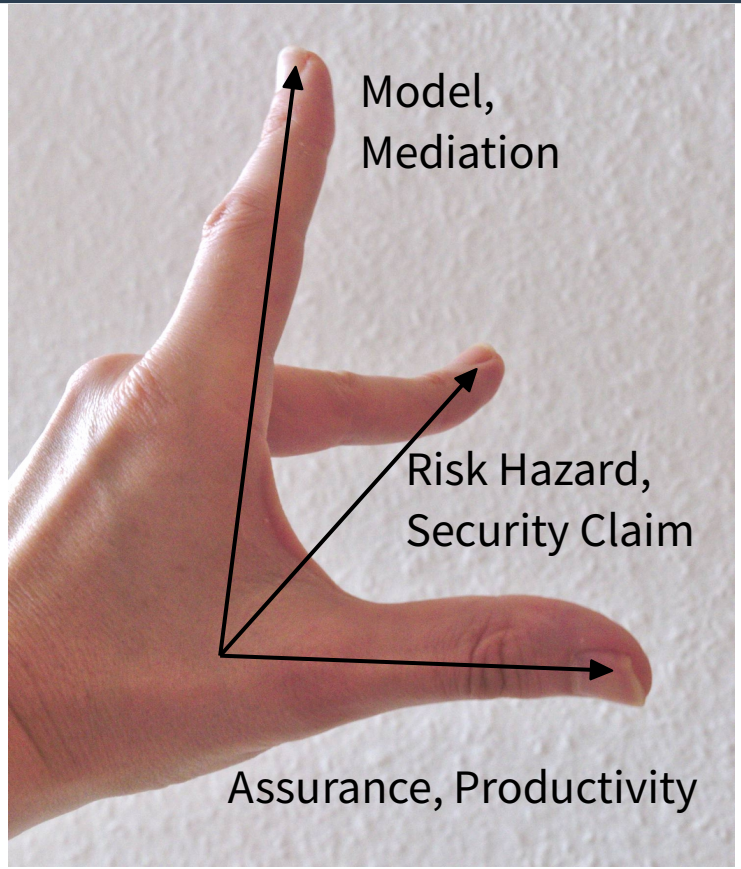
The Case of F(L)OSS in Standardization and Certification

- Unsponsored technologies suffer more from standardization since no actor seeks to internalize its positive network effect, i.e. neither capitalizes on the decreasing average costs through standardization nor invests into standardization.
- Unsponsored technologies lack the incentives to protect the invention effort and secure the revenue (from production & licenses). **Since no one owns them, anyone may abuse them** - most often they fall prey to ideological clashes – think of systemd and SysV.
- Let‘s face the truth, folks: **the copyleft bars standardization since you cannot own the product (tragedy of the commons)**, i.e. forks and incompatibilities may arise.
- And since security is a need developed and implemented over the long run, the survival rate of F(L)OSS groups often fall short of an impact.

Another Example: Agile Development and Certification

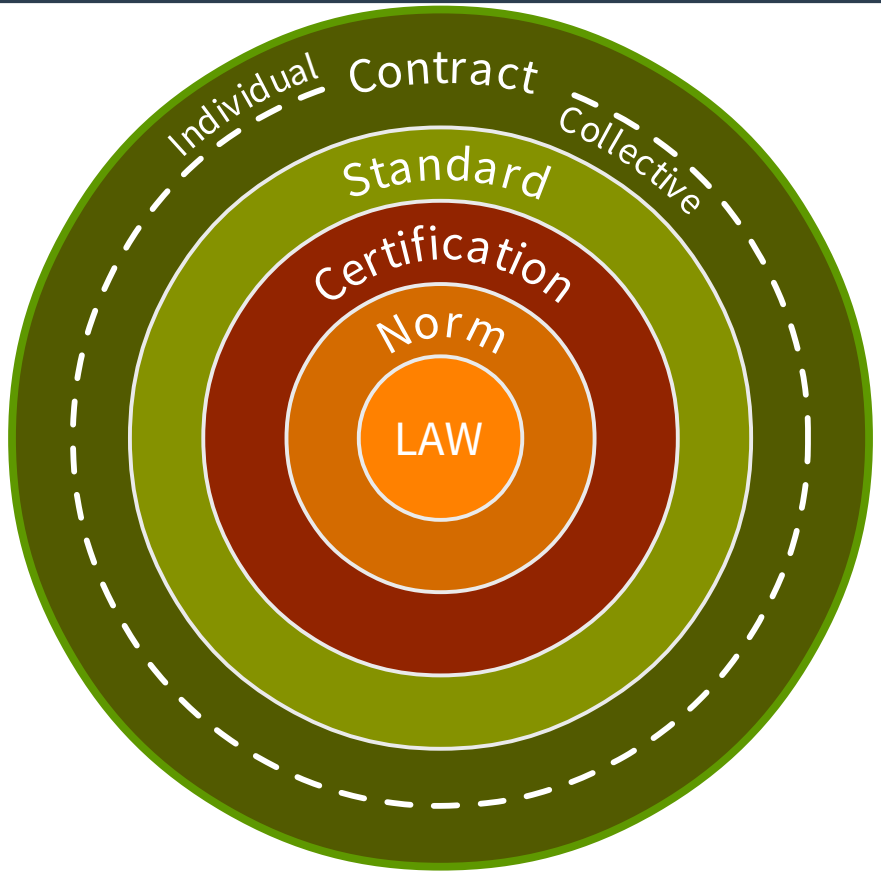
- Certificates aim at signalling the verification of a product/service owning correct and effective measures which meet claimed objectives.
- Agile aims at eliciting the real user needs by a human-centric narrative and and implementing these in story-based, peer-reviewed implementation cycles (run).
- Agile increases usability and quality but not productivity (crowding out).
- Certifying each run effectively inflates the certification costs since the consistency of security objectives and whether they are met by correct and effective measures need to be reconsidered for each run.
- Such process-based evaluations dump the developer's liability on the certifier.

Scopes of Standardization and Certification



- Models define the shape and scope of risk hazards and assurance
  - How are hazards expressed?
  - Who or what observes and verifies hazards in assurance and how?
- Model Influence
  - Techno-agnostic, such as Common Criteria
  - *Economic School of Stakeholders*
  - *Legal framework (legitimizing needs)*
- *Supervision of model's life cycle*

The Regulatory Scope: Legal Hierarchy



The Regulatory Scope: WTO and Conformity Assessments

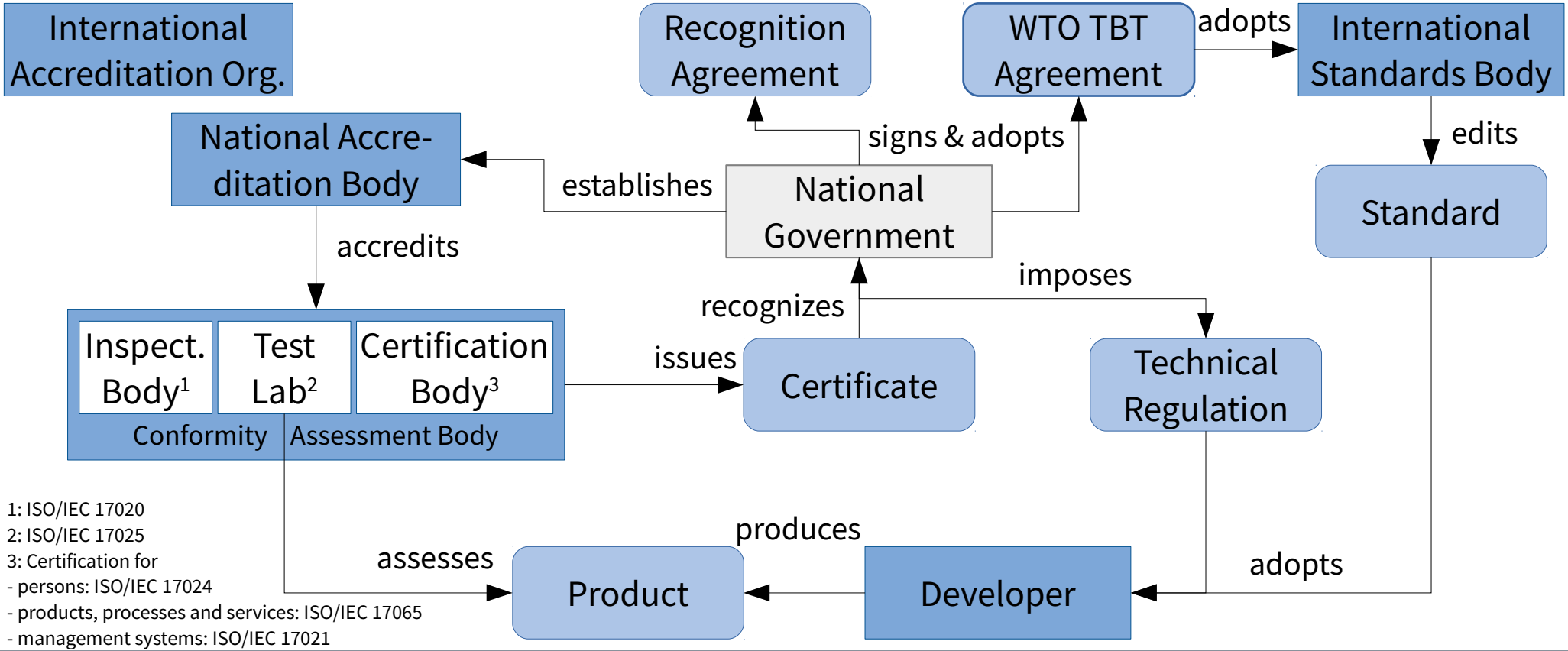
- World Trade Organization (WTO)
  - is an institutional umbrella for **multi lateral rade agreements** under the law of nations.
  - **harmonizes the global rules of trade and seeks to reduce barriers to trade.**
- **Technical regulations and standards** aim at the *characteristics and/or processes or production methods of a product – allowed per se* by WTO TBT Agreement, Annex 1.
- **Code of Practice for Standards**: transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, development dimension (Article 4, Annex 3).
- ***Standard conformity is voluntary whereas technical regulation is mandatory*** (Annex 1).
  A regulation may be a non-tariff barrier.
- **Conformity Assessment** is *any procedure used, directly or indirectly, to determine that relevant requirements in technical regulations or standards are fulfilled.* (Annex 1)

https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm, https://www.wto.org/english/tratop_e/tbt_e/tbt_info_e.htm

The Regulatory Scope: WTO's Assessment Requirements

- Preparation, Adoption, and Application of Technical Regulation (Articles 2-3)
  - Regulations *"are not prepared, adopted or applied with a view to, or with the effect of, creating unnecessary obstacles to trade"* (Art. 2.2).
  - *Legitimate objectives are national security requirements, prevention of deceptive practices, protection of human health or safety, protection of animal and plant life or health or the environment* (Art. 2.2).
  - Product requirements termed *as performance rather than design or descriptive characteristics* (Art. 2.8).
  - Transparency to other members (Art. 2.9), Equivalence of other member's regulation (Art. 2.7).
- Conformity Assessments (Articles 5-8):
  - Procedures of central government bodies, such as harmonization (Art. 5).
  - Recognition of by non-/government bodies, such as mutual recognition (Art. 6-8).
  - Regulatory measures and specifications are to be based on international standards (Art. 9).

The Regulatory Scope: Institutionalizing Assessments



EU Cyber Security Act

- **Regulation** aims at „horizontal requirements“ for cybersecurity certification in the *digital single market* that „**shall be binding in its entirety and directly applicable in all Member States.**“ (Art. 228 TEU)
- Established through a Trilogue between the European Parliament, the Council of the EU and the European Commission from September 2017 until December 2018
- Tasks for ENISA (CSA, Title II, Chapter Ia):
  1) Expertise: Knowledge and information (Art. 9), Research and Innovation (Art. 11), analyse threat landscape
  2) Policy: Development and implementation of Union policy and law (Art. 5), e.g. advisory and incident reports
  3) Capacity: Building (Art. 6), Awareness raising and education (Art. 10), e.g. vulnerability disclosure, CERTs & CSIRTs
  4) Cooperation: Operational cooperation at Union level (Art. 7)
  5) Certification: Market, cybersecurity certification, and standardisation (Art. 8)
  6) Enabling: International Cooperation (Art. 12)

Note: regulations, directives, decisions/recommendations are secondary legislation derived from the primary legislation of the EU treaty

EU Cyber Security Act: Justification

„(50) **Currently**, the **cybersecurity certification** of ICT products, services and processes **is used only to a limited extent.** When it exists, it **mostly occurs at Member State level or in the framework of industry driven schemes.** In this context, a **certificate issued by one national cybersecurity authority is not in principle recognised by other Member States.** Companies thus may have to certify their products, services and processes in several Member States … [e.g. for] national procurement procedures, **thereby adding to their costs.** Moreover, while new schemes are emerging, **there seems to be no coherent and holistic approach with regard to horizontal cybersecurity issues**, for instance in the field of the Internet of Things.

Existing schemes present significant shortcomings and differences in terms of product **coverage, levels of assurance, substantive criteria and actual utilisation, impeding mutual recognition mechanisms within the Union.“**

EU Cyber Security Act: Schemes

Justification (57) and Title III, Article 48:

„**Recourse to European cybersecurity certification** and EU statement of conformity **should remain voluntary**, unless otherwise provided in Union or Member States legislation adopted in accordance with Union law. **In the absence of harmonised legislation, Member States may adopt national technical regulations** in accordance with Directive (EU) 2015/1535 **providing for mandatory certification under a European cybersecurity certification scheme. Member States could also use the recourse to European cybersecurity certification in the context of public procurement** and Directive 2014/214/EU.

However, with a view to achieving the objectives of this Regulation and **avoiding the fragmentation of the internal market, *national* cybersecurity certification schemes or procedures** for the ICT products, services and processes **covered by a European cybersecurity certification scheme should cease to produce effects from the date established by the Commission by means of the implementing act.**“

EU Cyber Security Act: Assurance Levels

Article 46: „1. A European cybersecurity certification scheme may specify **one or more of the following assurance levels: basic, substantial and/or high**, for ICT products, services and processes.

The level of assurance shall be **commensurate with the level of the risk, in terms of the probability and impact of an incident,** associated with the intended use of an ICT process, product or service.

2. The **assurance levels** basic, substantial and high **shall refer to a certificate or an EU statement of conformity issued in the context of a European cybersecurity certification scheme, which provides for each assurance level respective security requirements including security functionalities and the corresponding degree of effort for the evaluation** of an ICT process, product or service. The **certificate or the EU statement of conformity is characterised with reference to technical specifications, standards and procedures related thereto**, including technical controls, **the purpose of which is to decrease the risk** of, or to prevent cybersecurity incidents as follows …“

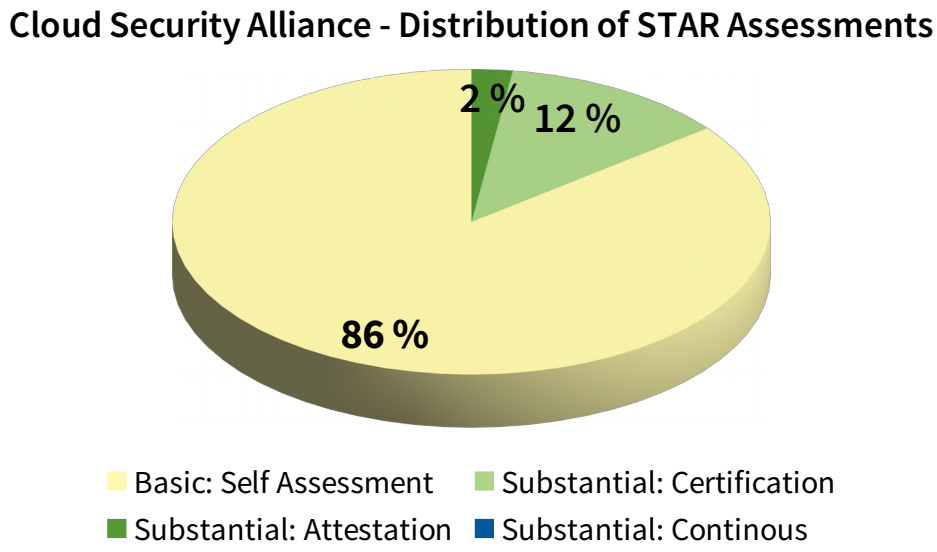
EU Cyber Security Act: Assurance Framework

Assurance Level	**Assurance Statement**	**Evaluation Target**	**Evaluation Goal**	**Evaluation Activities** *[at least]*
Basic (Art. 46(a))	Conformity *or* Certificate	**security requirements** [and] **functionalities** [are **met**] **and evaluated**	**minimise known basic risks** for cyber incidents and attacks	**review of a technical documentation***
Substantial (Art. 46(b))	Certificate		**minimise known** cyber **risks, incidents and attacks carried out by actors with limited skills and resources**	**reviewing the non-applicability of publicly known vulnerabilities *and* testing** [the] **correct implementation of security functionality***
High (Art. 46(c))	Certificate		**minimise risk of state-of-the-art cyber attacks carried out by actors with significant skills and resources**	**Substantial Activities *plus* assessing** [the] **resistance to skilled attackers via penetration testing***

***** *or substitute activities* with equivalent effect

EU Cyber Security Act: A Race To The Bottom?

- Moving from sector specific functional requirements towards horizontal assurance requirements is a clever move, but ...
- Schemes may suffer badly from fragmented requirements (product specific, operations, systems), ineffective implementation, and insufficient monitoring.



EU CSA vs. the Paragon of the New Legislative Approach

- The Regional Appeal Court Frankfurt/Main, 2012:
  The product declaration "CE-approved" is ***misleading*** *if the declarator by using this declaration only* ***confirms*** *his* ***product's conformity with the relevant regulations****.*
- The Regional Appeal Court Zweibrücken, 2014:
  Under liability law, ***such marks do not even contain a guarantee promise from which the product buyer can assert contractual claims for compensation against the manufacturer in the event of quality defects.*** *If such marks have no liability-related relevance vis-à-vis the manufacturer, this applies in particular to the certifying 'Notified Body', which only has to check the quality management system of the manufacturer..*
- **Enforcement:** *Prosecution of a company following an* ***accident where a person got their hand trapped in a roller and suffered multiple fractures.*** *The* ***company was fined £4,000*** *after being found to be non-compliant with the Supply of Machinery (Safety) Regulations.*
  [http://www.cemarkingassociation.co.uk/how-is-the-ce-mark-enforced/]

The Regulatory Scope: Scheme Types for Assessments

Private Schemes (1st Party Assessment)
A developer creates, tests, and qualifies the product.
Applicable to legal peers contracting their needs that cannot be generalized.

Contractual Schemes (2nd Party Assessment)
A developer creates and tests the product.
An independent second party is accredited for evaluating and certifying the product.
Applicable to groups with similar needs responding to external conformance needs.

Public schemes (3rd Party Assessment)
Adds an independent, third party to a contractual schemes that issues the certificate ad therefore a guarantee that all evaluation requirements are met.
Responsibilities and liabilities are distributed among participants.
Applicable to members in a subordinate relationship that are to provide compliance evidence.

The Regulatory Scope: Economic Reasoning

- Avoid market failure in order to keep the system (game) running:
  - Externalities: Network Effects(+), Lock In(-), Asymmetric Information(-)
  - Monopolies/Collusive Market Participants(-)
  - Public Goods/Tragedy of the Commons (→ FLOSS)
  - Inexistent/Incomplete Markets or Transaction Systems
- Foundations in Economic Schools:
  - Neo-Classical Models: marginal costs, scale economies, game and utility theory
  - Empirical Models: Institutional Economics, i.e. Government Mediation

What is a socially optimal standard then?
A market policy of choice (maximal utility) or complete information (minimal uncertainty)?

Outline

- Economies of Scale and Scope
- Utility in the Digital World
- Risk Management and this Clumsy Gut Feeling
- The Case for Standardization and Certification
- **Outlook**

The Regulatory Dilemma (I)

Businesses

- ... prioritize vertical integration in order to achieve quality assurance and compatibility in the supply chain but differentiation against their peers.
- ... prefer differentiation against their peers (horizontal), e.g. by certification.
- ... prefer protection of their local market and lobby often for the “new legislative approach” leading to chilling effects (co-/self-regulation, basic signalling requirements, incentives).

Regulators and consumers (of digital products/services)

- … are participants of multiple hazard environments that in turn refer to the same unique attributes they have.
- … may be unknowing of and unable to express their utility while their consumption depends primarily on network externalities.
- … want comparable quality assurance from their supply chain while being neutral towards vendors and technologies in order to race to the skill top and reduce transaction costs.

The Regulatory Dilemma (II)

Businesses

- … often understand certification as a means for escaping regulation and promoting risk exchange, i.e. transferring risky goods into another liability sphere.
- … often scrutinize whether the impact of signalling/screening schemes outweigh their required efforts.
- … call for regulator intervention, when transactions are impeded by cluttered security requirements.

Regulators and consumers (of digital products/services)

- … are often not in a superior position regarding asymmetric information when organizations deny information disclosure or supervision due to reputation damages, e.g. for qualification of attack patterns or assurance.
- … face a trade-off in setting up schemes that make the signal/screening only affordable to good but not bad players.

In Defense for Standardization and Certification (I)

- Standardization
  - + Transforms Scope Economies into Scale Economies by reducing transaction costs
  - + Increases user base (network externality and enhanced learning)
  - + Establish an infrastructure for innovation (strong correlation between the number of standards and indicators of innovation)
  - + Increases competition and reduces prices (compatibility)
  - + Creates ecosystems (complements, second sourcing)
- Certification
  - + Structures processes through splitting them into scorable work items
  - + Strengthens organizational roles
  - + Reduces uncertainty by providing a scoring system and reference values independent from competition
  - + Allows for differentiation

In Defense for Standardization and Certification (II)

- Standardization
  - + Spurs vertical integration and lessens/heightens the chance for monopolies
  - + Improves welfare if they prevent a race to the bottom
  - − May create monopolies through intertemporal lock-in
  - − Does not eliminate market fragmentation since smaller players will retreat into local niche markets due to the costs and liabilities imposed by standards
- Certification
  - + Signals independent verdicts based on conformance assessments
  - − Might be costly to the unprepared
  - − Might be slow in adopting trends when scoring models are unavailable or unproven
  - − Might fail to align the incentives of developers and consumers

POWED – Economics of Standardization and Certification

- *P: Its' prescriptive!* How would you describe and coordinate your interoperability solution while being alone and how would you ensure your access to other systems?
- *O: Others are better!* Why do you battle this standard rather than switching to the better one?
- *W: It's a waterfall model!* Eventually, we all submerge in that ocean we raised from.
- *E: It's expensive to use!* How much would you have to invest into signalling that your product is better than your competition and how much more revenue would you have made from not conforming to the standard?
- *D: It's documentation dependent!* So, you don‘t account your revenues and expenses and do not know what your employees do?

Privacy?

- Let‘s be honest. There is none!
- As long as privacy is not a property (right), there is no way to establish responsibilities and to effectively defend it against profiteering.
- But when privacy is a right, would we allow its defensive use to hide away harmful or reckless decisions?
  … Think of subprime borrowers.