Quantifying Security:

Oslofjord!

TOM GILB
COMPETITIVE
ENGINEERING
A HANDBOOK FOR SYSTEMS ENGINEERING, REQUIREMENTS ENGINEERING, AND SOFTWARE ENGINEERING USING PLANGUAGE

Ask me for a free electronic copy!
(by email or memory stick here)

Tom@Gilb.com

www.Gilb.com

Result Planning Limited

Norway/UK

Updated April 7 2008

Krakow, Poland April 8th 2008

THE PRINCIPLE OF 'QUALITY QUANTIFICATION'

- **All qualities can be expressed quantitatively,**
- ***'qualitative'* does *not* mean unmeasurable.**

"In physical science the first essential step in the direction of learning any subject is to find principles of numerical reckoning and practicable methods for measuring some quality connected with it.

I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it;

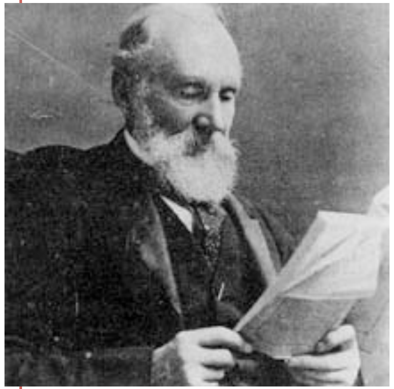
but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind;

it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of Science, whatever the matter may be."

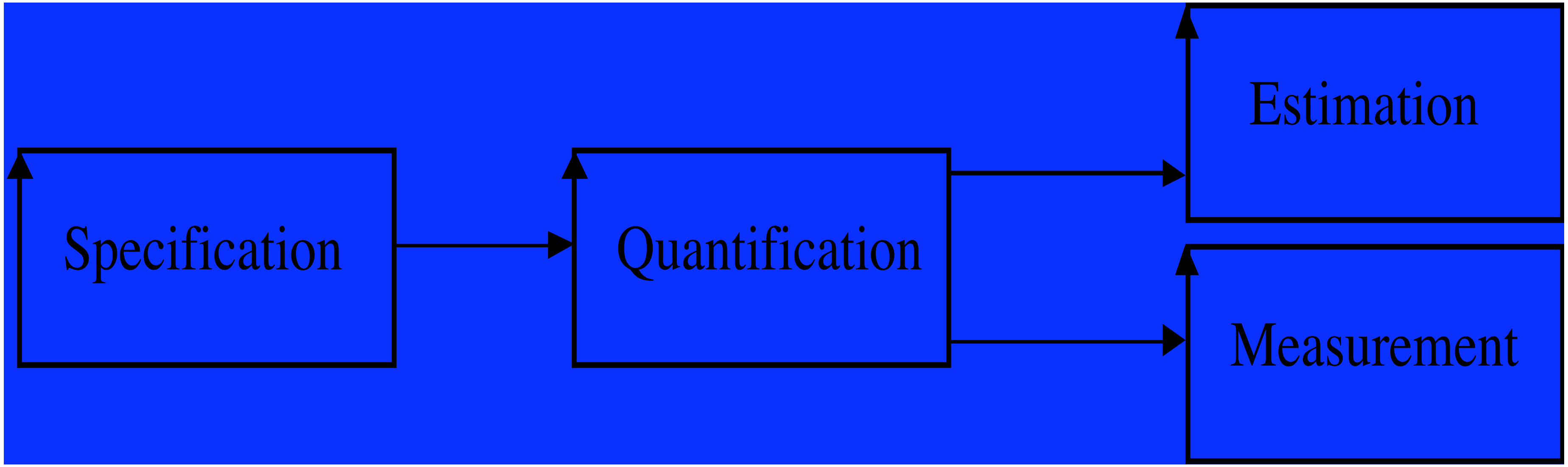
Lord Kelvin, 1893

from

http://zapatopi.net/kelvin/quotes.html



Basic Concepts:

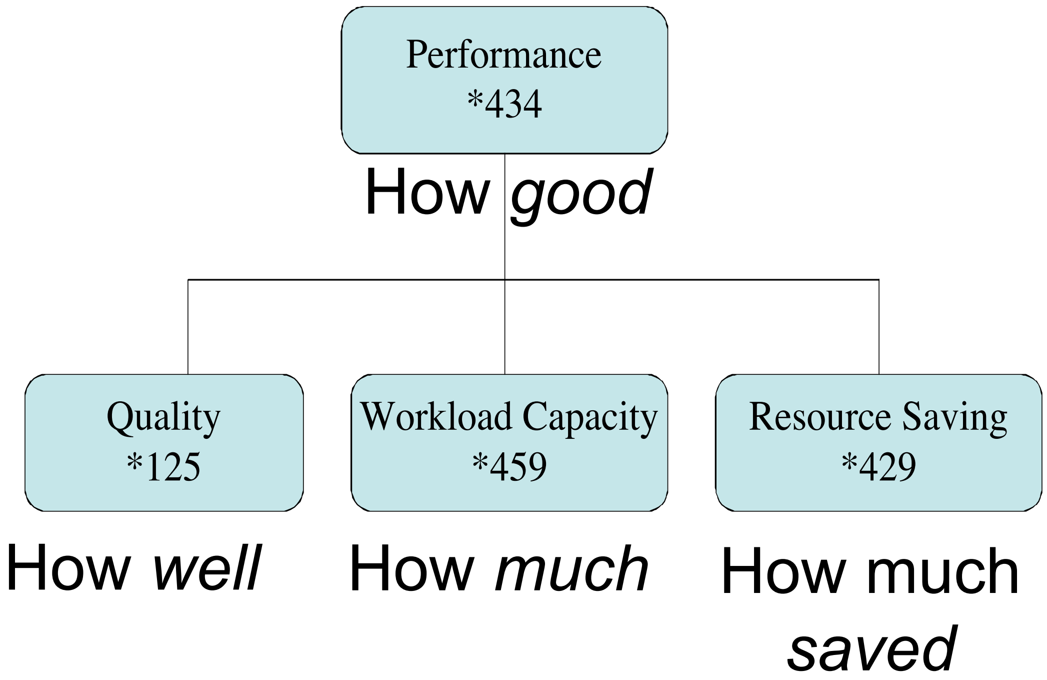


Quality: the concept, the noun

Planguage Concept *125, Version: March 20, 2003

A ‘**quality**’ is

- a scalar attribute -|-|-|-|- (Scale symbol)
- reflecting ‘how *well*’ ------Past Level<------------>
- a system functions. (Fn)------Past Level<--------->



Performance *434

How *good*

Quality *125

How *well*

Workload Capacity *459

How *much*

Resource Saving *429

How much *saved*

Can you Quantify Security?

- Can you define a Scale of measure for Security?

- **Security**:
- Type: Quality Requirement.
- Scale: ________________?

- Goal [Next Release, Our Software] ____ ?

ISA (Information Security Assurance) security sub-team of IEEE development Standard for Developing Software Life Cycle Processes, P1074 concluded:

- **"Efforts that do not treat security**
  - **as an integral part of systems engineering**
  - **and architecture**
  - **fail to provide security.**
- It no longer makes any business sense
  - to spend any money,
  - apply any resources and
  - proceed with any Software Development project
  - unless corporate assets and private customer data will be sufficiently secure."
  - [Barbara Biszick-Lockwood]
  - http://www.qualityit.net/

Example: “VERY TOP LEVEL PROJECT GOALS

Security Administration Compliance:

Security Administration Compliance:

Ambition*: to become compliant and to remain continuously compliant with all current officially binding security administration requirements both from CORP X and Regulatory Authorities.*

Scope: *Account Opening and Entitlement Reporting.*

Scale: % compliant with CORP X Information Security Standards (CISS) [CORP X Information Security Office (CISO)] on a defined System or Process.

Note: CISS is an officially binding security administration requirement with which we must become compliant.

“VERY TOP LEVEL PROJECT GOALS
Security Administration Compliance:

Security Administration Compliance:

Ambition: to become compliant and to remain continuously compliant with all current officially binding security administration requirements both from CORP X and Regulatory Authorities.

Scope: Account Opening and Entitlement Reporting.

Scale: % compliant with CORP X Information Security Standards (CISS) [CORP X Information Security Office (CISO)] on a defined System or Process.

Note: CISS is an officially binding security administration requirement with which we must become compliant.

========= Benchmarks=================

Past [CISS = RSA and IT DIVISION ISAG Compliance Matrix [Regional Security Administration and IT DIVISION Independent Security Administration Group, October 2003] **25%** <- JC, Nov-03

Note: The RSA/IT DIVISION Compliance Matrix originates from Otto CXXX and is based on CISS.

“VERY TOP LEVEL PROJECT GOALS
Security Administration Compliance:

Security Administration Compliance:

Ambition: to become compliant and to remain continuously compliant with all current officially binding security administration requirements both from CORP X and Regulatory Authorities.

Scope: Account Opening and Entitlement Reporting.

Scale: % compliant with CORP X Information Security Standards (CISS) [CORP X Information Security Office (CISO)] on a defined System or Process.

Note: CISS is an officially binding security administration requirement with which we must become compliant.

========= Targets ===================

Wish [Deadline = March 2004, Systems = High Criticality Systems] **100%**

Wish [Deadline = June 2004, Systems = {Medium & Low} Criticality Systems] **100**%

Note: Wishes are stakeholder valued levels that we are not yet sure we can deliver in practice, on time, so we are not promising anything yet, just acknowledging the desire.

Goal [Deadline = March 2004, Systems = High Criticality Systems] 90%±5%

Goal [Deadline = June 2004, Systems = {Medium & Low} Criticality Systems] 90%±5%

Goal [Midline = February 2004] **50%±10%** “intermediary goal short of 100%”

Note: Goal levels are what we think we can really promise and focus on. These types of goals push us into thinking about possible Evolutionary result delivery steps.

Stretch [Deadline = March 2004, Systems = High Criticality Systems] 95%±5%

Stretch [Deadline = June 2004, Systems = {Medium & Low} Criticality Systems] 95%±5%

Note: Stretch levels are something that we might be able to achieve if we have sufficient resources, focus and technology available, but we are not sure of that yet. We are NOT promising it now! So this is a way to hold the ideals up in case those things become available.”

"VERY TOP LEVEL PROJECT GOALS
Security Administration Compliance:

Security Administration Compliance:

Ambition: to become compliant and to remain continuously compliant with all current officially binding security administration requirements both from CORP X and Regulatory Authorities.

Scope: Account Opening and Entitlement Reporting.

Scale: % compliant with CORP X Information Security Standards (CISS) [CORP X Information Security Office (CISO)] on a defined System or Process.

Note: CISS is an officially binding security administration requirement with which we must become compliant.

========= Targets ====================

Wish [Deadline = March 2004, Systems = High Criticality Systems] 100%

Wish [Deadline = June 2004, Systems = {Medium & Low} Criticality Systems] 100%

Note: Wishes are stakeholder valued levels that we are not yet sure we can deliver in practice, on time, so we are not promising anything yet, just acknowledging the desire.

Goal [Deadline = March 2004, Systems = High Criticality Systems] 90%±5%

Goal [Deadline = June 2004, Systems = {Medium & Low} Criticality Systems] 90%±5%

Goal [Midline = February 2004] **50%±10%** "intermediary goal short of 100%"

Note: Goal levels are what we think we can really promise and focus on. These types of goals push us into thinking about possible Evolutionary result delivery steps.

Stretch [Deadline = March 2004, Systems = High Criticality Systems] 95%±5%

Stretch [Deadline = June 2004, Systems = {Medium & Low} Criticality Systems] 95%±5%

Note: Stretch levels are something that we might be able to achieve if we have sufficient resources, focus and technology available, but we are not sure of that yet. We are NOT promising it now! So this is a way to hold the ideals up in case those things become available."

“VERY TOP LEVEL PROJECT GOALS

Security Administration Compliance:

Security Administration Compliance:

Ambition: to become compliant and to remain continuously compliant with all current officially binding security administration requirements both from CORP X and Regulatory Authorities.

Scope: Account Opening and Entitlement Reporting.

Scale: % compliant with CORP X Information Security Standards (CISS) [CORP X Information Security Office (CISO)] on a defined System or Process.

Note: CISS is an officially binding security administration requirement with which we must become compliant.

========= Targets ===================

Wish [Deadline = March 2004, Systems = High Criticality Systems] 100%

Wish [Deadline = June 2004, Systems = {Medium & Low} Criticality Systems] 100%

Note: Wishes are stakeholder valued levels that we are not yet sure we can deliver in practice, on time, so we are not promising anything yet, just acknowledging the desire.

Goal [Deadline = March 2004, Systems = High Criticality Systems] 90%±5%

Goal [Deadline = June 2004, Systems = {Medium & Low} Criticality Systems] 90%±5%

Goal [Midline = February 2004] **50%±10%** “intermediary goal short of 100%”

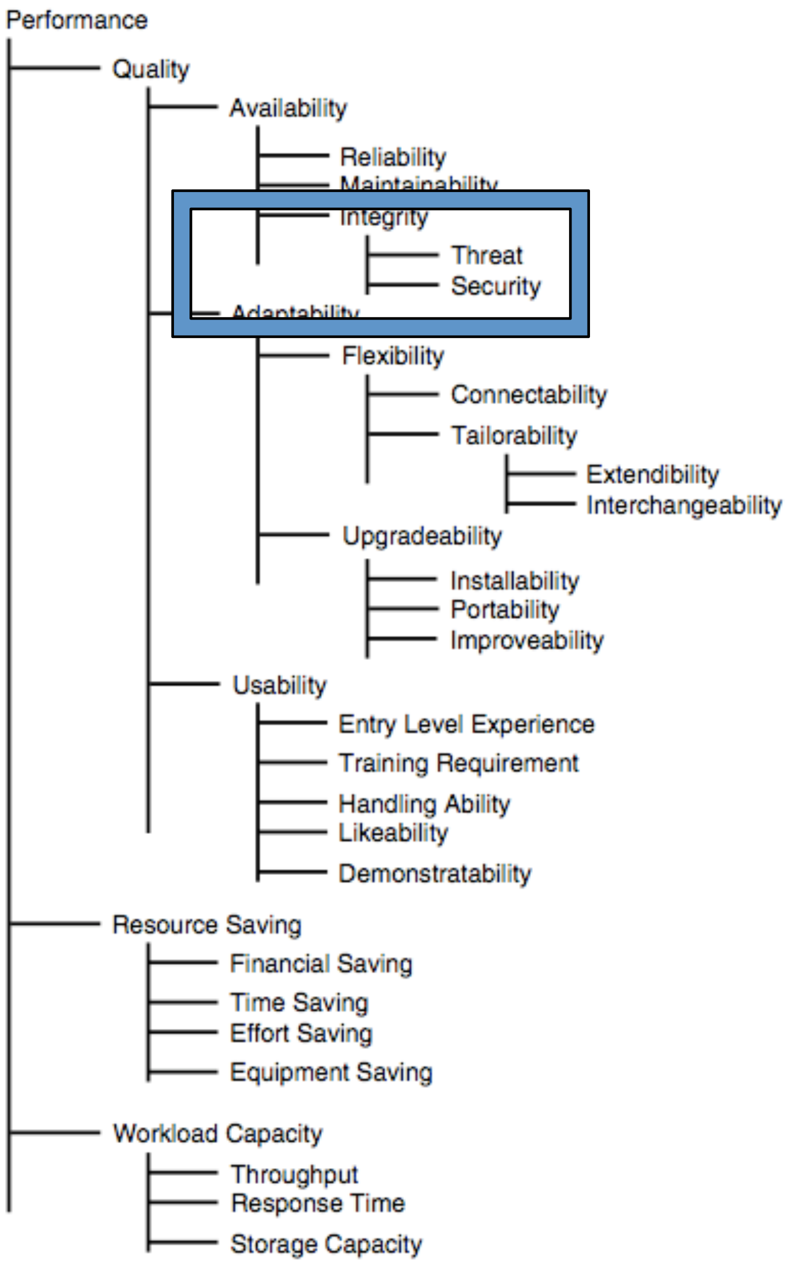
Note: Goal levels are what we think we can really promise and focus on. These types of goals push us into thinking about possible Evolutionary result delivery steps.

Stretch [Deadline = March 2004, Systems = High Criticality Systems] 95%±5%

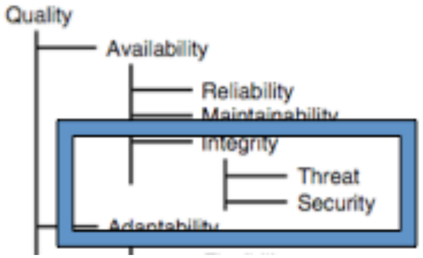
Stretch [Deadline = June 2004, Systems = {Medium & Low} Criticality Systems] 95%±5%

Note: Stretch levels are something that we might be able to achieve if we have sufficient resources, focus and technology available, but we are not sure of that yet. We are NOT promising it now! So this is a way to hold the ideals up in case those things become available.”

Security in Performance Requirements

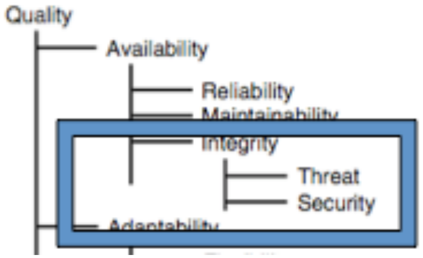


• A generic model of security
(Integrity, Security and Attack)
in the form of a Planguage specification.



- **Integrity**: ‘*The ability of the system to survive attack*’
- **Gist: Integrity is a measure of the confidence that the system has suffered no harm: its security has not been breached and, its use has resulted in no ‘corruption’ or impairment to it.**
- *Note: An attack on the Integrity of a system can be accidental or intentional.*
- *Note: The Integrity of a system depends on the frequency of threat to it and the effectiveness of its security.*
- Type: Elementary Quality Requirement.
- Scale: Probability for a defined [System] to achieve defined [Coping Action] when confronted with a defined [Attack] using defined [Security] measures, under defined [Conditions].
- Coping Action: defined as: {Detect, Prevent, Capture, Thwart, Recover}.
- *Note: here is an example of specifying a requirement using the defined scale above.*
- Goal [System = Our Product, Coping Action = Detect Attack, Attack = In House Amateur Hacker, Security = Microsoft Package, Conditions = Firewall Breached] 99%.

- A generic mode (**Pattern**)l of security (Integrity, Security and Attack) in the form of a Planguage specification.



- **Integrity**: ‘*The ability of the system to survive attack*’
- Gist: Integrity is a measure of the confidence that the system has suffered no harm: its security has not been breached and, its use has resulted in no ‘corruption’ or impairment to it.
- *Note: An attack on the Integrity of a system can be accidental or intentional.*
- *Note: The Integrity of a system depends on the frequency of threat to it and the effectiveness of its security.*
- Type: Elementary Quality Requirement.
- Scale**: Probability for a defined [System] to achieve defined [Coping Action] when confronted with a defined [Attack] using defined [Security] measures, under defined [Conditions].**
- **Coping Action**: defined as: {Detect, Prevent, Capture, Thwart, Recover}.

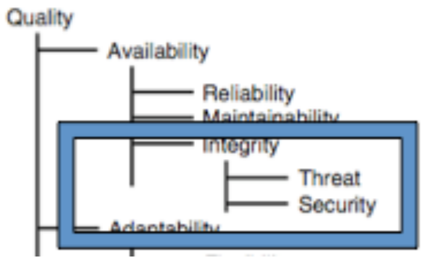
- *Note: here is an example of specifying a requirement using the defined scale above.*
- **Goal** [System = Our Product, Coping Action = Detect Attack, Attack = In House Amateur Hacker, Security = Microsoft Package, Conditions = Firewall Breached] 99%.

The Integrity formula: if you know or assume 2 factors, you can calculate the third!

Integrity =

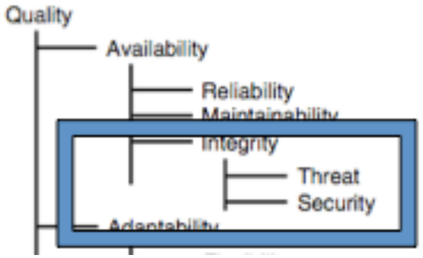
Sum of all instances of [1 - Threat x (1 - Security)].

- Or more simply:



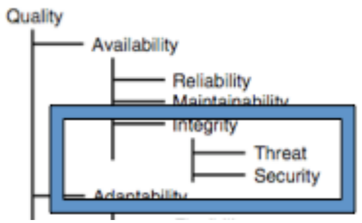
- **The Integrity level of a system**
  - **depends on the degree of threat**
  - **and the security design's ability**
    - **to cope with that class of threat.**

So, for example,



- if planned Integrity is maximum one failure per time period,
  - and there are 100 expected or assumed attacks on the system in a given timeframe,
  - then the effectiveness of the security device must be at least 99%.

Here is an example



Integrity:

Type: Elementary Quality Requirement.

Scale: **Probability for a defined [System] to achieve defined [Coping Action] when confronted with a defined [Attack] using defined [Security] measures, under defined [Conditions].**

Meter: test one or more Security measure designs for all defined Coping Actions, and all defined Attack(s), under all defined Conditions.

Goal [System = Survey Database using Confirmit software,

Coping Action = Detect,

Attack = Professional Top Class Hacker, Security = Complete Security Architecture [Version 1.0],

Conditions = {No Advance Warning, Inside Mainframe Building, All Electronic Specs Available to Hacker}] **50%**

Another example

<u>Security:</u>

Stakeholders: NSM

Scale: % probability the a defined [Assailant] does NOT succeed in a defined [Compromise] for defined [Data] under defined [Conditions].

Meter [for Supplier of Security System payment] Use a professional Norwegian hacker. Give them up to 100 break-in attempts.

Note [Meter] If 1 or more of these is successful, then payment is not due the security suppliers, since the assumption is that it cannot be a better than 99.00% system. If great accuracy is desired increase number of hacks, and make sure they are representative of the best, by using at least 10 per 1000 attempts by professional hackers.

Goal [Assailant = Professional Norwegian Hacker, Compromise = Detailed Knowledge, Data = Norwegian Government Budget, Conditions = Before Secrecy Lifted] 99.90 %

Example: with 'Relationships' background specified

Integrity:

Type: Elementary Quality Requirement.

Scale: Probability for a …. *as above examples in detail*

Goal […. as above examples in detail] 50% <- TG

Source: NASA Security Procedures 2004

Rationale: Deterrence of Professional Hackers

Authority: Congressional Budget for NASA

Issues:

I1: will the guideline level change in this years unpublished budget?

I2: does this impact NASA business outside the USA?

Dependencies

D1: Federal Penalties for Hacking.

Risks

R1: the proposed security technology does not work at the levels estimated

R2: improved hacking paradigms, beyond currently know state of the art.

Various Numeric level Specifications

Integrity:

Type: Elementary Quality Requirement.

Scale: Probability for a …. *as above example in detail*

Meter: test one or …. *as above example in detail*

Benchmarks -------------------------- reference levels

Past [2004, …..] : 15%

Record [Lab Tests]: 99%

Trend [Next Year]: 60% +

Constraints --------------------------- minimum levels

Fail 30%

Survival 20%

Targets ------------------------------ levels to aim at

Wish 80% +

Goal […. as above example in detail] 50%

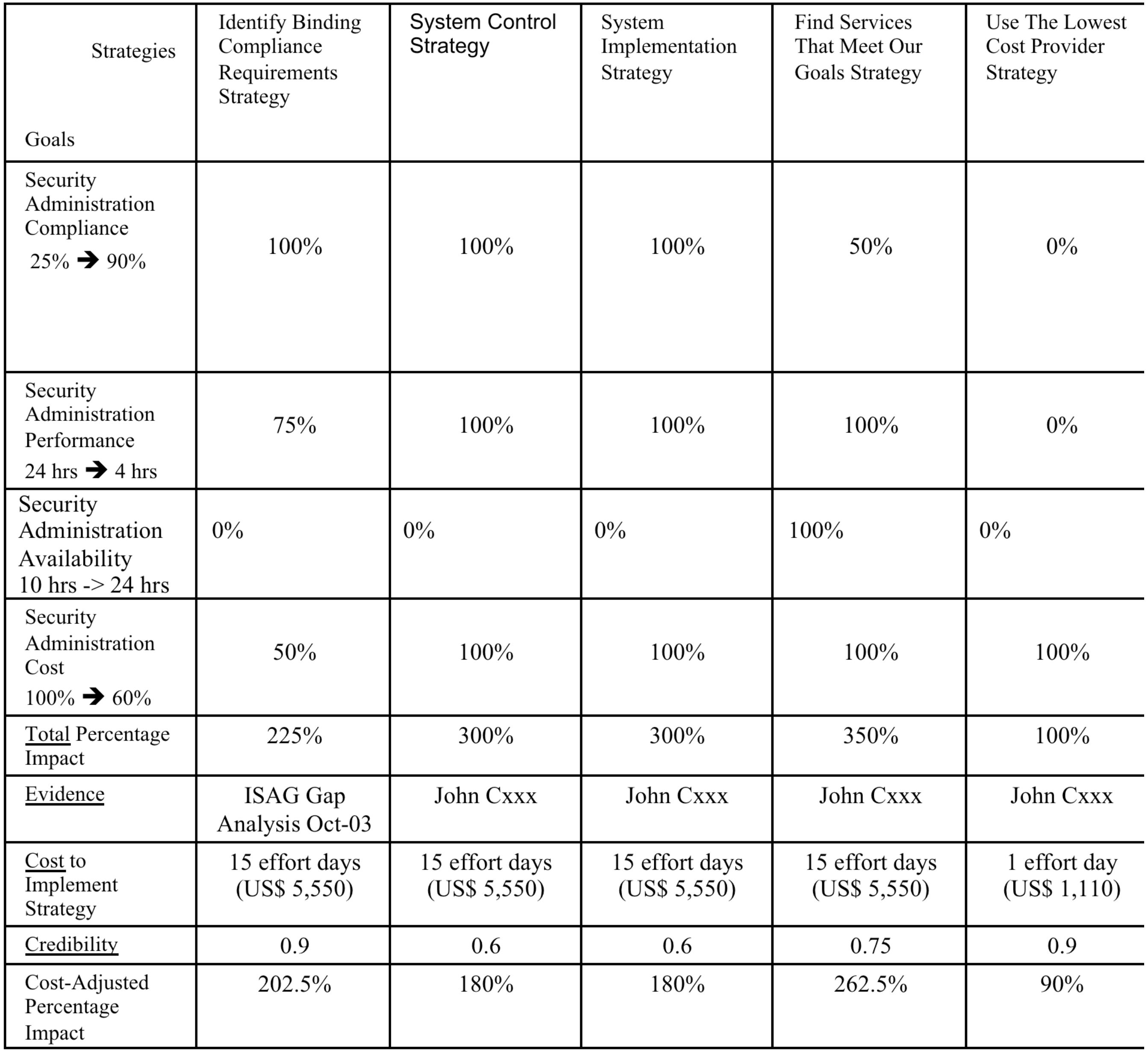
Stretch 55%

Impacts ----(if we reach the Goal level, what happens?)

Primary Impact: Legal Certification

Secondary Impact: Insurance Costs

Impact Estimation Table for Security (Real Example)



Strategies Goals	Identify Binding Compliance Requirements Strategy	System Control Strategy	System Implementation Strategy	Find Services That Meet Our Goals Strategy	Use The Lowest Cost Provider Strategy
Security Administration Compliance 25% → 90%	100%	100%	100%	50%	0%
Security Administration Performance 24 hrs → 4 hrs	75%	100%	100%	100%	0%
Security Administration Availability 10 hrs -> 24 hrs	0%	0%	0%	100%	0%
Security Administration Cost 100% → 60%	50%	100%	100%	100%	100%
Total Percentage Impact	225%	300%	300%	350%	100%
Evidence	ISAG Gap Analysis Oct-03	John Cxxx	John Cxxx	John Cxxx	John Cxxx
Cost to Implement Strategy	15 effort days (US$ 5,550)	15 effort days (US$ 5,550)	15 effort days (US$ 5,550)	15 effort days (US$ 5,550)	1 effort day (US$ 1,110)
Credibility	0.9	0.6	0.6	0.75	0.9
Cost-Adjusted Percentage Impact	202.5%	180%	180%	262.5%	90%

Love Attributes:
Brainstormed By Dutch Engineers

- Kissed-ness
- Care
- Sharing
- Respect
- Comfort
- Friendship
- Sex
- Understanding
- **Trust**

- Support
- Attention
- Passion
- Satisfaction
- …
- …
- …

Trust [Caroline]

- **Love.Trust.Truthfulness**

  Ambition: No lies.

  Scale:

  Average **Black** lies/month from [defined sources].

  Meter:

  independent confidential log from sample of the defined sources.

  Past Lie Level:

  Past [My Old Mate, 2004] 42 <-Bart

  Goal

  [My Current Mate, Year = 2005] Past Lie Level/2

  Black: Defined: Non White Lies

- Other aspects of Trust:
  - **Broken Agreements**
  - **Late Appointments**
  - **Late delivery**
  - **Gossiping to Others**

Camaraderie (Real Case UK)

- Ambition: to maintain an exceptionally high sense of good personal feelings and co-operation amongst all staff: family atmosphere, corporate patriotism. In spite of business change and pressures.
- Scale: probability that individuals enjoy the working atmosphere so much that they would not move to another company for less than 50% pay rise.
- Meter: Apparently real offer via CD-S
- Past [September 2001] 60+ % <- R & CD
- Goal [Mid 2002] 10%, [End 2002] <1% <- R & CD
- Rationale:
- maintain staff number, and morale as core of business and business predictability for customers.

Love: Biblical Dimensions < L Day, Boeing

The biblical citation (Book of First Corinthians) I included gives the quantification of the term "love" (agape in Greek). The 'quantification' for love would be as follows:

------------>

A person who loves acts the following way toward the person being loved:

1. suffereth long

2. is kind

3. envieth not

4. vaunteth not itself, vaunteth...:
or, is not rash (Vaunt = extravagant self praise)

5. is not puffed up

6. Doth not behave itself unseemly

7. seeketh not her own

8. is not easily provoked

9. thinketh no evil

10. Rejoiceth not in iniquity (=an unjust act)

11. rejoiceth in the truth

12. Beareth all things

13. believeth all things

14. hopeth all things

15. endureth all things

16. never faileth

Last Slide!

- Questions?
- These slides are at www.Gilb.com
- As is a paper on “Quantifying Security”
- And on
- “Quantifying Quality”