Bilgi Teknolojileri Yönetişim ve Denetim Konferansı

BTYD 2010

ISACA Serving IT Governance Professionals

Türkiye Bilişim Derneği 1971

Türkiye İç Denetim Enstitüsü 1995

eDem TODAİE eDevlet Merkezi

GRC "ISACA STYLE": DEFINITIONS, TOOLS & METHODOLOGIES

Kaya Kazmirci
Internal Audit Director, Avea
President ISACA Istanbul Chapter
kaya.kazmirci@isaca-istanbul.org
kaya.kazmirci@avea.com.tr
+90-555-255-8090
+90-532-487-7756

Our World Is Changing Dramatically...

Moore's Law: The amount of processing power available for a specific price doubles every 18 months

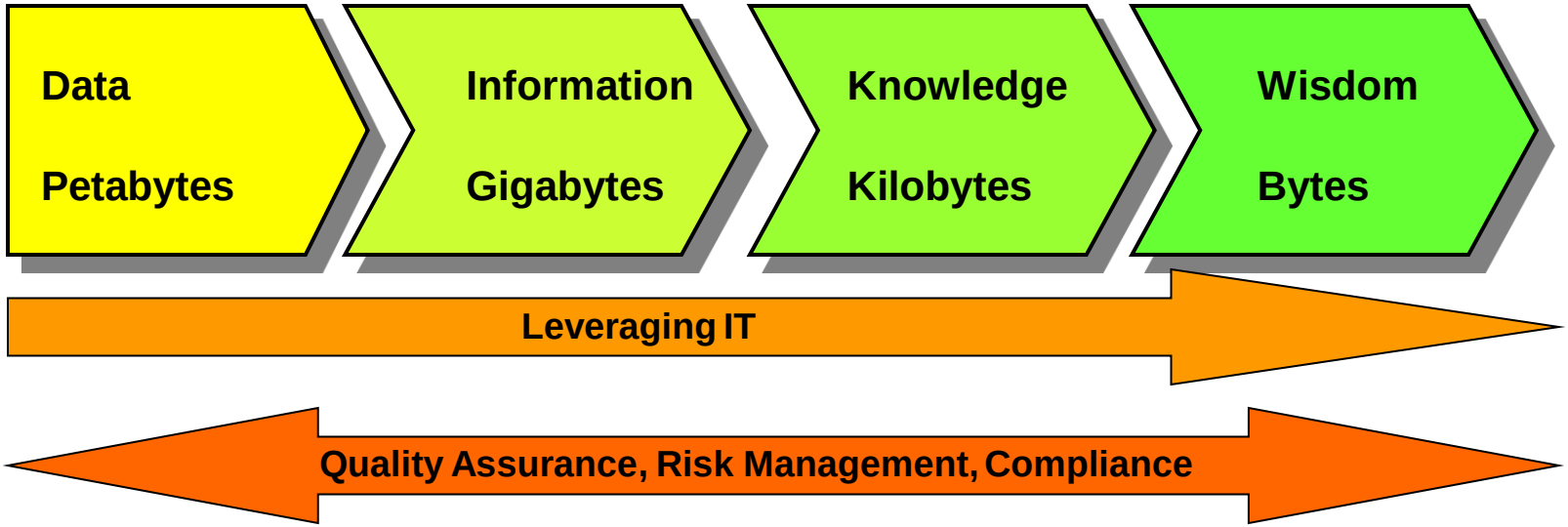
25 Billion: eTransactions completed today
50 Billion: eTransactions per day in 2014
(Economist)

1.5x : 54% Annual storage shipments growth (IBM)
"More storage will be shipped in the coming 2 years than shipped in the previous 20 years" (IDC)

60%: Part of SW TCO spent on maintanance circa 1984 (Dartmouth College)
70%: SW Maintenance TCO % today (IBM)

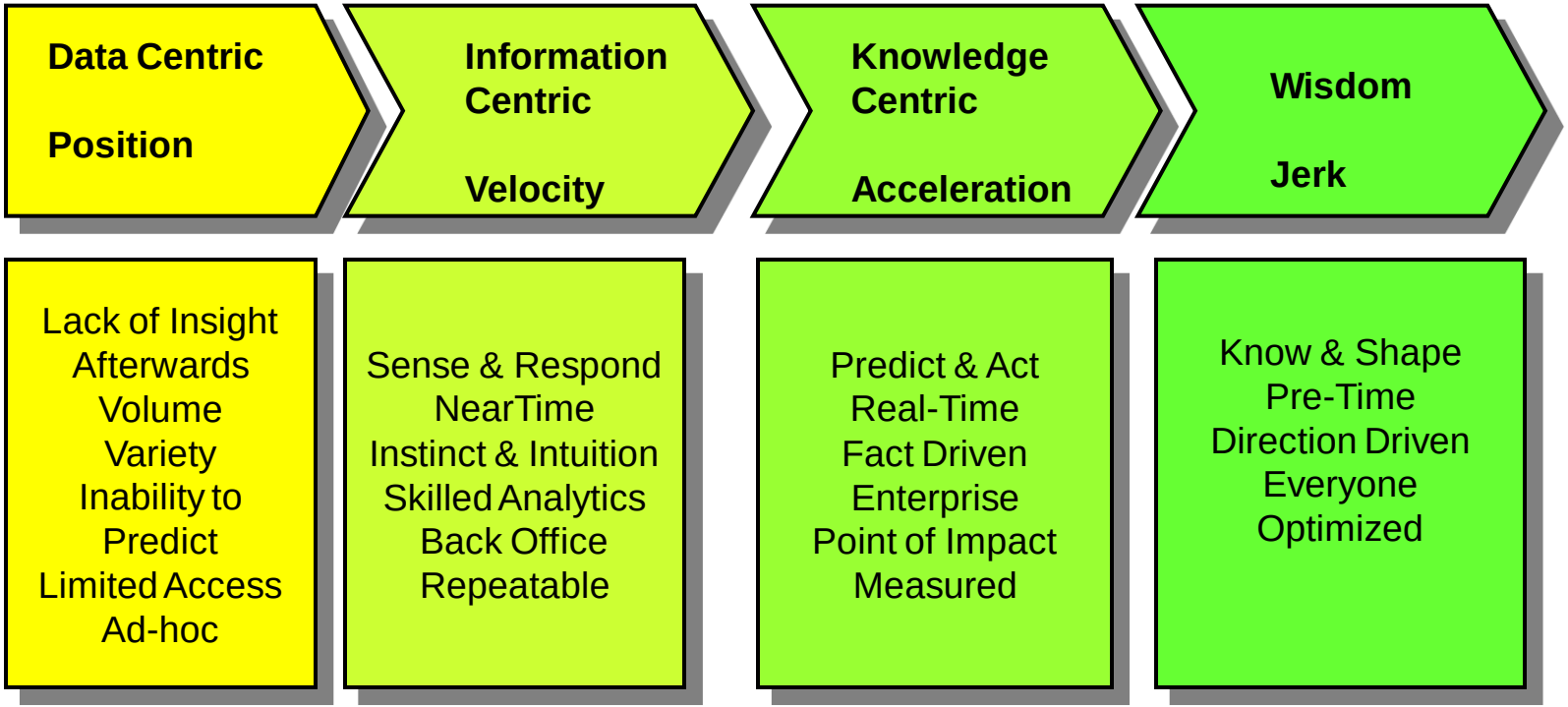
30%: Medical Imaging share of Global Storage used (IBM)

We must evolve our thinking...

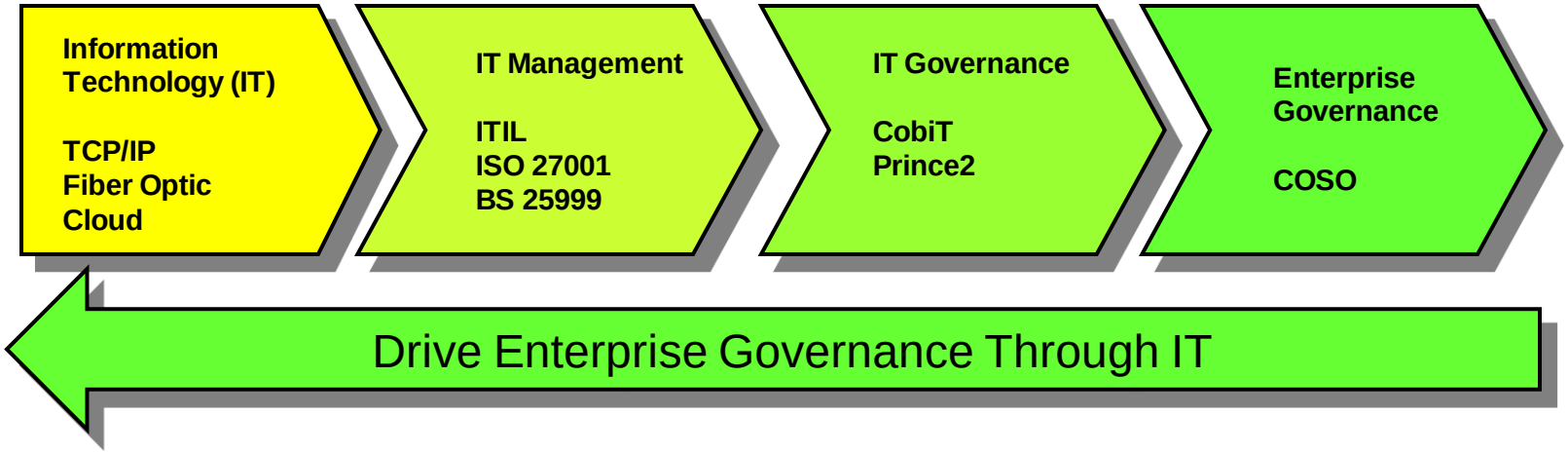


So we can sift the nuggets from the sand...

… And focus on what matters

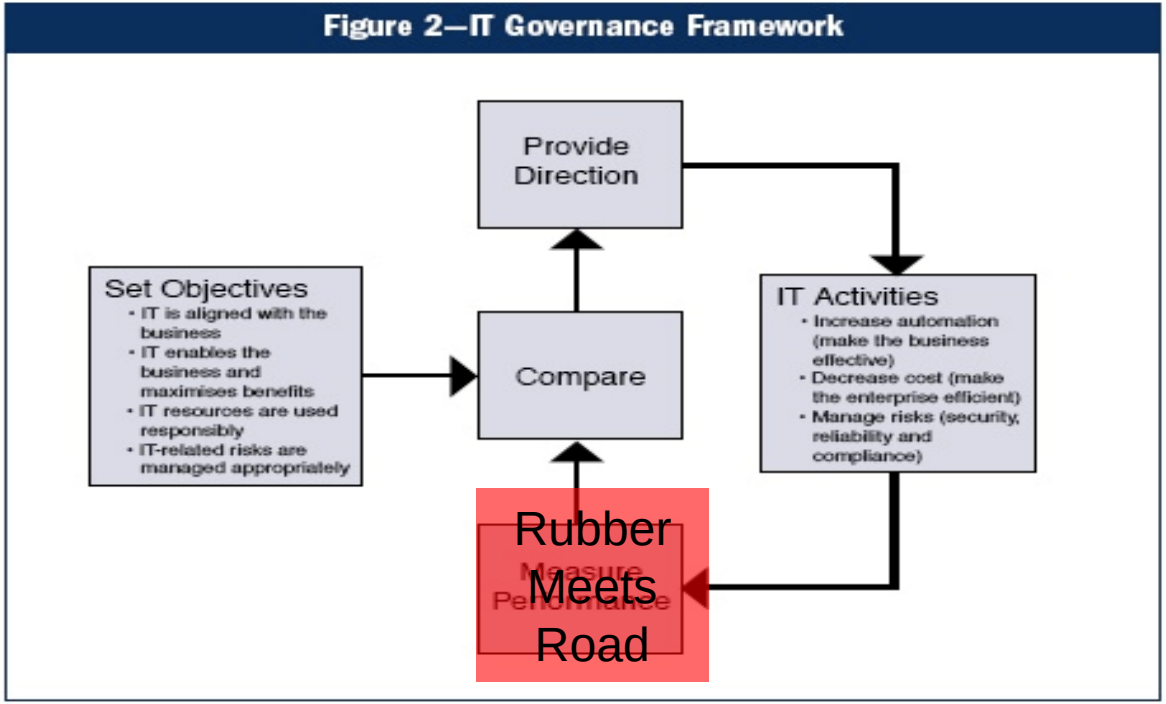


Our Approach Must Change



How do/should we measure IT's contribution?
What does IT spending contribute to the bottom line?
What is ROI for each IT project?
What is/should our Architecture be?
How effective/efficient is our change management?
How quickly can we respond to/predict our business products/demand?

Some Definitions: IT Governance...



"*… the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.*" ITGI

IT Risk

The chance that information systems will not satisfy the *business requirement* of ensuring the achievement of *IT objectives* and responding to *threats* to the provision of IT services

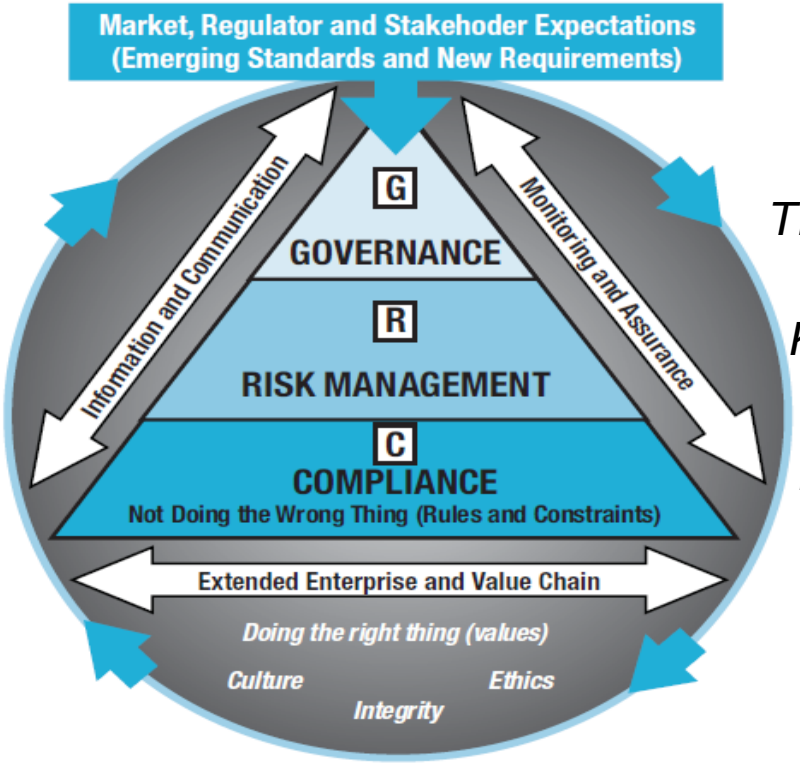
What can be lost

Compliance

"What we should be doing, but are challenged by, and told to do"

Optimised	Include regulatory stakeholders in Enterprise governance creating an integrated seamless structure of Government, Enterprise, & related Stakeholder interest
Managed	Implement first then "Suggest" improvements to the "powers that be"
Defined	Continuously follow market practice, benchmarks & new developments
Repeatable	Adopt regulations or standards that are maturity-driven & designed for continuous improvement over time.
Initial	Work through a list of all-or-nothing requirements

How Do They Fit Together?



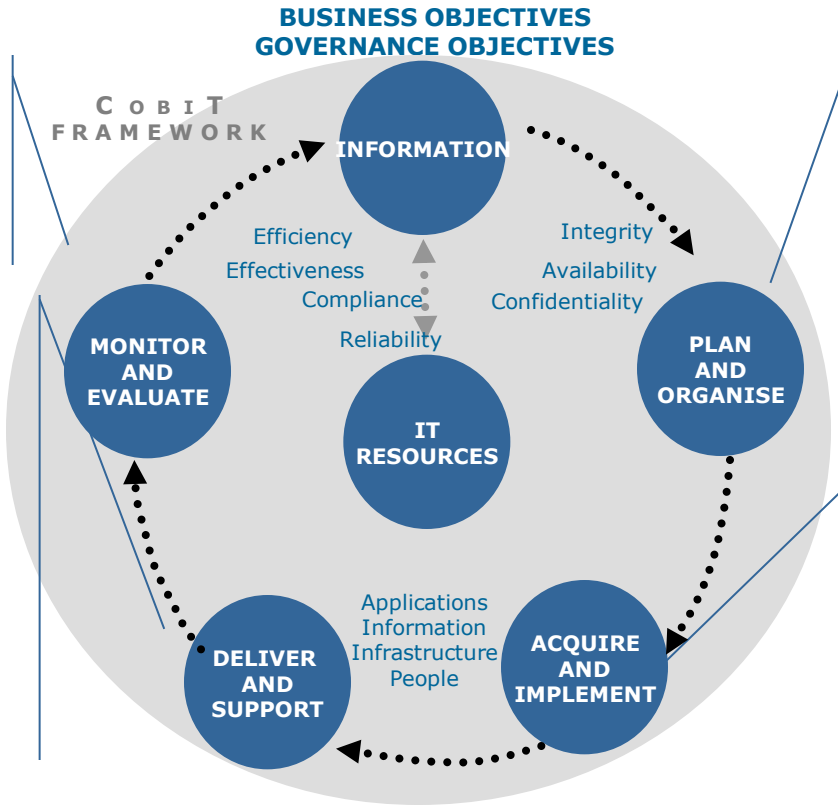
The management of management

Keeping track of what we can loose

Not doing the wrong thing

BT

CobiT: An Approach To IT Governance



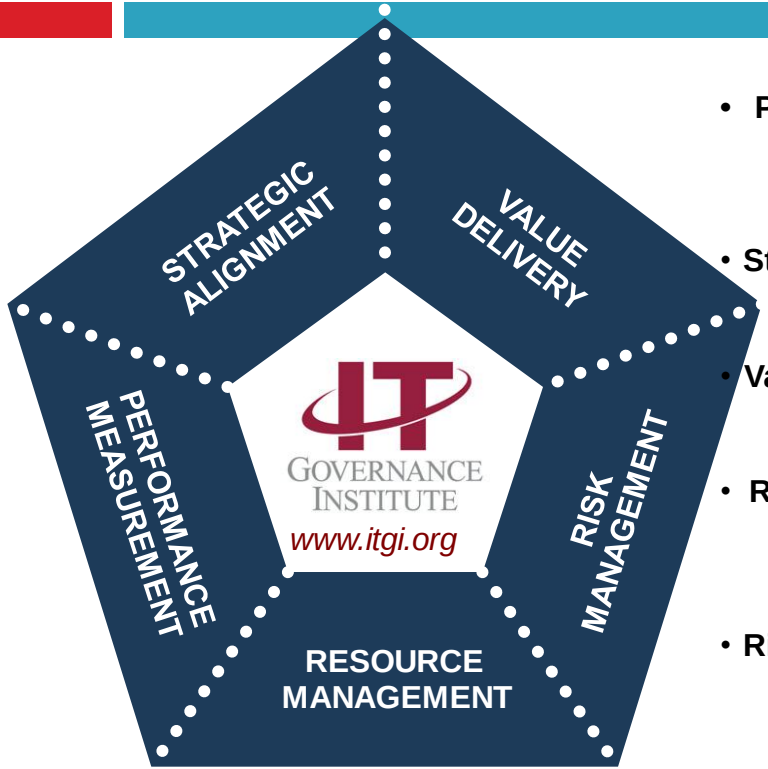
ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure regulatory compliance.
ME4 Provide IT governance.

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and change.

IT Governance Focus Areas

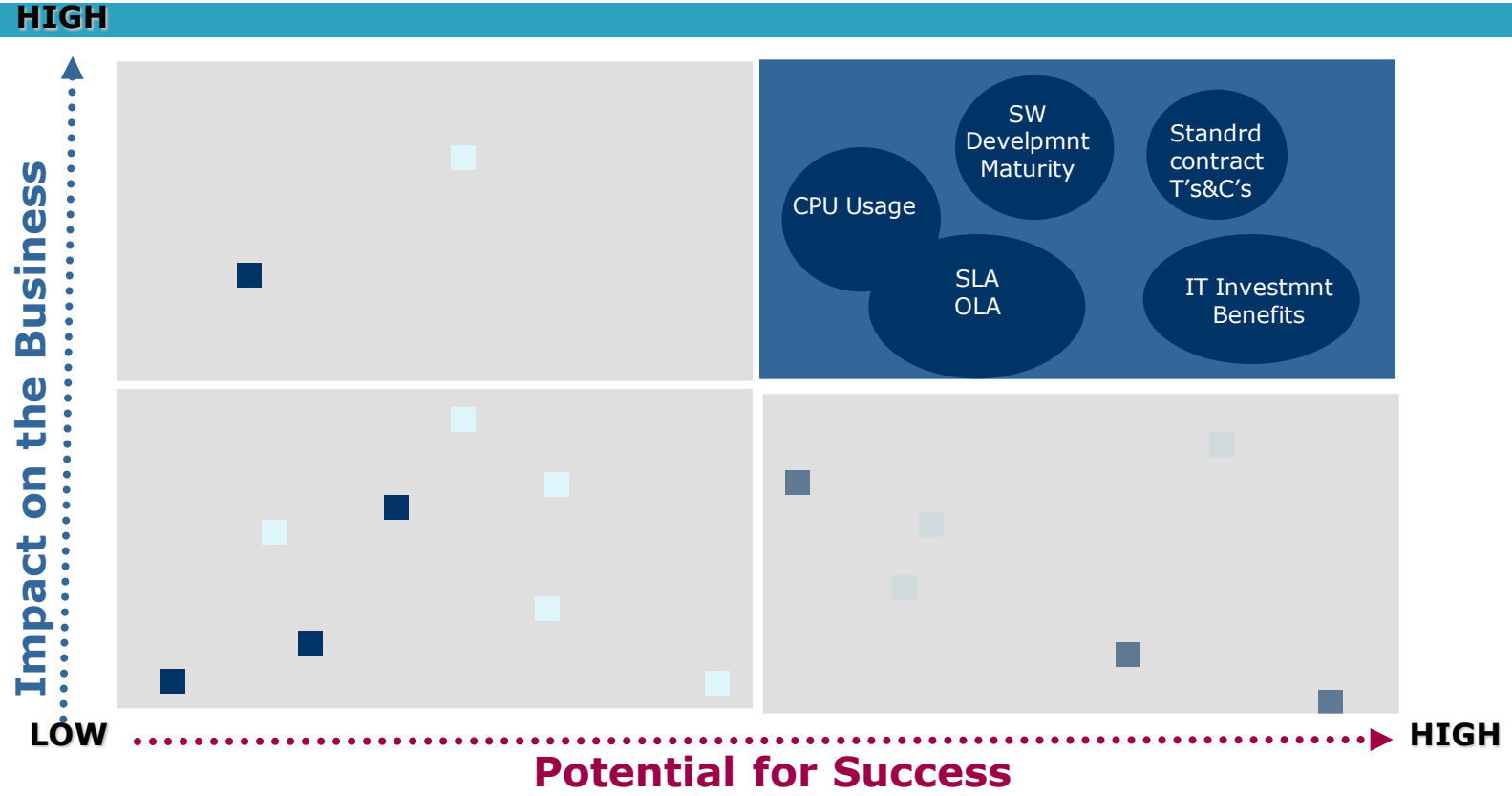


- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting
- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation.

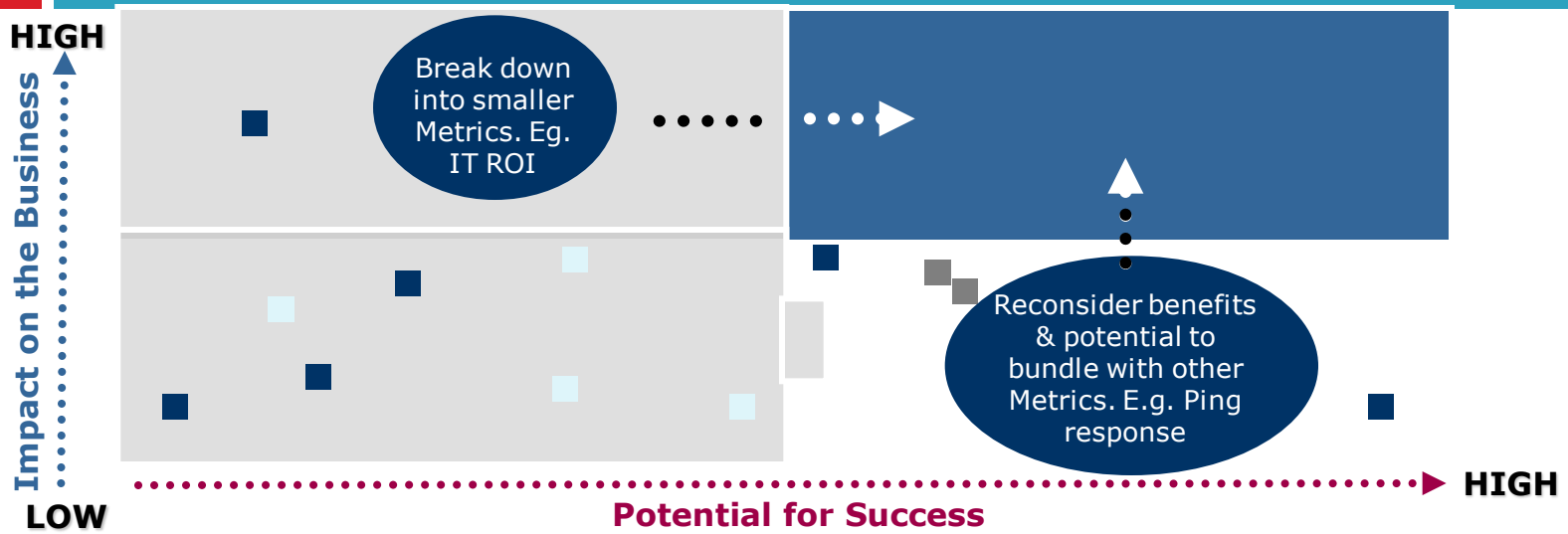
Metrics Selection

- You can only manage what you measure (Gary Hardy)
- Pick fewer rather than more metrics to implement & report
- KISS (Keep it simple & stupid) i.e. CXO's & Call Center operators should understand it
- Be careful with derivatives v single metrics
- Select metrics that reflect your focus areas

“Implementing Metrics” Opportunity Grid



Redoing “Hard-to-justify” Metrics

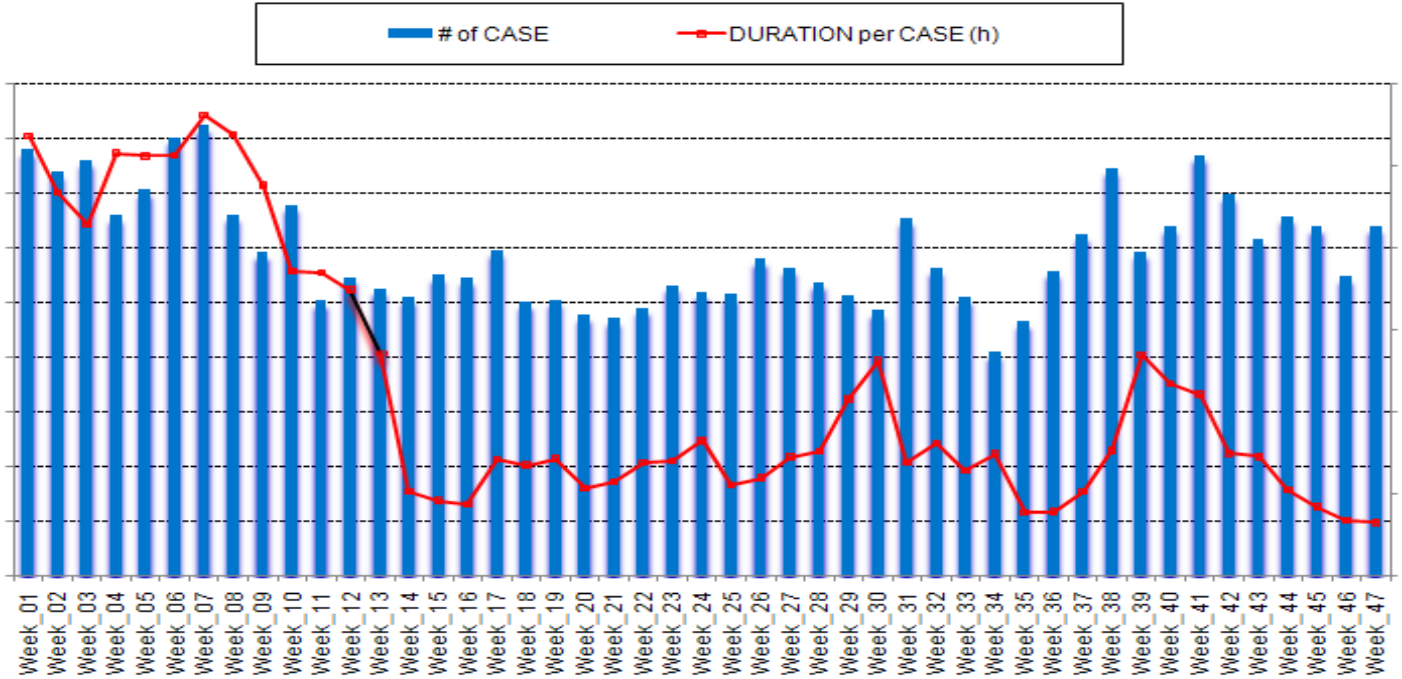


- Ensure that everyone (business too) understands & accepts them
- Automated measures prefered to manual ones
- Use cheap/integrated/existing tools to measure (e.g. MS, UNIX, ping, tracert, MRTG)
- Ensure that the tools are subject to change management
- Ensure that measurer & measuree are segregated

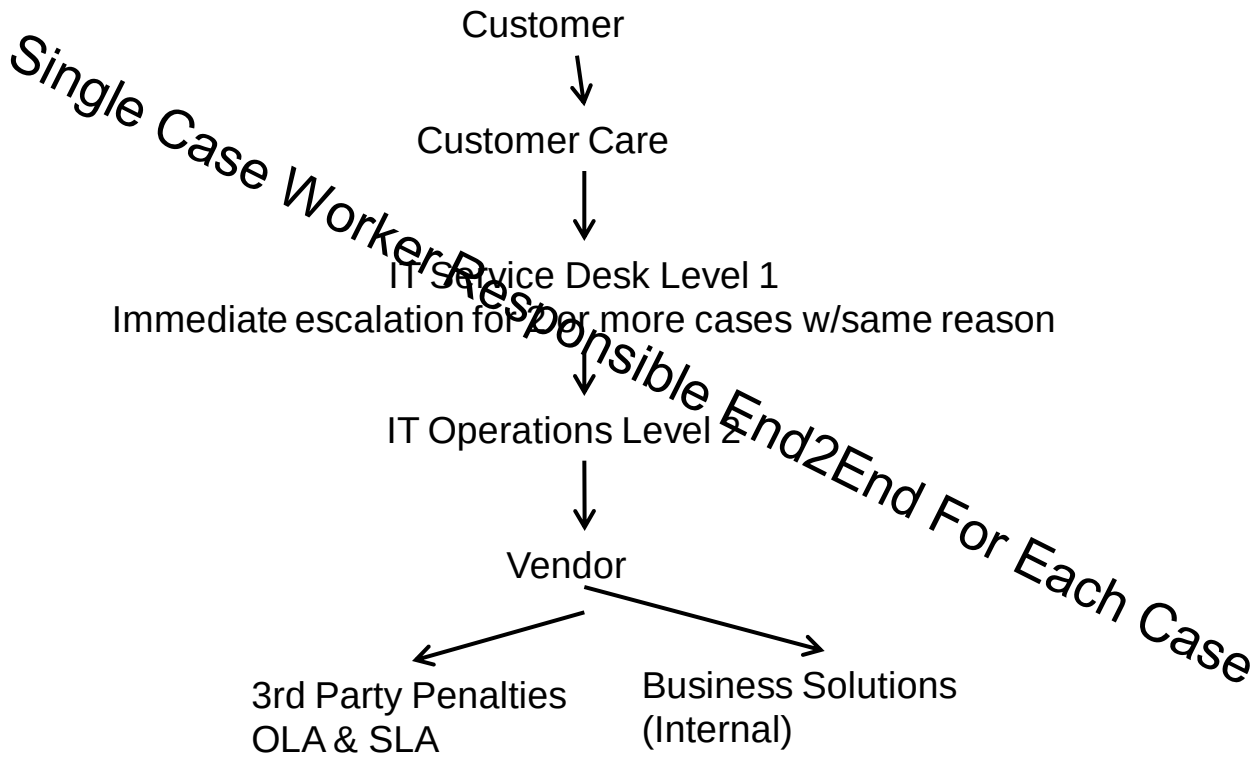
Case Study In Customer Service

- Avea introduced a “One price-unlimited calling” based product (Her Yöne Özgürlük)
- Market responded very well
- Demand exploded
- We had some issues to sort out
- How did we succeed?

Avea IT Service Desk Performance 2009



Implement Strong Case Managment



OLA's Implemented, Measured & Enforced

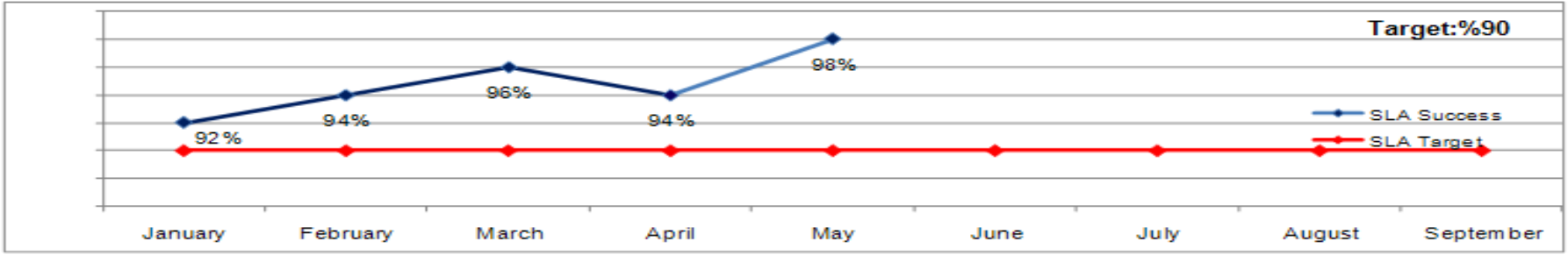
OLA

L1 (IT SERVICEDESK)	L2 (ALL SECOND)
2/3 Y hr.	1/3 Y hr.

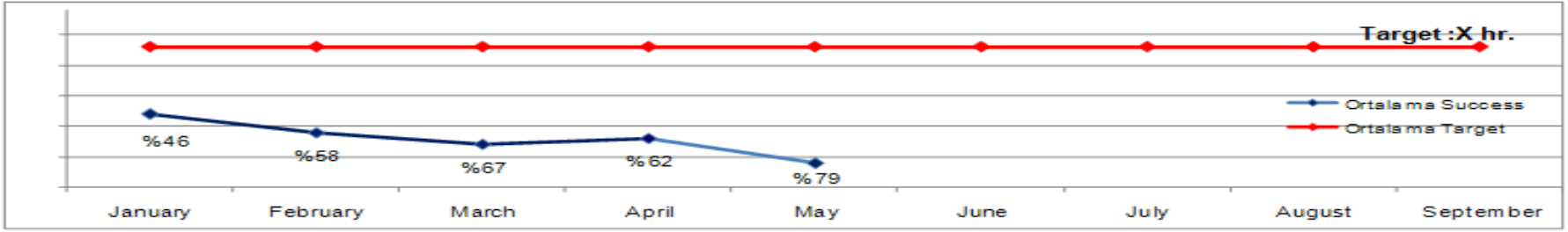
L1 2/3 Y Hrs → All Customer Care submitted L1 Cases are to be closed in target time. Clock starts the next day for Cases submitted after COB
L2 1/3 Y Hrs →L2 Cases closed in target time 24x7

Implement SLA's (2010)

SLA1: 90% of Cases to be closed in Y target time (hrs)



SLA2: Average Case Close less than target (hrs)



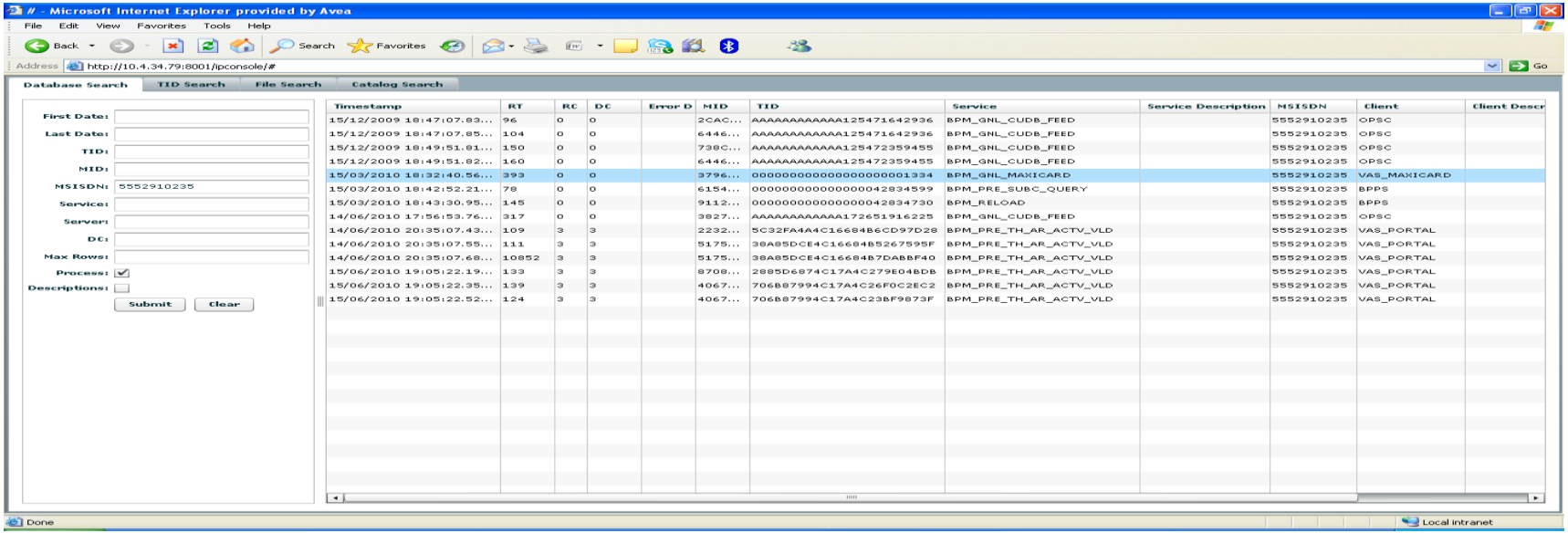
How Did We Support Our Case Workers?

With Some Tools That We Developed .....

P.S. Don’t try this kind of sw development at home

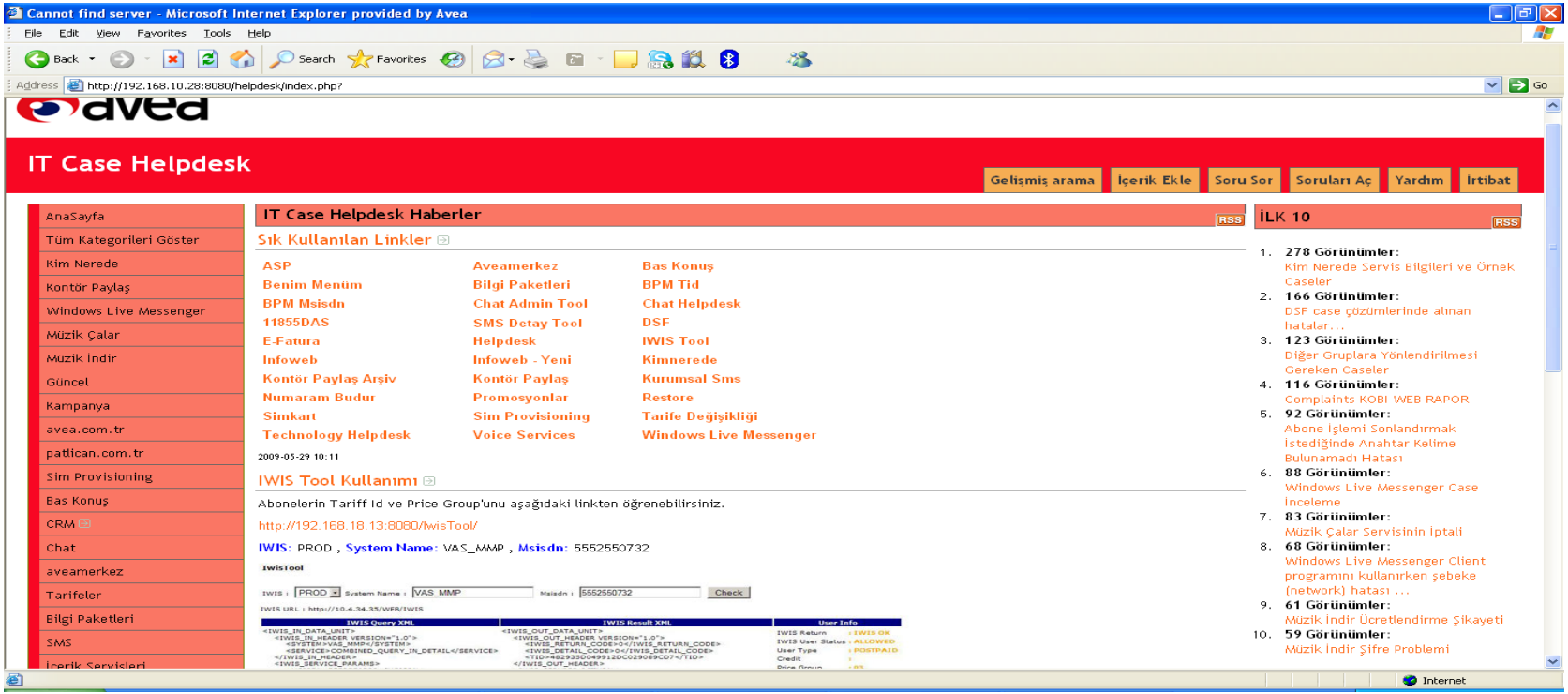
We have hundreds of sw developers on call to support us

What Services Has Our Customer Used?

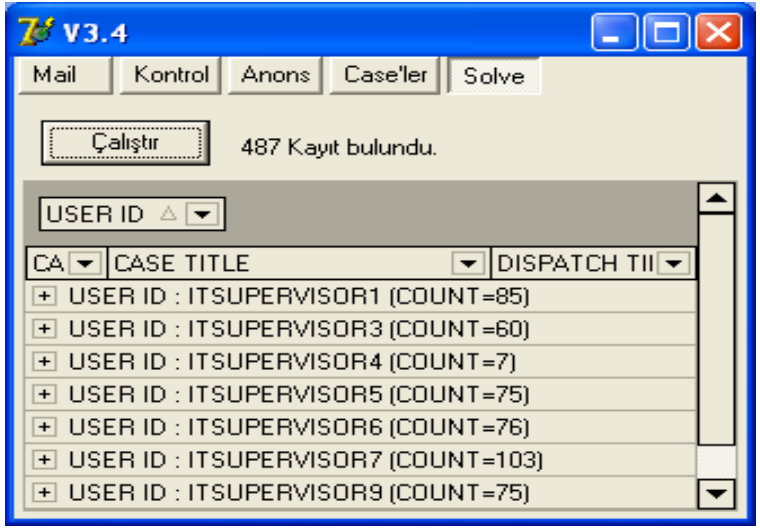


Customers (bless'em) don't always remember all of the details of their use

KM DB Tool Allows Fix Collection & Reuse



Case Workers Productivity Display Tool



Case workers get daily feedback about their performance
Guess what happened/s to consistently low performers?

What Else Did We Do?

- Prioritize older cases or multiple cases with the same reason
- Trained Case Workers on EVERYTHING they requested
  - Mostly products
  - Infrastructure
  - Technology
- Weekly coordination meetings with representation from ALL Solution Groups
  - Standard Agenda including
    - All Open L2 Cases
    - All Open Multiple Cases with the same reason
    - Root cause analysis for above
    - Fixes implemented
- Monthly reporting to CTO
- Encourage/reward proactive solutions

DS1 Define & Manage Service Levels

Started Here

1 Initial/Ad Hoc when There is awareness of the need to manage service levels, but the process is informal & reactive. The responsibility & accountability for defining & managing services are not defined. If performance measurements exist, they are qualitative only w/ imprecisely defined goals. Reporting is informal, infrequent & inconsistent.

2 Repeatable but Intuitive when There are agreed-upon service levels, but the [illegible]ormal & not reviewed. Service level reporting is incomplete & may be irrelevant or misleading for customers. Service level reporting is depend[illegible]e skills & initiative of individual managers. A service level co-ordinator is appointed w/defined responsibilities, but limited authority. If a process [illegible]pliance to SLAs exists, it is voluntary & not enforced.

3 Defined when Responsibilities are well defined, but w/discretionary authority[illegible]LA development process is in place w/checkpoints for reassessing service levels & customer satisfaction. Services & service levels are [illegible]mented & agreed-upon using a standard process. Service level shortfalls are identified, but procedures on how to resolve shortfalls are [illegible]here is a clear linkage between expected service level achievement & the funding provided. Service levels are agreed to, but they may not add[illegible] business needs.

4 Managed & Measurable when Service levels are increasingly defined in the system requirements definition phase & incorporated into the design of the application & operational environments. Customer satisfaction is routinely measured & assessed. Performance measures reflect customer needs, rather than IT goals. The measures for assessing service levels are becoming standardised & reflect industry norms. The criteria for defining service levels are based on business criticality & include availability, reliability, performance, growth capacity, user support, continuity planning & security considerations. Root cause analysis is routinely performed when service levels are not met. The reporting process for monitoring service levels is becoming increasingly automated. Operational & financial risks associated w/not meeting agreed-upon service levels are defined & clearly understood. A formal system of measurement is instituted & maintained.

Ended Here

5 Optimised when Service levels are continuously re-evaluated to ensure alignment of IT & business objectives, whilst taking advantage of technology, including the cost-benefit ratio. All service level management processes are subject to continuous improvement. Customer satisfaction levels are continuously monitored & managed. Expected service levels reflect strategic goals of business units & are evaluated against industry norms. IT management has the resources & accountability needed to meet service level targets, & compensation is structured to provide incentives for meeting these targets. Senior management monitors performance metrics as part of a continuous improvement process.

Teşekkür Ederim!

- İzzet Gökhan Özbilgin & ISACA Ankara Chapter In Formation
- Gary Hardy, Rolf von Roessing and the CobiTeers (aka CSC)
- Metin Yılmaz, Çoşkun Şahin, Okan Cengaver, Füsun Feridun, Aslı Barış Seyis, Nurcan Önder and Alper Arpacıoğlu (Avea)
- Eda Alp and Defne Eroğul (IBM)

BTYD 2010

www.btyd.org