I.T. – the risk at the heart of your business

Chartered Quality Institute (Bristol)

I.T. systems – doing a better job

Colin Butcher CEng FBCS CITP
Technical director, XDelta Limited
www.xdelta.co.uk

xdelta

Personal background

- Systems architect specialising in mission critical systems
- Engineering background (printing, power generation)
- Wide range of experience (aerospace, healthcare, finance, transport, power and energy)
- Strong interest in mentoring and teaching

xdelta

XDelta – what we do

- Lead mission-critical systems projects:
  - Strategic planning
  - Technical leadership
  - Project direction
- Minimise risk of disruption to business:
  - Design for change while in continuous operation
  - Prepare in advance for ease of transition
- Ensure long term success through skills transfer

xdelta

The “elephant in the room”

We are all now utterly reliant on computer systems and digital communications. I.T. has become pervasive. Regrettably few people understand it very well. Too many I.T. projects fail.

Most of what we deliver has no physical reality. Those involved need excellent conceptual skills and the ability to communicate ideas clearly. It requires outstanding thinkers and leaders.

Most projects start to go wrong through mis-match of expectations and lack of detailed understanding. Poor planning, unreasonably tight timescales and inadequate budgets make things worse.

Somehow we have to do a better job. Part of that is quality.

xdelta

Agenda

- Warning – this is a quick look at a huge subject !

- The problem with I.T.
- The need for quality
- I.T. systems structure and terminology
- Security, availability and performance
- I.T. systems lifecycle
- Leadership and people
- Summary

xdelta

Some of the problems with I.T.

- Everything is conceptual – no physical reality
- It's not yet an engineering discipline – "art & craft"
- Many layers of abstraction – complex and confusing
- Often poorly documented and explained – hard to control
- Rapid pace of change – hard to be consistent over time
- People and communication – difficult to get clarity

xdelta

The “wild west”

- The computer industry isn’t very interested in keeping old stuff working – it wants to sell new stuff
- The industry is largely in the hands of the resellers
- Very little regulation or legislation
- Very little in-depth understanding and available information
- Many decisions end up being based on cost, not capability

The need for quality – a tool to help

- Enforce standards
- Catch mistakes early
- Review design and implementation decisions
- Improve consistency
- Keep track of change
- Demonstrate thorough and appropriate testing

xdelta

I.T. systems – terminology – structure

- Data centre – provides power, cooling, physical security etc.
- Infrastructure – data network (LAN), storage network (SAN)
- System platform – hardware, operating systems
- Database – logical structure of data, the “filing system”
- Application software – “business logic”, “user interface”

xdelta

I.T. systems – terminology – connectivity

- Private inter-site links - WAN (Wide Area Network)
- Security – firewalls (filter traffic), DMZ (De-Militarised Zone)
- End to end encryption - SSL, IPsec (Secure Socket Layer, Internet Protocol security)
- Inter-site links over Internet - VPN (Virtual Private Network)
- Remote access – VPN (“dialup”)

I.T. systems – terminology – virtualisation

- Hosts – physical machines, lots of memory and cores
- Hypervisor (eg: VMware, Hyper-V, KVM)
- Virtual machines, virtual servers, virtual desktops
- Good for improved availability, not so good for performance
- More abstraction layers, increased complexity

xdelta

I.T. systems – terminology – cloud

- A “management wrapper” around virtual systems
- Automates the deployment of resources and charging:
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Software as a service (SaaS)
- What level of performance do you get ?
- Where is your data and whose jurisdiction applies ?

xdelta

Mission-critical systems

- All systems are mission-critical in one way or another
- Systems that are relied on to get something done, without data loss or corruption and without disruption
- Some kind of severe penalty for systems failure, be it financial, or legal, or business-threatening, or life-threatening
- Most businesses are now 24x7x365, like it or not. Need a 24x7 infrastructure, not a 12x5 infrastructure.
- Most systems are interconnected – security is vital

xdelta

Mission-critical systems – terminology

- Availability:
  - Probability of system being available for use when needed
- Disaster tolerance (DT):
  - Surviving major site outages without loss of service
- High availability (HA):
  - No single points of failure (SPoF)
- Disaster recovery (DR):
  - Restarting operations, typically from another location (DR site)
- Data replication – synchronous or asynchronous

xdelta

Mission-critical systems – characteristics

- Systems must:
  - Survive failures (resilience and failover)
  - Survive changes (adapt and evolve)
  - Survive people (simplify and automate)
  - Never corrupt or lose critical data (data integrity and security)
- What is the “operational window” ?
- Safety-critical systems also have to be “fail-safe”
- Real-time systems also have precise performance targets

xdelta

Survivability – how long have you got ?

	Planned (Maintenance)	Unplanned (Failure)
Human error	?	?
Data loss / corruption	?	?
System platform	?	?
Infrastructure	?	?
Application Software	?	?
Security breaches	?	?
Performance problems	?	?

xdelta

System failures – how are you affected ?

- How would you like it to fail ?
- How do you cater for failures ?
- What level of outage is acceptable ?
- What level of data loss is acceptable ?
- How do you set expectations of what's possible ?

The closer you get to 100% uptime the harder and more expensive it is.

xdelta

Availability – some major issues

- Who takes responsibility when it fails ?
- How can you demonstrate that you did what you could to avoid failure ?
- How can you demonstrate that you did what you could to limit the damage and scope of failure ?
- How do you cope with changing software and changing requirements ?
- What regulatory frameworks and legislation apply ?
- Cannot just “bolt on” availability later

xdelta

Stages in the life and death of a system

- Requirements
- Design
- Implementation
- Test
- Regulatory approval
- Transition into service
- Operation, support and change management
- End-of-life and transition out of service

It is by no means a smooth and linear progression from stage to stage.

xdelta

Requirements – it all starts here

- Clarity is essential
- Do not over-specify !
- Understand the problems you're trying to solve:
  - Usability – how will people interact with it ?
  - Security – data at rest, data in transit
  - Performance – responsiveness, throughput
  - Manageability – alerting, monitoring, logging
- Minimise complexity
- What are the acceptance criteria ?

Be prepared to reconsider if you don't like the price or the timescales.
Know what compromises you can safely make.

xdelta

Availability, security and performance

- Availability is the underlying concern
- Security breaches make a system or its data unavailable
- Performance related failures make a system unavailable or fail to meet a specific deadline
- System outages will affect your reputation
- Data theft or corruption can destroy your business

xdelta

What is I.T. security ?

- It’s making sure that someone else doesn’t:
  - Steal or destroy your intellectual property
  - Get access to your data or systems
  - Get access to your clients data or systems
  - Stop you getting access to your data or systems
- What are the potential consequences ?
  - Damage to reputation
  - Disruption to your business
  - Disruption to your clients businesses
- How would you know if you’d been compromised ?

xdelta

I.T. security – where are the problems ?

- People:
  - They lose things
  - They forget to do things
  - They expect things to be quick and easy
- Technology:
  - It’s complex
  - The language is arcane
  - It’s immature and evolving rapidly
- We need:
  - Protection against carelessness
  - Protection against malicious attackers

xdelta

I.T. security – some major issues

- Who takes responsibility for your security ?
- What regulatory frameworks and legislation apply ?
- How can you recover from data loss or theft ?
- Protection of information “at rest”
- Protection of information “in transit”
- Protection from external attacks
- Intrusion detection

xdelta

I.T. security – key areas

- Authentication – are you who you say you are ?
- Access control – what are you allowed to look at / change ?
- Encryption – protecting information “at rest” and “in transit”
- Beware insiders – those you trust most can do the most damage to you
- Consider the combination of disparate pieces of available information together with the opportunity and time for someone else to exploit them

xdelta

Performance – what is “fast” and “slow” ?

- Bandwidth – determines throughput
  - It’s not just “speed”, it’s “units of stuff per second”
- Latency – determines response time
  - Determines how much data is in transit
  - “data in transit” is at risk if there is a failure
- Jitter - determines predictability of response, or “diff latency” (variation of latency with respect to time)
  - Important for establishing timeout values
  - Latency fluctuations will cause system failures under peak load
- Can’t make it go faster, we can stop it going slower

xdelta

Capacity, scalability and parallelism

- What happens as the system grows over time ?
- Understand how your workload could break down into parallel streams of execution
- Contention and saturation – running out of capacity
- Increasing the capacity of the overall system:
  - “Scale up” or “vertical scaling” – adding resources to a machine or buying a bigger machine (CPU count, memory, I/O adapters, etc.)
  - “Scale out” or “horizontal scaling” - adding more machines

xdelta

Performance – some major issues

- Who takes responsibility for meeting performance requirements ?
- How can you demonstrate that you meet them ?
- How do you cope with changing software and changing requirements ?
- What regulatory frameworks and legislation apply ?
- Cannot just “bolt on” performance later
- Newer hardware may make things worse

xdelta

Testing

- Understand the requirements and acceptance criteria
- How do we generate a typical workload ?
- How do we generate representative data sets ?

- Test under normal, failure and recovery conditions
- Don’t just confirm that the system behaves as expected
- Must test for scalability as well as functionality

- Change control and regression testing over the lifetime of the system
- Where will you test it before it goes into production ?

xdelta

Transition into service / out of service

- Migrate user community with minimal disruption
- Minimise risk of data loss
- Minimise risk of loss of service
- Migrate live data + historic data
- Migrate connectivity, eg: data centre move

- How can we split transition into manageable steps ?
- Is anything a one-way step ?
- How much can we do in advance ?
- How could we revert to the original system ?

xdelta

The risk continuum

- What is the probability of a situation occurring ?
- What is the impact if that situation occurs ?
- What are the long-term consequences ?

- Most projects handle medium risk well enough
- Many projects over-specify to cater for low risk issues
- Some projects under-specify and fail to cater for high risk issues

- We need to identify critical components / people
- We need to identify critical stages during the project

xdelta

Planning and implementation

- Estimating and planning are key
- You cannot know everything up front
- Make effective assumptions to get started
- Beware assuming that everything will go well
- Cumulative discrepancies add up very quickly
- How will you monitor progress ?
- Checklists are essential, especially under pressure

“More software projects have gone awry for lack of calendar time than all other causes combined.”

“The mythical man-month” – Brooks

xdelta

Management

- Concentrate on quality of information and decision making
- Be thoughtful, not reactive - do not rush to respond
- Regular briefings, in person, phones off, no e-mail
- Need people to be committed and involved
- Never have one person working on their own
- Find good people, guide them and trust them
- Good administrative support lets people focus on their work
- Good management enables people to get things done

“Never tell people how to do things. Tell them what to do and they will surprise you with their ingenuity.”

General George Patton

xdelta

Leadership and people

- Build groups of excellent people who work well together
- Choose people who are willing to share information and help each other
- Give them the support and help they need so that they aren't distracted by trivia
- Confidence good; arrogance bad
- We're all in this together!

"The best executive is the one who has sense enough to pick good people to do what he wants done, and self-restraint enough to keep from meddling with them while they do it."

Theodore Roosevelt

xdelta

Procurement and responsibility

- Procurement – must do enough work up front:
  - It's not just about cost
  - Understand what is technically feasible
  - Understand what is strictly necessary
  - Clearly establish the scope
  - Define clear objectives
  - Define clear acceptance criteria

- Avoid split responsibility and be absolutely clear where the "duty of care" lies

xdelta

Project direction

- Design and implementation:
  - Have clear objectives. Think ahead as far as you can. Have a well-structured systems architecture. Understand the constraints. Focus on the core functions. Implement them as well as is possible.

- Project leadership:
  - Ensure that everyone involved maintains a consistent understanding of the project. Plan ahead as best you can.

- Budget and Schedule:
  - They have to be appropriate for the problems you're trying to deal with. Don't set them first!

xdelta

Key success factors

- Strong team of good people – no passengers
- Collaboration and willingness to share information
- Build “proof of concept” early on and learn from it
- Minimise complexity – “Occam’s Razor”
- Well structured and documented design
- Clearly defined interfaces
- Rigorous testing
- Document your decisions (what, how, why)

- Make life as easy as you can for those who come after you

xdelta

I.T. – the risk at the heart of your business

Chartered Quality Institute (Bristol)

Thank you for your participation

Colin Butcher CEng FBCS CITP
Technical director, XDelta Limited
www.xdelta.co.uk

xdelta

Further information – security (1)

- ICO (Information Commissioners Office)
  - *https://ico.org.uk/for-organisations/guide-to-data-protection/*
  - *https://ico.org.uk/for-organisations/guidance-index/*

- UK Government, Dept. of Business Information and Skills
  - Publication “Small businesses: What you need to know about cyber security” – March 2015
  - *https://www.cyberstreetwise.com/it-policies*

- UK Government, Cyber Essentials scheme:
  - *https://www.gov.uk/government/publications/cyber-essentials-scheme-overview*

xdelta

Further information – security (2)

- IASME (Information Assurance for Small to Medium-sized Enterprises)
  - *https://www.iasme.co.uk/index.php/about*
- GCHQ – 10 steps to cyber security
  - *https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary*
- CERT (National Computer Emergency Response Team)
  - *https://www.cert.gov.uk/what-we-do/*
- FCC (Federal Communications Commission - USA)
  - *https://www.fcc.gov/cyberforsmallbiz*

xdelta