A Successful Tool to Create Positive Change: Results of an IT Risk Assessment and Benchmark at Scandinavian Universities

Jan-Martin Löwendahl – CIO, Chalmers University of Technology, Sweden
Magnar Antonsen – IT Director, University of Tromsø, Norway
Jonas Everbrand – CIO, University of Kalmar, Sweden
Johan Lidros – CEO, Transcendent Group, USA
Contents

- Background
- Project Scope & Methodology
- Project Results
  - IT-Risks
  - Cost Benchmark
  - Quality IT-Processes
  - Conclusions
- How were the Results Used?
- Impact of the Project
- Q&A
Background

- IT does matter!
  - A tool for change...
    - ... to get IT to be the enabler of academic excellence that we all know it can be!
The Horrible Truth

transcendent (tran-sen'-dent), adj. 1. going beyond ordinary limits; excelling; superior; extraordinary. syn: unequaled, unrivaled, peerless, supreme
"A number of serious risks has been identified, that can impact the completeness and accuracy in information and usage of IT"
We have a need - How to Create the Change ("pain") Factor?

- Cost
- Benchmark (within the industry higher education)
- International accepted standards
- Independent assessment of an outside organization
Contents

- Background
- Project Scope & Methodology
- Project Results
  - IT-Risks
  - Cost Benchmark
  - Quality IT-Processes
  - Conclusions
- How were the Results Used?
- Impact of the Project
- Q&A
## Participating Universities

<table>
<thead>
<tr>
<th></th>
<th>Number of Universities</th>
<th>Number of Students</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002 Project - Doctoral/Research Universities* (Sweden/Norway)</td>
<td>14</td>
<td>287000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sweden</td>
<td></td>
<td>211000</td>
</tr>
<tr>
<td>Total</td>
<td>26</td>
<td>371000</td>
</tr>
<tr>
<td>Total Numbers: Universities in Sweden</td>
<td>48</td>
<td>337000</td>
</tr>
<tr>
<td>Coverage 46 %</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage approximately 80-85 %</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Numbers: Universities in Norway</td>
<td>38</td>
<td>210000</td>
</tr>
<tr>
<td>Coverage 4 %</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage approximately 40 %</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Carnegie classification

---

transcendent (træn-sen-dent), adj., 1. going beyond ordinary limits; excelling; superior; extraordinary, syn: unequalled, unrivaled, peerless, supreme
Participating Universities

2002 (14 universities)

**Sweden**
- Chalmers University of Technology - 7,500 students, founded 1829
- Karlstad University - 10,000 students, founded 1999
- Linköping University - 22,000 students, founded 1960
- Stockholm University - 35,000 students, founded 1878
- Uppsala University - 37,000 students, founded 1477
- Gothenburg University - 36,000 students, founded 1891
- Royal Institute of Technology - 12,500 students, founded 1826
- Lund University - 34,000 students, founded 1666
- Swedish Institute of Agriculture Science - 4,000 students, founded 1812
- Örebro University – 13000, founded 1977

**Norway**
- Bergen University - 17,000 students, founded 1946
- Norwegian University of Science and Technology - 18,450 students, founded 1996
- Oslo University - 32,000 students, founded 1811
- Tromsø University – 9,000 students, founded 1972

2004 (12 universities)

- Malmö University – 11000 students
- Blekinge Institute of Technology – 3000 students
- University of Kalmar – 7000 students
- University of Jönköping – 8000 students
- University of Borås – 6000 students
- University of Halmstad – 6000 students
- Mid Sweden University – 9000 students
- Högskolan Dalarna – 6000 students
- University of Gävle – 7000 students
- Mälardalen University – 9000 students
- The Stockholm Institute of Education – 7000 students
- University of Trollhättan/Uddevalla – 5000 students
High Level Overview IT-Risk Assessment with Benchmark

**Three Main Areas**

1. IT- and Telephone Costs
2. Quality of General IT Processes
3. IT-Risk Management

**Work Steps**

- Information gathering of IT and “business” processes
- Interviews and workshops to identify and rate IT risks
- Overall assessment of key risk areas
- Assessment of the quality of the four main IT-processes
- Assessment of IT and telephone costs
- Gap analysis, comparison to best practices and development of suggested actions
High Level Overview IT-Risk Assessment with Benchmark

**Benchmark**

- Benchmarks between participating universities, other available higher education industry benchmarks and other industries outside of higher education
- Benchmark with Domestic and International IT-standards

**Reporting**

- One comprehensive individual report per university
- One comprehensive report analyzing and summarizing the results for all universities as well as suggested actions for common high risk areas/weaknesses
- One high level (executive) report summarizing the results for all universities
- One full day seminar with all participants to discuss results and common actions
STEP 1 – Questionnaire

• IT
  • Total IT Costs
  • Central IT Costs
  • Faculty/Department IT Costs
  • IT Costs - Specific Areas
• Telephone Costs

STEP 2 – Quality Review and Calculation of Key Measures

Cost per “user” (students and employees), student/employee, etc.
Cost per system
Cost as part of revenues
Etc.

STEP 3 – Analysis

In the comprehensive analysis the universities were divided into relevant groups based on size and educational focus. In addition, other factors were analyzed to understand differences in costs such as size, location (large/small city), number of campuses, size and areas of education, size of research, etc.

STEP 4 – Reporting

Approximately 50 diagrams with key measures and benchmark data were provided and analyzed with general conclusions and suggestions.
IT & Telephone Costs

Total IT Costs
Central IT Costs
  • Common systems (Common administrative systems such as payroll, finance, registration, etc, and other common systems such as email)
  • Campus network
  • High speed Internet connectivity
  • Security
  • Help-desk
  • Research ("super" computers) etc

Faculty/Department IT Costs
  • Payroll
  • Hardware/software
  • Rent
  • Research ("super" computers)
  • Etc.
IT & Telephone Costs

IT Costs - Specific Areas
• Library
• Distance learning
• Cost per workstation
• Quality of data gathered per area
• Cost measurement infrastructure (policy/procedures to track, measure, approve and follow-up IT/telephone costs/investments)
• Training (students, teachers, administrative personnel)

Telephone Costs
• Fixed telephone infrastructure and charges
• Cell phones
• VoIP
STEP 4 – RESULTS

The diagram indicates the results per university and per area with key measurements. The example to the right shows the costs per university system and per user.
The methodology provides an analysis of the organizations information technology high risk areas/opportunities, mitigating controls and provides suggested action steps for the identified areas for improvement. Key IT risks and opportunities were identified through interviews and questionnaires. Risk level was defined by management during workshops. The overall process is described below:

**Identified IT high risk areas (at a gross risk level)**

**Assess risk management**

- Gross risk
- Net risk

**Risk acceptance – Can management accept the existing risk level?**

**Gross Risk Map**

**Net Risk Map**

**Risk Management**

- Likelihood
- Significance
Example: Description of Identified Risk Areas

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Description</th>
<th>Business Impact</th>
<th>Business Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Vendor Management and Service Level Agreements</td>
<td>XYZ is heavily dependent on external vendors in certain areas. Examples of critical vendors include: Meditech, Digex and AT&amp;T. The organization is responsible for assuring mitigating control procedures are in place for these vendors. To assure that risks such as: availability, data integrity, security and privacy are appropriately addressed they need to be documented and measured. As part of the vendor management process, it is also important to ensure that service level agreements are in place to define the process / data owners expectations of the service level, security, etc. from the service provider (IT department or outsourcing vendor). Lack of or unclearly defined service level agreements increase the risk of inappropriate allocation of resources, and service levels. Lack of service level agreements also increases the complexity of measuring the quality of delivered service.</td>
<td>If vendor provided systems and services are not available, it could impact the businesses ability to do work resulting in: - System downtime - Security / privacy issues - Non-regulatory compliance - XYZ’s IT costs could be higher than industry averages - Unexpected costs / contract issues could arise with external vendors</td>
<td>ALL</td>
</tr>
<tr>
<td>2 Viruses</td>
<td>XYZ is heavily dependent on information technology to process transactions. It is important for good controls to be in place to check all systems on a regular basis to ensure no viruses are introduced into the environment.</td>
<td>Virus infection could cause data loss, system downtime, and large costs to the organization in lost time and recovery efforts.</td>
<td>ALL</td>
</tr>
<tr>
<td>24 IP Telephony</td>
<td>XYZ employs several hundred employees and spends a significant amount of money in telephone charges through the local exchange and long distance providers. There is a possibility that XYZ could utilize another form of technology called “Internet Protocol (IP)” Telephony for phone needs. IP telephony utilizes the existing corporate wide area network for transferring phone calls.</td>
<td>We recommend that XYZ perform a cost/benefit study to assess the possibility of utilizing IP Telephony. This could result in lower phone costs for the corporation.</td>
<td>ALL</td>
</tr>
</tbody>
</table>

Virus infection could cause data loss, system downtime, and large costs to the organization in lost time and recovery efforts.

Business Impact

- System downtime
- Security / privacy issues
- Non-regulatory compliance
- XYZ’s IT costs could be higher than industry averages
- Unexpected costs / contract issues could arise with external vendors

Business Unit: ALL
### Assessment of High Risk Areas

After the high risk areas are identified each high risk areas mitigating controls are assessed and rated. The rating scale and an example is provided below. Mitigating controls are compared to IT best practices.

<table>
<thead>
<tr>
<th>Potential Risk Item</th>
<th>Previous Audits and Results</th>
<th>Quality of Existing Policies and Procedures</th>
<th>Other Control Factors (i.e. external auditing, consulting work)</th>
<th>Comments</th>
<th>Suggested Review Periodicity</th>
<th>Gross Risk Voting</th>
<th>Quality of mitigating controls</th>
<th>Mitigating controls Only Likely Goodness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Management and Service Level Agreements</td>
<td>A review of vendors and agreements are reviewed during the General Controls Review (GCR). However, that review has not been conducted since 2000</td>
<td>An outsourcing policy is being developed. This provides guidelines for selecting and maintaining an appropriate risk level/relationship with service providers. There are no policy and limited procedures in place to address appropriate level and monitoring of internal and external service level agreements.</td>
<td></td>
<td>Recommend audit</td>
<td>R</td>
<td>6.2, 4.6</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>IT Costs / Resource Allocation</td>
<td>No specific audits have been performed in this area.</td>
<td>All budgets are approved by the finance department. New initiatives are approved by senior management. There are no specific guidelines related to tracking, measuring or calculating ROI of IT-costs/investments. IT-costs are usually the third or fourth largest expense in the financial industry.</td>
<td></td>
<td>Recommend audit</td>
<td>O</td>
<td>5.5, 4.15</td>
<td>2</td>
<td>3.5</td>
</tr>
<tr>
<td>Viruses</td>
<td>No specific audits have been performed in this area.</td>
<td>The organization has documented policies and procedures in place. Virus software is executed automatically anytime a file from a foreign source is opened. Updates are automatically pushed out to PC’s and servers.</td>
<td>N/A</td>
<td>Recommend audit</td>
<td>R</td>
<td>6.5, 5.65</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>IT Asset Management</td>
<td>No specific audits have been performed in this area.</td>
<td>A policy addresses inappropriate licensing, moving equipment, ownership, etc. Approval of purchases must be performed by the VP only. Limited regular physical inventories are performed and limited tools exist to track inventories within the corporation.</td>
<td></td>
<td>Recommend audit</td>
<td>O</td>
<td>3.5, 3.4</td>
<td>3</td>
<td>3.4</td>
</tr>
</tbody>
</table>

[1] **Uncontrolled** – The process (control/procedures) does not exist (0 %)
1 **Informal** – The process is informal and unstructured (25 %)
2 **Defined** – The process is documented and communicated (50 %)
3 **Controlled** – The process is implemented and quality assured (75 %)
4 **Best Practice** – Best Practices are followed and encouraged (100 %)
Quality of General IT Processes

- In total, we have assessed 33 IT sub-processes with a total of 298 requirements and approximately 650 audit steps within the four main IT processes:
  - Organization and Management
  - System Development
  - Computer Operations
  - Security

- To be able to make an adequate comparison with best practices (domestic and international IT standards) and between organizations regarding their handling of IT risks and quality level, we use recognized international IT standards for each area in the assessment, e.g. ISO 17799, BS15000, ITIL, COBIT and CMMi.

- Every sub-process and every requirement is risk rated (High --3/Medium-2/Low-1) to create a risk based benchmark and result

The quality of the 650 requirements are assessed. Depending on how well the requirement is controlled, a rating will be assigned based on a scale of 0 to 4 as listed in the table to the right.

<table>
<thead>
<tr>
<th>Rating of Control</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Uncontrolled: The process does not exist (0 %)</td>
</tr>
<tr>
<td>1</td>
<td>Informal: The process is informal and unstructured (25 %)</td>
</tr>
<tr>
<td>2</td>
<td>Defined: The process is documented and communicated (50 %)</td>
</tr>
<tr>
<td>3</td>
<td>Controlled: The process is implemented and quality assured (75 %)</td>
</tr>
<tr>
<td>4</td>
<td>Best Practice: Best Practices are followed and encouraged (100 %).</td>
</tr>
</tbody>
</table>
Methodology Sources

The following is a list of some the sources / various governing bodies in which our assessment Process Methodology has been developed. Although this is a lengthy list of sources, it is not a comprehensive list of sources.

<table>
<thead>
<tr>
<th>Methodology Sources</th>
<th>Organization &amp; Management</th>
<th>Application Development</th>
<th>Computer Operations</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>COBIT</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IFAC</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ISO-I7799 (BS 7799)</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>GMITS – ISO/IEC TR 13335</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>PMI</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO 15408</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>DISC PD0005</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>BS 15000</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NIST (SP 500, SP 800 etc)</td>
<td></td>
<td></td>
<td>X</td>
<td>(X)</td>
</tr>
<tr>
<td>ITIL</td>
<td>X</td>
<td>(X)</td>
<td>X</td>
<td>(X)</td>
</tr>
<tr>
<td>IT Baseline Protection Manual</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>ISO 9126</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CMM</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>CASPR</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Quality of General IT Processes

Industry benchmark based on Transcendent Group data or other available information from organizations such as Computer Security Institute, ISACA etc.

Standard is 100%.
The first two columns in each process is the average for each project which is compared with the average for other industries.

<table>
<thead>
<tr>
<th>Organization &amp; Management</th>
<th>Application Development &amp; Maintenance</th>
<th>Computer Operations</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>22%</td>
<td>18%</td>
<td>19%</td>
<td>20%</td>
</tr>
<tr>
<td>22%</td>
<td>20%</td>
<td>20%</td>
<td>40%</td>
</tr>
<tr>
<td>30%</td>
<td>40%</td>
<td>20%</td>
<td>60%</td>
</tr>
<tr>
<td>67%</td>
<td>70%</td>
<td>70%</td>
<td>75%</td>
</tr>
</tbody>
</table>

0 **Uncontrolled** – The process (control/procedures) does not exist (0 %)
1 **Informal** – The process is informal and unstructured (25 %)
2 **Defined** – The process is documented and communicated (50 %)
3 **Controlled** – The process is implemented and quality assured (75 %)
4 **Best Practice** – *Best Practices* are followed and encouraged (100 %)
Assessment of General IT Processes

Quality Benchmark General IT Processes

- Organization/Management
- Application Development/Maintenance
- Computer Operations
- Security

Organizations:
- Organization X
- Average
# Reporting - Areas for Improvement

Each area for improvement will be described in detail with risk level, responsibility, investment and priority.

## Classification of risk and responsibility for recommendations regarding the IT environment at Organization XYZ

<table>
<thead>
<tr>
<th>Areas of improvement</th>
<th>Risk</th>
<th>Responsibility</th>
<th>Investment</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A – Organization and Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. System ownership</td>
<td>2</td>
<td>B</td>
<td>**</td>
<td>I</td>
</tr>
<tr>
<td>2. IT strategy</td>
<td>1</td>
<td>A</td>
<td>*</td>
<td>I</td>
</tr>
<tr>
<td>3. ROI</td>
<td>2</td>
<td>A</td>
<td>*</td>
<td>II</td>
</tr>
<tr>
<td>4. Personnel</td>
<td>1</td>
<td>B</td>
<td>*</td>
<td>I</td>
</tr>
<tr>
<td>5. IT risk management</td>
<td>2</td>
<td>A</td>
<td>*</td>
<td>II</td>
</tr>
<tr>
<td>6. Service level agreement</td>
<td>2</td>
<td>B, D</td>
<td>**</td>
<td>III</td>
</tr>
<tr>
<td>7. Technical direction</td>
<td>2</td>
<td>B</td>
<td>*</td>
<td>II</td>
</tr>
<tr>
<td>8. Etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Risk Classification

Each area has been risk classified according to the following:

1. Very critical to organization’s efficiency and to the fulfillment of the goals of the operations in the short- and long-term.
2. Critical for good internal control, efficiency and reliability in organization’s IT-operations.
3. Essential for good internal control, efficiency and reliability in organization’s IT-operations.

### Responsibility

The areas of responsibility for each area of improvement have been defined as follows:

- A. Management of Organization (board, leadership team, etc.)
- B. CIO
- C. IT-manager Faculty
- D. System owner

This classification of responsibility is based on the organizations current organizational structure, best practices and legal requirements.

### Investment

We have estimated the total investment needed to act on the recommendation according to the following scale:

- * $3,000-$30,000
- **$30,000-$60,000
- ***> $60,000

The cost is based on an internal cost of $55 per hour.

### Priority

For each recommendation we provide the priority level for implementation for each improvement item as a support for the creation of an action plan. The following categories are used:

- I Immediate action
- II Project to be initiated or completed within 6 months
- III Action within 18 months
### A.1 IT STRATEGY

#### RESPONSIBILITY:

#### TIMING (DATE):

#### MANAGEMENT COMMENTS/ACTION PROPOSED:

#### RESPONSIBILITY:

---

<table>
<thead>
<tr>
<th>OBSERVATION</th>
<th>LEVEL OF RISK: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization X does not have an IT strategy stating the long-term goals and objectives of the IT function.</td>
<td>RISK</td>
</tr>
<tr>
<td>To a significant degree, the ability of Organization X to meet long-term growth and profitability goals is dependent upon the existence of management information systems. Information is essential to accurate decision-making. The best assurance that information systems are implemented on a timely basis is the preparation and execution of a short- and long-range information systems plan. The information systems plans should be integrated and regularly updated with the Organization’s business plan. The lack of a long-range plan exposes Organization X to the risks of not having proper systems to support operations and the development of non-supportive or un-required systems.</td>
<td></td>
</tr>
</tbody>
</table>

**RECOMMENDATION**

We recommend an information systems plan be developed in conjunction with the organization’s business plan. The long range plan should include the following:

- The software systems needed to satisfy management's information requirements for the next three to five years.
- The hardware necessary for the software requirements.
- An implementation schedule for each of the systems including personnel requirements.
- The short-term information systems plan should include steps to accomplish the long-range information systems plan. Over the life cycle of an information system, costs can be greatly increased if the proper amount of design is not accomplished prior to the beginning of the programming phase (or selection of software from vendors). The higher costs are usually manifested in the form of continual requests to change programs or purchase additional software to meet the needs of the company. An information systems plan will help reduce these costs.
The below table summarizes the identified areas for improvement arranged by area, responsibility and estimated cost.

<table>
<thead>
<tr>
<th>Area of Improvement</th>
<th>Responsible Owner</th>
<th>Investment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Management of Organization</td>
<td>IT-Director</td>
</tr>
<tr>
<td>Organization and Management</td>
<td>12</td>
<td>7</td>
</tr>
<tr>
<td>Systems Development and Maintenance</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Computer Operations</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Security</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>13</td>
<td>24</td>
</tr>
</tbody>
</table>

Most of the improvement suggestions fall under the IT-Director. However, senior management of the organization are responsible for approximately 27% of areas for improvement. The total investment to address all the identified areas for improvement is approximately $1,140,000 divided accordingly by risk classification:

- Risk Classification 1: $285,000
- Risk Classification 2: $630,000
- Risk Classification 3: $225,000
- Total: $1,140,000
Contents

- Background
- Project Scope & Methodology
  - IT-Risks
  - Cost Benchmark
  - Quality IT-Processes
- Project Results
- How were the results used?
- Impact of the project
- Q&A
## IT Risks – Result per Risk Type

<table>
<thead>
<tr>
<th>Type of Risk</th>
<th>Universities 2004</th>
<th>Universities 2002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure</td>
<td>57 %</td>
<td>45 %</td>
</tr>
<tr>
<td>Availability</td>
<td>22 %</td>
<td>18 %</td>
</tr>
<tr>
<td>Relevance</td>
<td>6 %</td>
<td>13 %</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>0 %</td>
<td>13 %</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>8 %</td>
<td>7 %</td>
</tr>
<tr>
<td>Specific Risks</td>
<td>7 %</td>
<td>4 %</td>
</tr>
<tr>
<td>Total</td>
<td>100 %</td>
<td>100 %</td>
</tr>
</tbody>
</table>

**Integrity risk.** The risk that data cannot be relied on because it is incomplete or inaccurate.

**Confidentiality risk.** This risk refers to the risk associated with inappropriate access to systems, data or information.

**Availability risk.** The risk that information system or information is not available when needed.

**Infrastructure risk.** The risks that an organization does not have an IT infrastructure that can effectively support the current and future business needs in an efficient, cost-effective and well-controlled fashion. The infrastructure includes the following areas: hardware, networks, software, people, processes (policy and procedures).

**Relevance risk.** The risk that an organization is not fully utilizing technology to obtain business advantages (additional revenues or cost reductions).
Results – Gross Risks

| Potential Risk | Opportunity | Risk and Opportunity | Some risk mitigation in place |

Bruttorisker

Significance

Likelihood

3.00

3.50

4.00

4.50

5.00

5.50

6.00

6.50

7.00

3,00

4,00

5,00

6,00

7,00

transcendent (tran-senˈdent), adj., 1. going beyond ordinary limits; excelling; superior; extraordinary. syn: unequaled, unrivaled, peerless, supreme
## Results – Identified & Prioritized Risks

<table>
<thead>
<tr>
<th></th>
<th>Risk Management</th>
<th></th>
<th>Data integrity Ladok (student admission and documentation system)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Insufficient information available for IT decisions</td>
<td>28</td>
<td>Student essay “cheating”</td>
</tr>
<tr>
<td>3</td>
<td>High level IT Policies</td>
<td>29</td>
<td>Financial system (Agresso, Raindance etc)</td>
</tr>
<tr>
<td>4</td>
<td>System/process owners capabilities to define requirements and acquire IT system and resources</td>
<td>30</td>
<td>Internet Image and Content</td>
</tr>
<tr>
<td>5</td>
<td>Compliance to internal policies/decisions</td>
<td>31</td>
<td>Internationalization</td>
</tr>
<tr>
<td>6</td>
<td>Project Management</td>
<td>32</td>
<td>IT Strategy</td>
</tr>
<tr>
<td>7</td>
<td>Integration between administrative systems</td>
<td>33</td>
<td>Academic freedom</td>
</tr>
<tr>
<td>8</td>
<td>Data storage/management</td>
<td>34</td>
<td>Macintosh computers</td>
</tr>
<tr>
<td>9</td>
<td>IT is not in alignment with the universities long term plan</td>
<td>35</td>
<td>Help-desk</td>
</tr>
<tr>
<td>10</td>
<td>Regulatory Compliance</td>
<td>36</td>
<td>Information overflow</td>
</tr>
<tr>
<td>11</td>
<td>IT coordination resources/skills (central IT, faculty, department)</td>
<td>37</td>
<td>Telephones</td>
</tr>
<tr>
<td>12</td>
<td>Skills IT personnel</td>
<td>38</td>
<td>Theft of hardware</td>
</tr>
<tr>
<td>13</td>
<td>End user skills (students, teachers, administration)</td>
<td>39</td>
<td>Software license management</td>
</tr>
<tr>
<td>14</td>
<td>Teachers do not utilize existing IT infrastructure</td>
<td>40</td>
<td>Roles and responsibilities IT</td>
</tr>
<tr>
<td>15</td>
<td>IT as and competitive advantage for recruiting/research</td>
<td>41</td>
<td>Payroll/HR system</td>
</tr>
<tr>
<td>16</td>
<td>Spam</td>
<td>42</td>
<td>System/Information Ownership</td>
</tr>
<tr>
<td>17</td>
<td>Distance learning (E-learning)</td>
<td>43</td>
<td>Email</td>
</tr>
<tr>
<td>18</td>
<td>Standardization</td>
<td>44</td>
<td>Back-up management</td>
</tr>
<tr>
<td>19</td>
<td>Availability critical systems</td>
<td>45</td>
<td>IT costs to high or incorrect allocated</td>
</tr>
<tr>
<td>20</td>
<td>Availability administrative systems</td>
<td>46</td>
<td>Tools for financial follow-up</td>
</tr>
<tr>
<td>21</td>
<td>Disaster - Business Continuity &amp; Disaster Recovery</td>
<td>47</td>
<td>Security administration</td>
</tr>
<tr>
<td>22</td>
<td>Formalized procedures</td>
<td>48</td>
<td>Outsourcing/vendor management</td>
</tr>
<tr>
<td>23</td>
<td>Information security</td>
<td>49</td>
<td>Security flaws Microsoft products</td>
</tr>
<tr>
<td>24</td>
<td>Journal registration/management</td>
<td>50</td>
<td>In-house developed systems</td>
</tr>
<tr>
<td>25</td>
<td>Dependency to key individuals</td>
<td>51</td>
<td>Single sign-on</td>
</tr>
<tr>
<td>26</td>
<td>Educational support systems</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Result – Net Risks

- Potential Risk
- Opportunity
- Risk and Opportunity
- Some risk mitigation in place

Likelihood vs. Significance graph

Nettorisker

Some risk mitigation in place
## Key Risks/Opportunities

### 2004

#### RISKS
- **Dependency key individuals**
- Availability core systems
- Availability Phone systems
- Back-up Management

#### RISKS/OPPORTUNITIES
- Internet Image
- Lack of formalized procedures

#### OPPORTUNITIES
- Cooperation IT: Central/faculty/department IT
- IT as an competitive advantage

### 2002

#### RISKS
- Data integrity core systems
- Availability phone systems
- Availability research systems
- **IT roles & responsibilities**
- **Compliance to internal policies/decisions**
- Employee skills central and local IT (faculty/department)
- Teachers do not use IT infrastructure

#### OPPORTUNITIES
- Cooperation IT: Central/faculty/department IT
- **Student Portals (the self administrated student)**
Contents

- Background
- Project Scope & Methodology
- Project Results
  - IT-risks
  - Cost Benchmark
  - Quality IT-processes
  - Conclusions
- How was the Result Used
- Impact of the Project
- Q&A
## Summary Result IT Costs

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IT costs in percentage of revenues</td>
<td>6,8 % 7,1 % including rent</td>
<td>6,4 %</td>
<td></td>
</tr>
<tr>
<td>IT costs per &quot;user&quot; (FTE* students and employees)</td>
<td>$686 (SEK 6147)</td>
<td>$1440 (SEK 10786)</td>
<td></td>
</tr>
<tr>
<td>IT costs per FTE Students</td>
<td>$730 (SEK 5475)</td>
<td>$1514 (SEK 11355)</td>
<td>$1400 (SEK 10500)</td>
</tr>
<tr>
<td>IT costs per FTE Employee</td>
<td>$7100 (SEK 10778)</td>
<td>$6090 (SEK 45694)</td>
<td>$14000 (SEK 105000)</td>
</tr>
<tr>
<td>Allocation central IT and local IT (faculty, department, institute)</td>
<td>45 % central 55 % Faculty/Department IT</td>
<td>31 % central 69 % Faculty/Department IT</td>
<td>37 % central 63 % Faculty/Department IT</td>
</tr>
</tbody>
</table>

* Full Time Equivalent
General Conclusions IT Costs

General Conclusions 2002 Project (Doctoral/Research Universities)
• High IT costs compared with other industries and with large variations between the participating universities: IT costs in percent of revenues; Average 6.4 %, highest 9.3 %, lowest 4.4 %

• Specialized universities have higher IT costs

• A large part of IT costs are on the faculty/department level (average 69 %)

• Universities with a larger percentage central IT have a lower total IT cost

General Conclusions 2004 Project Master’s Colleges and Universities
• High IT Costs compared with other industries with large variations between the universities: IT costs in percent of revenues; Average 6.8 %, highest 10.1 %, lowest 4.9 %

• Larger universities have a lower IT costs (large scale advantages)

• Universities with more then one campus have approximately 20 % higher IT-costs

• Huge variations in IT costs for distance learning between the universities
General Conclusions IT Costs

Differences between Doctoral/Research Universities and Master Colleges Universities

• Doctoral Research Universities have much higher cost per user/student or employee which mainly due to
  • More research (61% of revenue compared with 20% of revenue)
  • Type of education areas (faculties) - universities with a higher portion of Science and Technology have a higher IT cost.

• Master Colleges Universities have larger portion of IT centralized than Doctor/Research Universities (45% compared with 31%)

• Doctoral/Research Universities have significant higher cost for administrative systems then Master Colleges Universities
Contents

- Background
- Project Scope & Methodology
- Project Results
  - IT-risks
  - Cost Benchmark
  - Quality IT-processes
  - Conclusions
- How was the Result Used
- Impact of the Project
- Q&A
Quality IT Processes – Result

Informal: The process is informal and unstructured (25 %)
Quality Benchmark – All Processes

QUALITY BENCHMARK - ALL PROCESSES

Universities 2002

0.0%  25.0%  50.0%

28.8%  27.2%  24.1%  22.7%  20.7%  20.1%  19.7%  17.1%  16.9%  15.6%  13.6%  13.1%

=Average 2004

Genomsnittsvärde = Average 2004
Quality Benchmark – Average per Sub-Process

Computer Operations

A. Manage Performance and Capacity
B. Ensure Continuous Service (prevent business interruption)
C. Manage Operations

Security

A. Security Administration and Management
B. Data Classification and Ownership
C. Logical (Technical) Security
D. Physical Security
E. Monitor and Compliance
F. Special Protection Issues
### Responsibilities - Identified Areas for Improvements

<table>
<thead>
<tr>
<th>Responsible</th>
<th>2002</th>
<th>2004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Team</td>
<td>30%</td>
<td>34%</td>
</tr>
<tr>
<td>CIO</td>
<td>2 %</td>
<td>0 %</td>
</tr>
<tr>
<td>IT Director Central IT</td>
<td>45 %</td>
<td>44 %</td>
</tr>
<tr>
<td>System Owner</td>
<td>13 %</td>
<td>19 %</td>
</tr>
<tr>
<td>Dean, Prefect or equal</td>
<td>5 %</td>
<td>1 %</td>
</tr>
<tr>
<td>Department or Faculty IT</td>
<td>5 %</td>
<td>2 %</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100 %</strong></td>
<td><strong>100 %</strong></td>
</tr>
</tbody>
</table>
### Risk Level and Total Cost to Identified Weaknesses

<table>
<thead>
<tr>
<th>General IT Process</th>
<th>Total Recommendations</th>
<th>Risk Level</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization &amp; Management</td>
<td>171</td>
<td>44%</td>
<td>77</td>
<td>45%</td>
<td>73</td>
</tr>
<tr>
<td>Application Development &amp; Maintenance</td>
<td>60</td>
<td>16%</td>
<td>24</td>
<td>40%</td>
<td>36</td>
</tr>
<tr>
<td>Computer Operations</td>
<td>80</td>
<td>21%</td>
<td>26</td>
<td>33%</td>
<td>54</td>
</tr>
<tr>
<td>Security</td>
<td>74</td>
<td>19%</td>
<td>1</td>
<td>1%</td>
<td>64</td>
</tr>
<tr>
<td>TOTAL</td>
<td>385</td>
<td>100%</td>
<td>128</td>
<td>33%</td>
<td>227</td>
</tr>
</tbody>
</table>

The average investment per university to address identified weaknesses the general IT processes

- **Investment level * ($4000-$40000)**: $275 000
- **Investment level ** ($40001-$80000): $925 000
- **Investment level *** ($80001-)**: $300 000
- **Total**: $1 500 000
Contents

- Background
- Project Scope & Methodology
- Project Results
  - IT-risks
  - Cost Benchmark
  - Quality IT-processes
  - Conclusions
- How were the Results Used
- Impact of the Project
- Q&A
Conclusions

IT Risks
IT Costs
Quality in Main IT processes
AN EFFECTIVE AND EFFICIENT IT OPERATION

There are several elements necessary to assure an effective and efficient IT Risk Management process. The key elements and their relations are illustrated below:

BUSINESS OPERATIONS

INFORMATION SECURITY POLICY AND STANDARDS

IT STRATEGY
- Hardware
- Software
- Organization
- Responsibility

SYSTEM AND INFORMATION RESPONSIBILITIES

IT OPERATIONS (PROCEDURES)
- Organization and management
- Development and maintenance
- Computer operations
- Security administration
- Logical security

APPLICATIONS
- Controls to assure
  - Completeness
  - Correctness

ON GOING EXAMINATION, UPDATING AND CONTROL OF POLICY AND PROCEDURES
Results

Executive Managements Responsibility
- IT-strategy
- System/information Ownership
- Information Security
- Coordination
- Measurements
- Compliance
- IT costs/ROI

System Owners
Responsibility for the "information", functionality, service defined

IT Departments Responsibility
Infrastructure
- Computer Operations
- Application Development
- Security Infrastructure
- Help-desk

Business Operations
- Management
- Information Security Policy and Standards
- IT Strategy
- System and Information Responsibilities
- IT Operations (Procedures)
- On Going Examination, Updating and Control of Policy and Procedures

IT Strategy
- Hardware
- Software
- Organization Responsibility

System and Information Responsibilities
- Organization and management
- Development and maintenance
- Computer operations
- Security administration
- Logical security

Infrastructure
- Controls to assure
- Completeness
- Correctness
Contents

- Background
- Project Scope & Methodology
- Project Results
  - IT-risks
  - Cost Benchmark
  - Quality IT-processes
  - Conclusions
- How were the Results Used
- Impact of the Project
- Q&A
How was the Project Results Utilized

- **List** of common weaknesses were prioritized and converted into projects.
  - The projects were then divided among the participants or run as joint projects.

- **List** of universities with strong areas (knowledge sharing)
  - This has helped many collaboration efforts just by the fact that we know more about each other.
Contents

- Background
- Project Scope & Methodology
- Project Results
  - IT-risks
  - Cost Benchmark
  - Quality IT-processes
  - Conclusions
- How were the Results Used
- Impact of the Project
- Q&A
Things that we were able to implement and that has made a difference to how we govern and produce IT-services

- **Top-down decision fora that enables majority decisions**
- Vision, goals and strategy that are actually supported by management
- Bottom-up systems ownership framework that enables user control
- Project steering framework
- Cost accounting model for IT
- ...
IT Costs at Chalmers 1996-2003

Chalmers IT-cost

- 1996: MSEK 123, 8.0%
- 1997: MSEK 136, 8.9%
- 1998: MSEK 158, 10.0%
- 1999: MSEK 197, 11.6%
- 2000: MSEK 183, 10.5%
- 2001: MSEK 162, 9.0%
- 2002: MSEK 146, 7.8%
- 2003: MSEK 135, 7.0%
- Forecast 2003: MSEK 140, 7.5%

- Total IT costs from 1996 to 2003: MSEK 1,176

- IT costs as % of turnover:
  - 1996: 8.0%
  - 1997: 8.9%
  - 1998: 10.0%
  - 1999: 11.6%
  - 2000: 10.5%
  - 2001: 9.0%
  - 2002: 7.8%
  - 2003: 7.0%

- Forecast IT costs 2003: MSEK 140, 7.5%
Q & A

Johan Lidros Project Manager (2002 and 2004)
Johan.lidros@transcendentgroup.com

Jan-Martin Löwendahl (Chairman Steering Committee 2002)
Jan-martin.Lowendahl@gartner.com

Magnar Antonsen (Steering Committee 2002)
Magnar.Antonsen@cc.uit.no

Jonas Everbrand (Chairman Steering Committee 2004)
jonas.everbrand@hik.se