Creating an IT plan is more than words on a page

Karoline Westerlund[1]

[1]Umeå universitet, SE-901 87 Umeå, Sweden, karoline.westerlund@umu.se

Keywords
IT plan, IT governance, Security, Risk analyses, Shadow IT

1. Summary

This paper presents an approach making awareness of security issues further out in the organization by creating an IT plan for one department at our university. The IT plan provides a structure to help organize and define roles and responsibilities, an enabler. The IT plan should be communicated, understood and accepted.

2. ABSTRACT

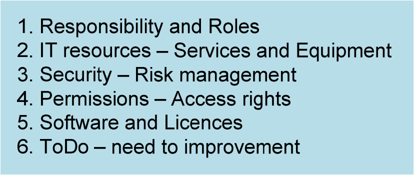
I was contacted by the Head of Administration at one of our departments asking what authority their IT support group had when it came to IT resources and security issues.

I thought it would be interesting to share their experiences and work together with them. I invited myself to the group and we started a one year long journey meeting once a month which resulted in an IT plan as Dean signed up. For me it was interesting to see what issues they were facing and what local solutions they had developed instead of using our central IT services. Trust was important and I decided not to lecture them. Instead I asked questions about their choices of solutions, hopefully making them rethinking.

The objective was to provide a structured methodology to help the IT group developing and implementing an IT plan for governance and planning of IT resources at their department. The outcome was to define decision rights and liability frameworks for desired behavior regarding IT usage. The department needed to understand and commit to the plan and for that we needed full commitment from the department's leadership.

The IT group supported 170 employees and 2000 students. Together, they used a variety of IT services and managed a large amount of information. They had a mixture of centrally provided services and local solutions developed and managed by the IT group.

The IT plan had to align with the university's governance policies and regulations and supplement with local rules that were unique to their needs. I wanted to point out the most important areas to cover, keep it short so people actually took part of it and put some more detailed documents in an appendix, see figure 1.



1. Responsibility and Roles
2. IT resources – Services and Equipment
3. Security – Risk management
4. Permissions – Access rights
5. Software and Licences
6. ToDo – need to improvement

Figure 1 Areas covered in the IT plan

Every meeting covered one of the areas. I put up the frame and questions and the first thing we did was to identify the key responsibility roles and assign people to the roles. We used the RACI matrix, responsibility assignment matrix, to visualize. We determined the key points of the responsibilities and mandates they had.

We identified the support they gave to the most commonly IT services used on a daily basis and what areas they covered. Standard specifications were set for workplaces for different roles. The most important security issues related to behavior were highlighted. Here we are talking about information security, backup, password, phishing mail and virus.

It is important to have control over higher permissions to the applications. We set up a matrix of applications, persons connected and what kind of permission.

Software and licenses is a complicated area. To maintain control you must established procedures for purchasing and installation of software. We developed a description of various software normally available and pointed out one responsible person in the group.

During the year we identified areas that needed improvement. A new matrix describing activities, expected results and responsible appointed person was prepared. One important security issue was that they had their own backup solution and the hardware placed in a room in the basement with no security classification. A new lesson had to be learned – how to identify risk factors and classify the information. Another lesson learned was that what is not documented is not – you have to understand the need of documentation and know where you will find it.

When we started our work we agreed upon that the Head of administration is to be responsible for the IT plan, keep it alive and update it with the IT group and communicate it to everyone in the department. When the IT plan was approved by the Dean the Head of Administration called for an all staff meeting presenting the IT plan and pointed out the most important security issues they had to relate to.

This kind of work did not come easy for the group. They had a lot of information but needed help to transform it to an IT plan.

3. REFERENCES

Westerlund, K (2015) *The importance of having a disaster recovery planning process* EUNIS (2015) ISSN 2409-1340 http://www.eunis.org/eunis2015

Westerlund, K (2015) *Setting goals and measuring the value of Enterprise IT Architecture using the COBIT 5 framework* EUNIS (2015) ISSN 2409-1340 http://www.eunis.org/eunis2015

Westerlund, K (2013) *One way to communicate the value of Enterprise Architecture – maturity levels for IT applications*, EUNIS (2013) ISBN 978-9934-10-433-6 http://eunis2013.rtu.lv/content/program

Westerlund, K (2012) *How we built an Enterprise Architecture framework meeting our needs*, EUNIS (2012), www.eunis.pt/images/docs/abstacts/P2C1.pdf

Westerlund, K (2011) *On Budget is Not Enough – Lesson Learned Leaving an Email System from the 90s*, EUNIS (2011), www.eunis.ie/papers/On-Budget-Is-Not-Enough_KarolineWesterlund_Paper.pdf

4. AUTHORS' BIOGRAPHIES

K. Westerlund. I work as an IT-strategist at Umeå University since 1997. I am a part of the IT Office and we have a mandate from the University Management to take strategic responsibility for all common IT at the university. Between the years 1994 to 1997 I worked as a project manager and was responsible for the development of an IT system supporting human recourses, named Primula, for higher education in Sweden. At the beginning of the 90s I worked as a development strategist at Umeå University and in the sector. During the years 2006 to 2012 I was a member of the Ladok Board. I have studied informatics, economics and law at Umeå University. I have the strategic responsibility for IT security. On an annual basis, I give a number of seminars in various fields such as Enterprise Architecture, Governance, Management and Information Security.