Chapter 3

Improving IT incident handling performance with information visibility

In large internal IT organizations, multiple teams are often involved in handling incidents, so these teams come to depend on one another. We hypothesize that the knowledge these teams have of the agreed upon and realized incident handling performance of themselves and other teams will impact their performance. We tested this hypothesis at a large financial institute, using log data from the IT service management application and a survey to measure the knowledge of teams.

We found (1) a significant positive correlation between incident handling performance of a team and the knowledge a team has of its own performance, (2) no correlation between the knowledge of agreed upon performance and realized performance within a team, (3) that teams have very little knowledge of agreed upon or realized performance of other teams, and (4) that improving the knowledge a team has of the agreed upon and realized performance of that team and dependent teams, results in higher incident handling performance. The results show that increasing information visibility within and across teams in large IT providers is one way to improve incident handling performance.

3.1 Introduction

Internal information technology (IT) organizations of large multi-nationals often have more than 2000 employees. Such large scale IT allows to utilize economies of scale and centralizing activities to specialized IT service-teams. These IT service-teams are typically positioned in one of three service layers: (1) Infrastructure as a Service (IaaS), (2) Platform as a Service (PaaS), or (3) Software as a Service (SaaS). A service-team in a layer delivers technology based services to the next layer in the chain, as depicted in Figure 8, ultimately to the (internal) business partners.

What a service-team offers is usually predefined in a service catalog (Hiles, 2002). A service catalog typically defines the offered technology, the predefined maximum duration of IT incidents and the minimum average availability. What service-teams in a layer have to deliver to the next layer in the chain is predefined in Service Level Agreements (Sallé & Bartolini, 2004). A Service Level Agreement (SLA) formalizes the dependencies between the layers, including IT incident handling (Hiles, 2002).

Dependencies between service-teams in the chain are often critical. For instance disruption of an IaaS service causes disruption of the IT services on PaaS and SaaS level. A shared task of service-teams is therefore to handle IT incidents that occur during their service delivery (Bartolini et al., 2006; Team, 2010b). When an IT incident occurs the first service-team that discovers the IT incident assigns the task to resolve the IT incident to the service-team that seems to cause the incident. However, the assigned service-team may not be the one that has caused the incident, or is not able to completely resolve the incident. As a result IT incident handling tasks get routed between service-teams. Effective routing of incidents allows service-teams to solve IT incidents swiftly.

Yet, other variables affect effective incident handling, as service-teams need to be capable of handling assigned incidents. For instance a service-team may have a large backlog of incidents that prevents swift incident handling. In that case it is insufficient to just route the incident to a service-team. A subsequent phone call or the temporary reallocation of resources might be required. To be able to take such actions, visibility of incident handling performance by members of the service-team is required.

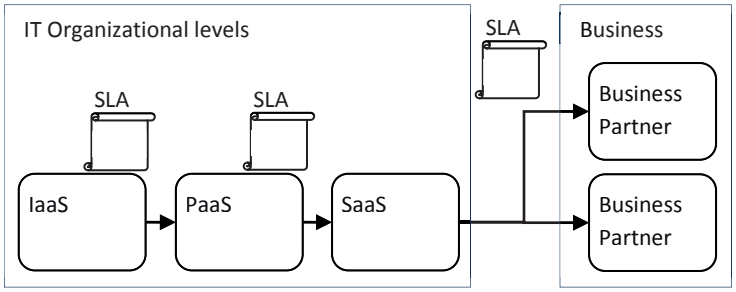

Figure 8, Service chain of an IT service provider offering services to business partners

Research in supply chains shows that improved supply chain visibility improves performance of the supply chain (Bartlett et al., 2007; Caridi et al., 2010b). Supply chain visibility for instance mitigates large fluctuation in inventory by optimizing the flow of goods (Disney & Towill, 2003; H. L. Lee et al., 1997). Supply chain visibility is defined by (Francis, 2008) as "the identity, location and status of entities transiting the supply chain, captured in timely messages about events, along with the planned and actual dates/times for these events".

As routing in supply chains resembles routing of IT incident handling tasks, we use the supply chain visibility concept in our research. We define visibility as: "*the quality of known information characterizing predefined entities in a predefined IT domain*". For this research this means: "*incident handling performance information known by IT service-team members that are part of IT service chains*".

We hypothesize that visibility of incident handling performance information positively correlates with incident handling performance. We argue that incident handling performance information is the primary type of information that has to be visible to IT staff, as this type of information indicates how well incidents should be handled and are handled by service-teams.

We investigate performance of incident handling in chains of service-teams. Based on our visibility concept we measure how much a service-team 'sees' of incident handling.

The visibility is measured in terms of (1) the 'seen' realized incident handling performance and (2) the 'seen' agreed incident handling performance defined in SLAs. The two visibility measures are correlated with the realized incident handling performance, to evaluate the hypothesis. Control theory is used to express the hypothesized relationship between visibility and performance.

Research was conducted in an IT organization of a multinational financial institute, at seven interdependent service-teams. We found that visibility of incident handling performance of a service-team significantly correlates with the incident handling performance of that team. We also found that knowledge about the performance of other, dependent, service-teams is extremely low. We did not find any correlation between the visibility of SLAs and incident handling performance. The results of this first case study are reported in (Vlietland & van Vliet, 2013).

In a follow-up case study in the same organization, we tested the usage of information visibility to *improve* incident handling performance. For one service-team, we used visibility based interventions to change the team's perception of the realized incident handling performance. The interventions are performed by the central incident management team by making the realized incident handling performance visible, for instance through incident handling reports. Over a period of 10 months in which we gathered empirical data, we found incident handling performance of this team improved from less than 10% to over 80%.

The remainder of this chapter is organized as follows. Section 3.2 discusses service-teams and incident handling. Section 3.3 describes the research design of both case studies. Section 3.4 covers the results of the first case study, in which we investigate the correlation between visibility of incident handling performance and actual incident handling performance. Section 3.5 elaborates on the results of the second case study, which focuses on improving incident handling performance by improving visibility. Section 3.6 elaborates on the threats to validity and the limitations of this research. Section 3.7 conclusion concludes the research, deduces the implications and suggests future research avenues.

3.2 Service-teams and Incident handling

As explained in the previous section, service-teams are positioned in layers (Bartolini et al., 2006). A team in a layer uses technology from other teams, typically from a lower layer in the chain. Figure 9 shows a chain segment.

In this figure, service-team Intel servers (IaaS) delivers computing capacity to a Windows hosting service-team (PaaS) that uses it to host a Windows webserver. This hosting service is delivered to a Business application service-team to host a web-enabled business application (SaaS). The arrows indicate the direction of service delivery, flowing from left to right. Each service-team in the chain enriches the service and offers it to the next layer in the chain.

A team does not solely deliver technology as it should also act on events, for instance when delivered technology gets disrupted (Bardhan et al., 2010; Jantti, 2011). In that case a team delivers an act or a deed next to technology(Jäntti, 2012a). We use the term IT services as a combination of technology and performed actions (Ellram et al., 2007; Peppard, 2003). As a service-team has an agreed responsibility with service-teams higher in the chain it has to take care of its supplying IT services, next to managing its own IT service(s) (Niessink, 2001).

The following example illustrates the involvement of multiple service-teams:

> *A SaaS service-team notices a disruption in its service. The team records the disruption as an incident in an IT Service Management (ITSM) application that is used to manage and route incident information. The team subsequently starts investigating the root-cause. The team discovers that the disruption is caused by a failed Windows hosting service and routes the recorded incident to the Windows hosting service-team. This is indicated by the dotted arrow and the icon in Figure 9. The hosting team receives the incident and starts investigating the root- cause. The team discovers that the hosting server is down and routes the recorded incident to the IaaS service-team. This team solves the incident and brings the services back online.}*

Many incidents are typically assigned to service-teams. As a consequence, a service-team has a backlog of assigned IT incidents as shown in Figure 9. The size of the backlog varies based on the amount of (related) incidents. Each service-team has to organize incident handling in such a way that all assigned incidents are resolved within the time constraints of the SLA.

Incidents can differ in priority and each registered incident is therefore tagged with an incident priority. High priority incidents must be resolved immediately; low priority incidents may be resolved later. Incident priority is typically based on user urgency and business impact. The maximum allowed duration of an incident for each priority is predefined in the service catalog.

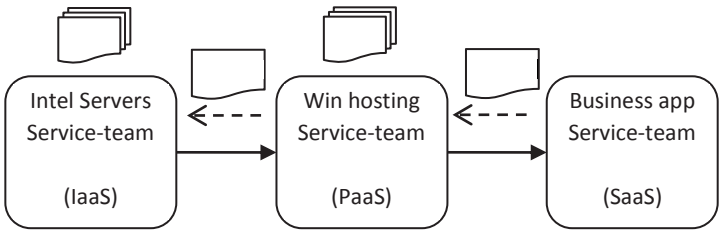

Figure 9, Routed IT incident between service-teams

The registration, assigning and tracking of incidents might be centralized to an Incident Management (IM) team. The central IM team tracks the handling of incidents on behalf of the technology oriented service-teams. Next to tracking, the central IM team provides incident handling performance reports (Jäntti, Lahtela, & Kaukola, 2011). Incident handling performance reports contain, for each incident priority, the percentage of incidents that are handled within the maximum duration by that service-team.

As all IT service-team members are potentially involved in IT incident handling we reason that the (1) agreed incident handling performance and the (2) realized incident handling performance should be known to all members of the service-team.
As mentioned earlier the dependencies between service-teams are typically critical; if a service is disrupted, dependent services get disrupted too. For instance in Figure 9 the business application gets disrupted when the windows hosting service is down. Given these critical dependencies we argue that knowledge about incident handling performance and agreed service levels should not be limited to the own service-team. The service-team members should also know the realized incident handling performance and agreed incident handling performance of interdependent service-teams.

3.3 Research design

Our literature research did not result in any literature about the correlation between incident handling visibility and incident handling performance. Nevertheless a large body of related literature was found that we discuss and use to build the model and shape the hypotheses.

We follow OGC for the definition of an IT incident: "an event which is not part of the standard operation of a service and which causes or may cause disruption to or a reduction in the quality of services and customer productivity" (OGC, 2007; van Bon et al., 2007).

We use control theory to theorize the relationship between performance goal, action and realized performance. Although control theory is historically used as a mathematical model to explain the behavior of physical systems, the basics can be also applied to human actors (Andrei, 2006; Wiener, 1965). Control theory consists of three fundamental concepts, as shown in Figure 10

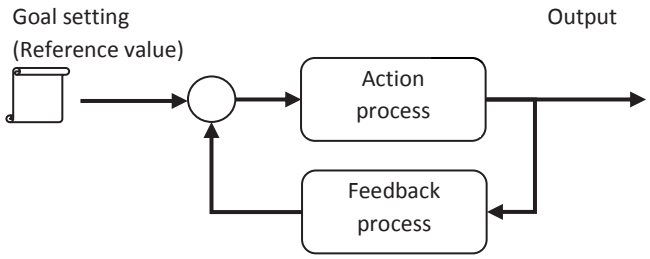

Figure 10, Control theory model

The first fundamental concept is goal setting, which in this case is predefined by the SLA for the service-team. The members of IT service-teams take action to achieve the incident handling goals. The second concept of control theory is feedback. Feedback enables the IT service-team members to know the realized performance. The third concept is the comparison function that compares the realized performance and the set goal. The difference between the two values is fed into the action process initiating (adapted) action to reach the goal.

The time between a change in output of the comparison function and the response of this change fed back into the comparison function is the time constant of the feedback loop. This time constant characterizes the response time of a system (Andrei, 2006).

The constellation of staff in a service-team that controls IT incident handling is abstracted with social network theory. Social networks are defined as nodes with links to other nodes (Freeman, 1979). In our case the nodes are human actors. A service-team is a group of linked nodes, forming a micro-level network, as shown in Figure 11.

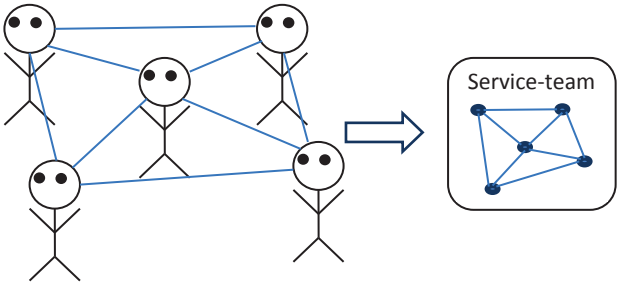

Figure 11, Linked human actors in a service-team

A node from a micro-level network can also be linked to a node of another micro-level network. These connections form meso-level links as shown in Figure 11. IT incident information is exchanged between nodes in different service-teams through the meso-

level links. The information included in recorded incidents is exchanged via the ITSM-application. Additional information is be shared via telephone and email.

A notably meso-level link between nodes is the action of one node to influence incident handling performance of another service-team. For instance service-team B appeals to supplying service-team A to speed up handling of an incident so that the incident is resolved within the SLA constraints of service-team B.

The links (see Figure 12) at the micro-level and meso-level are used for hypothesis building further in this section.

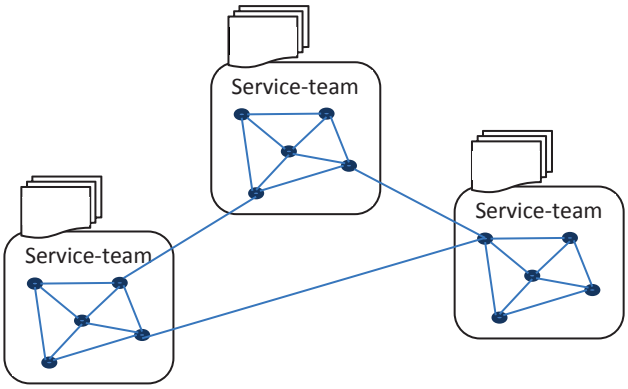

Figure 12, Linked service-teams

The visibility of agreed and realized performance information needs to be high by IT service-team members for effective control in and between service-teams. High visibility enables effective comparison of the agreed and realized value, triggering effective consequential action. High visibility information is indicated with the dashed line in Figure 13.

The supply chain visibility concept is used to measure the visibility of the known information in the control model. Caridi et al. (2010a) use the dimensions accuracy, quantity and freshness to measure visibility. For this research we simplify the visibility measure to the dimensions accuracy and freshness. Accuracy is defined as the knowledge of the node about agreed and realized incident handling performance information. For freshness we use the time constant parameter of control theory.

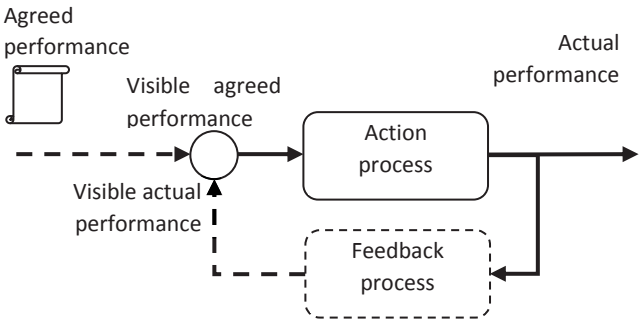

Figure 13, Control theory model augmented with visibility

Based on control theory and social network theory we argue that visibility leads to effective action in service-teams and the utilization of the social network links within and between service-teams to improve incident handling performance.

Visibility of incident handling performance of the own service-team is defined as: own visibility. Visibility of incident handling performance of other service-teams in the meso-level network is defined as: surrounding visibility. The dotted arrows in Figure 14 represent team members that have visibility over agreed and realized incident handling performance of the own and surrounding service-teams. Visibility of agreed incident handling performance helps members to understand their service-team goals and initiate action in the service-team to enable service delivery in accordance with these agreements:

> *[H1] We hypothesize that visibility of agreed incident handling performance values of the service-team positively correlates with incident handling performance of that service-team*

The same line of thought is applied to the visibility of realized performance. Visibility of realized performance metrics allows nodes improve their decision making and define necessary action to handle incidents:

> *[H2] We hypothesize that visibility of realized incident handling performance of the service-team positively correlates with incident handling performance of that service-team.*

Visibility of agreed performance of other service-teams in the meso-level network enables nodes to mitigate differences in agreed service levels. For instance service-team A knows that the agreed service levels of interdependent service-team B are lower than the agreed service-level of the own service-team. Knowing this enables service-team A to take mitigating actions to secure their own service-levels:

[H3] We hypothesize that visibility of agreed incident handling values between service-teams in the meso-level network positively correlates with incident handling performance of the service-team that has that visibility.

In the same line of thought visibility of realized performance values of other service-teams improves the control cycle by enhanced feedback, which improves decision making and action taking.

[H4] We hypothesize that visibility of realized incident handling performance of other service-teams in the meso-level network positively correlates with incident handling performance of the service-team that has that visibility.

If a correlation is found between visibility of realized performance and incident handling performance, it becomes relevant to investigate whether increasing visibility will positively impact performance. By increasing visibility the control cycle is (re)enabled as visibility brings new facts into the team comparison and action process. The control cycle is then utilized to improve incident handling performance. This leads to a fifth hypothesis:

[H5] Visibility based interventions positively impact incident handling performance.

Figure 14 shows the modeled relationship of visibility, performance and the nodes. The nodes have visibility over agreed and realized performance of the own service-team and dependent service-teams. The dotted arrows represent visibility. The arrows have a reference to the hypotheses and an indication of the visibility type (e.g. own surrounding). For instance a node of Service-team C has surrounding visibility over the agreed and realized performance of best-known Service-team A.

The financial institute that was subject to our research has a centralized IT organization of 4,000 fte. The organization is split into IT Service Delivery Centers (SDC). Each SDC delivers predefined IT services to a single internal business partner. An SDC consists of IT service-teams that each deliver technology enabled IT services to groups of end users. Incident handling monitoring and reporting is centralized to a supporting incident management team.

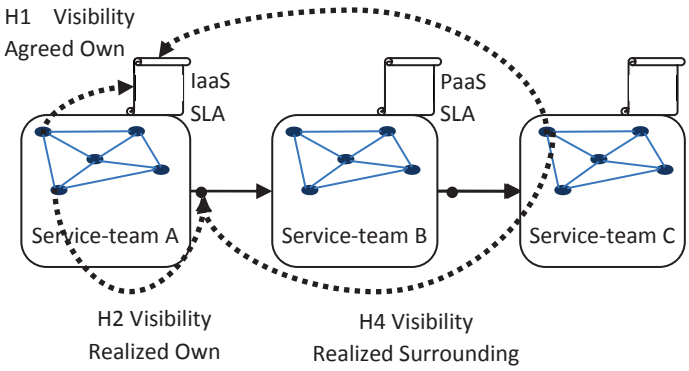

Figure 14, Hypothesized visibility and performance

The IT services of each software service-team are predefined in a service catalog. The service catalog contains a service description of each IT service covering the offered technology and the predefined maximum duration of IT incidents. The service catalog defines four incident priorities each with a maximum duration which is applicable for all service-teams in the SDC. Each incident priority is based on user urgency and business impact. The services to the business partner are formalized with SLA's, based on the service descriptions in the service catalog.

The team manager of a service-team is accountable for the agreed IT service delivery. The team manager takes care of overall team management. Accountability for incident handling performance is delegated to an incident coordinator which is part of the service-team.

An ITSM application is used to record and manage IT incidents between a service-team and the supplying service-teams. Each incident that is recorded in the ITSM application is tagged with an incident priority and a timestamp. Each incident that is solved is tagged with (1) the name of the team that solved the incident and (2) the closing timestamp of the incident.

The incident handling performance of a service-team is monitored by the centralized incident management team. This centralized team uses the ITSM application to generate reports that are monthly sent to the manager of the SDC.

We first tested hypotheses H1 --- H4, using data from a collection of interdependent service-teams. This visibility correlation case study is described in Section 3.4. Next, a second case study was performed to test hypothesis H5, by conducting visibility-based interventions in a single service-team, while measuring the effect thereof on the

performance of the team. The latter case study is described in Section 3.5. Both case studies were done within the same network of service-teams.

The first case-study consists of five phases, as defined by Runeson and Höst (2009): (1) Case study design, (2) preparation for data collection, (3) collecting evidence, (4) analysis of collected data, and (5) reporting. The phases of the second case study also match those defined in Runeson and Höst (2009), albeit that the collection and analysis of data go hand in hand in the latter, and are grouped under "interventions and data collecting". The case study design of both studies is defined in this section, while the other phases are discussed in Sections 3.4 and 3.5, respectively.

3.4 Visibility Correlation Case Study

3.4.1 Preparation for data collection

In the first stage one software service (SaaS) is selected, based on archival record study and interviews with involved management staff. Selection criteria are: (1) the services of all interdependent service-teams are clearly defined, (2) the incident definitions (e.g. priorities) are the same for all service-teams and (3) one ITSM repository is used in all service-teams. Criteria (2) and (3) are chosen to ease the subsequent analysis. After the selection, the meso-level network is analyzed and modeled, based on the SLAs and technical dependencies between the service-teams.

The meso-level network selected consists of seven service-teams, shown in Figure 15. The service-teams are distributed over the SaaS, Paas and IaaS layers. The links in Figure 15 illustrate the chains of delivery. The numbers between brackets show the number of team members of each service-team.

Each service-team in the network delivers services, predefined in a service catalog. The service catalog contains service descriptions of all services in the network, including incident handling and four incident priority definitions. Each incident priority has its maximum duration: 2 hours for priority 1, 8 hours for priority 2, 3 business days for priority 3 and 10 business days for priority 4 incidents, regardless of the interdependencies between the IT service-teams.

The SLAs contain the predefined services that are agreed between the layers of service-teams (Hiles, 2002). For instance, the Infra Server service-team provides IaaS that is used by the Unix service-team to host a Unix webserver and the hosting platform is used by the SaaS service-team to host the web-enabled financial application. The SaaS service-team delivers the hosted application to the internal business partner.

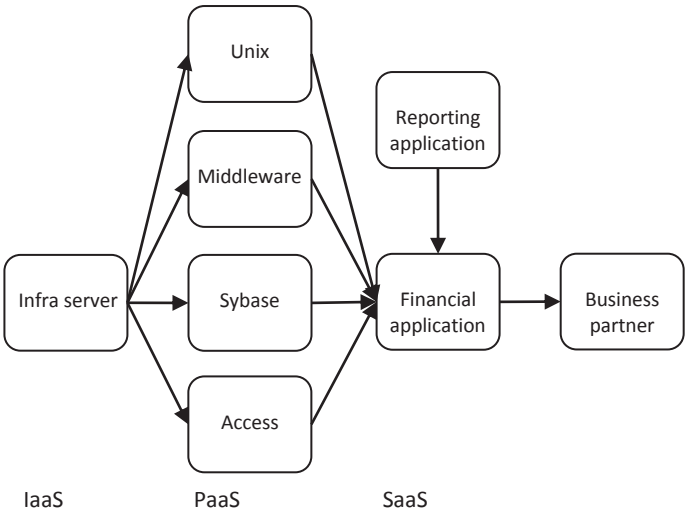

Figure 15, Network constellation of research domain

The network has 107 nodes (team members), distributed over the seven service-teams. Each of the service-teams has a team manager that has accountability for service delivery as agreed in the service catalog and SLAs.

Service level agreements are agreed and documented by a separate contract management team; the service-teams do not have an active role in this. The contract management team is positioned in a separate branch in the organizational structure and is located at another geographical location. This incurs the risk that agreed upon service levels are known to members of the contract management team and not to members of the service-teams.

Incident registration as result of user phone calls is performed by an outsourced helpdesk. The helpdesk handles phone calls, registers the incident in an ITSM-application and routes them to the applicable service-team. Service-team staff uses the ITSM-application to pick the high ranking incidents from the backlog.

Correct usage of the ITSM-application and recorded data is monitored by incident managers. These incident managers are part of a separate incident management team located in a separate hierarchical branch. The centralized incident management team distributes incident management reports to the team managers of the service-teams on a monthly basis. The fact that a helpdesk takes care of customer interaction and incidents are monitored by a centralized team may negatively impact performance visibility.

3.4.2 Collecting evidence

Quantitative data about the agreed service levels are extracted from the service catalog and SLAs. Data about the incident handling performance of the last six months are collected from the ITSM repository. The data are collected one month after the survey is completed to be able to measure the effect of visibility on performance. We performed a walkthrough of the data and cross month data check for consistency purposes. To prevent validity issues we used the raw dataset without a data cleanup.

We collect quantitative data about the existing visibility in the network with a survey as shown in the Appendix. The survey measures the existing knowledge of the agreed and realized performance of nodes. Data is collected for each of the incident priorities.

With a pretest to test the understandability of the questionnaire we found that visibility of surrounding performance was very low. As we need a reasonable level of visibility to enable correlation with incident handling performance we limited the measurement of surrounding visibility to that of the best known service-team.

The first part of the questionnaire collects the data about visibility of the own service-team. Question 1-4 collect data about the visibility of the agreed incident handling performance of the own service-team. Question 6-9 collect data about the visibility of the realized incident handling performance of the own service-team.

The second part collects the data about visibility of surrounding service-teams in the network. Questions 10-11 collect data about the agreed incident handling performance of the best-known, surrounding service-team. Question 12-16 collect data about realized incident handling performance of the best-known, surrounding service-team.

We aim to measure the factual knowledge of service-team nodes, so we use multiple-choice questions with one correct, four incorrect and a 'don't know' option (questions such as 'do you know?' extract perceptions, not factual knowledge).
The questionnaire includes one open question to collect the respondents' thoughts and comments about the incident handling process, with the aim to enhance our understanding of the answers to the multiple choice questions.

Table 6 summarizes the four visibility measurements, categorized in (1) agreed and realized service levels and (2) visibility of the own and best known surrounding service-team.

Table 6, Used variables for performance visibility measurement

Visibility	Agreed	Realized
Own service-team	Agreed service levels of the own service-team	Realized average incident handling duration of the own service-team.
Best known service-team	Agreed service levels between the own team and the best known service-team.	Realized average incident handling between the own team and the best known service-team.

Performance data was collected in October. The survey was conducted from the third week of September to the second week of October. The survey covered all 107 nodes in the network and resulted in 92 responses.

All performance and visibility variables used in this case study are listed in Table 7, together with the corresponding metrics. The same set of variables is used in the second case study, reported in section 3.5. All these variables have an implicit variable denoting the team. That is, they are computed for each team separately.

Table 7, Definition of variables and their metrics

Variable	Definition	Formula
t	time of survey	
m	Month (-4, -3, -2, -1, 0, 1)	
p	Priority (1, 2, 3, 4)	
n	Incident number n	
P(n)	P = 1 (incident n solved in SLA time); P = 0 (incident n not solved in SLA time)	
N	Total number of incidents for one priority	
P(p, m)	Average performance for priority p incidents in month m	$\mathrm{P(p,m)} = \sum_{n=1}^{N} \frac{P(p,m,n)}{N}$
r	Respondent number r	
R	Total number of respondents	
VA(r)	V=1 (answer of the respondent correspond with SLA performance variable); V=0 (answer of the respondent does not correspond SLA performance variable)	
VAO(p)	Average visibility of all respondents on the agreed performance of the own service-team for incident priority p	$\mathrm{VAO(p)} = \sum_{r=1}^{R} \frac{VA(p,r)}{N}$
VAS(p)	Average visibility of all respondents on the agreed performance of the best known service-team for incident priority p	$\mathrm{VAS(p)} = \sum_{r=1}^{R} \frac{VA(p,r)}{N}$
VR(r,m)	V=1 (answer of the respondent correspond with realized performance variable); V=0 (answer of the respondent does not correspond realized performance variable)	
VRO(p,m)	Average visibility of all respondents on the realized performance of the own service-team in month m for incident priority p	$\mathrm{VRO(p)} = \sum_{r=1}^{R} \frac{VR(p,m,r)}{N}$
VRS(p,m)	Average visibility of all respondents on the agreed performance of the best known service-team in month m for incident priority p	$\mathrm{VRS(p)} = \sum_{r=1}^{R} \frac{VR(p,m,r)}{N}$

3.4.3 Analysis of collected data

Table 8 shows the number of handled incidents in the months May (t-4) to October (t+1).

Table 8, Number of incidents per month

Service-team	May	Jun	Jul	Aug	Sep	Oct	Total
Infra Server	626	673	579	494	607	592	3571
Middleware	25	32	16	24	32	34	163
Financial application		112	171	24	65	46	418
Reporting app	119	15	58	72	58	162	484
Sybase	21	26	766	703	628	777	2921
Unix	905	1022	1005	747	743	835	5257
Access	450	36	878	784	923	908	3979
Total	2146	1916	3473	2848	3056	3354	16793

The duration of each incident is determined by comparing the registration timestamp and the resolving timestamp. This duration is then compared with the predefined maximum duration of that incident, to determine whether the incident was solved in time. The maximum duration is, for each incident priority, predefined in the service catalog.

Incident handling performance of a service-team is defined as the percentage of incidents solved in time. This percentage is determined for each priority, for each month separately. Variable $P_{(p,m)}$ represents the incident handling performance, where *p* is the priority and *m* is the month.

The performance data of October $P_{(p,t+1)}$ is used for the correlation analysis. Table 9 shows the incident handling performance in October for each incident priority for each service-team.

Table 9 shows for instance that Infra Server service-team (delivering infrastructure as a service), has a weighted average incident handling performance of 0.85 in October, which implies that 85% of the 592 recorded incidents have been handled within the agreed service-levels.

Table 9, IT incident handling performance $PR_{(p,t+1)}$

Service-team	1	2	3	4	Total
Infra Server	0.50	0.51	0.92	0.64	0.85
Middleware		0.40	0.71	1.00	0.68
Financial application		0.00	0.57	1.00	0.54
Reporting app				0.97	0.97
Sybase	0.67	0.46	0.87	0.74	0.85
Unix	0.50	0.60	0.90	0.76	0.87
Access	0.00	0.17	0.10	0.18	0.11
Total	0.36	0.50	0.67	0.71	0.66

The empty cells imply that not all service-teams recorded priority 1, 2 or 3 incidents that month. We validated the missing figures with respondents. The respondents explained that staff tends to spend time on resolving incidents, rather than logging them. This is particularly applicable to priority 1 incidents as they need to be solved in 2 hours.

Incident handling performance of low priority incidents (prio 4) is higher than high priority (prio 1) incidents. Probable causes are (1) the lack of knowledge about the agreed incident handling duration, (2) the inability to handle priority 1 incidents in 2 hours and (3) the lack of logging all priority 1 incidents. Additional research is required to determine the actual cause(s).

The table shows that 66% of the incidents in the network were handled within the SLA in October. Notable is the bad performance of the Access service-team, while performance of the other teams was rather high.

Visibility of agreed incident handling performance is determined for each incident priority, by comparing each answer to the questionnaire with the applicable value in the service catalog. The visibility of own agreed incident handling performance in the service-team is defined as the percentage of nodes that correctly answered the question. Variable $VAO_{(p)}$ represents the average Visibility of the Agreed incident handling performance of the Own service-team. The variable *p* represents the priority, as the visibility is determined for each priority separately.

Visibility of realized incident handling performance is determined for each incident priority, by comparing the answers of the questionnaire with the applicable realized incident handling performance value $P_{(p,m)}$, for each of the six months for which data is

collected. Visibility of own realized incident handling performance is defined as the percentage of nodes that correctly answered the question for month *m*.

Variable $VRO_{(p,m)}$ represents the average Visibility of Realized incident handling performance of the Own service-team, for each of the six months (*m*). The variable *m* runs from four months back in time to one month ahead in time, based on the month of the survey *(m=t-4… t+1; t=0=month of survey)*.

Visibility of agreed incident handling performance of the best known service-team by a node is evaluated in the same way as for the own service-team. Naturally the agreed and realized levels of the best known service-team are used, instead of the agreed and realized levels of the own service-team. The variable $VAS_{(p)}$ represents the average agreed visibility of the best-known service-team. The variable $VRS_{(p,m)}$ represents the average realized visibility of the best-known service-team.

The correlation between visibility and incident handling performance is evaluated with Pearson correlation analysis as the first analysis showed a linear relationship between performance and visibility.

For performance we use the performance figure $P_{(p,t+1)}$ that is one month after closure of the survey *(m=t+1)*. This performance figure is used to assess the impact of visibility on incident handling performance.

The correlation is first performed for each of the six *(m = t-4 … t+1)* visibility datasets $VRO_{(p,m)}$ and $VRS_{(p,m)}$ to determine the dataset that has the highest correlation with performance $P_{(p,t+1)}$. The visibility dataset with the highest correlation is used to determine the time constant of the feedback loop, the freshness of the information.

The correlation analysis showed that a significant correlation existed between the performance dataset of October and the average of the visibility datasets of August and September. Visibility datasets of prior months did not result in a significant correlation.
The visibility results of Figure 16 are therefore based on the performance datasets of August and September.

3.4.4 Reporting

Figure 16 shows the average visibility of agreed own performance (VAO), realized own performance (VRO), average visibility of agreed best-known (surrounding) performance (VAS) and the realized best-known (surrounding) performance (VRS).

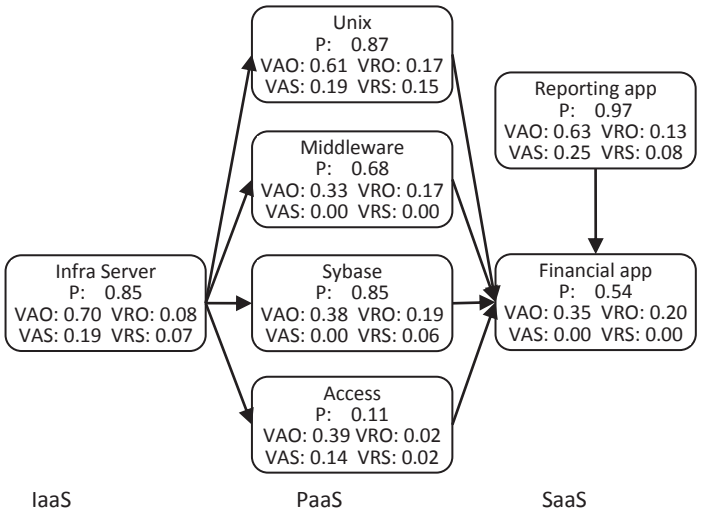

Figure 16, Performance and visibility per service-team

The results in Figure 16 show that the overall VRO is very low and the overall VAO is more than three times higher than VRO. Notable is the Access service-team which has hardly any visibility (0.02) on its own realized performance while the agreed performance is much higher (0.39). This notable difference triggered us to verify the cause: the manager of the team clarified that the team performance suffered from a severe lack of resources due to the implementation of a new policy. As the performance is very low as well (0.11, see Table 9), we suggest that team capacity should be added to the model as presented in the research design (Section 3.3).

The answers to the qualitative question provide additional interesting results. One respondent shares his need for *"a great team of incident-coordinators and a better overview of all incidents including meetings with all coordinators.... just like before"*. This confirms that incident coordinators have a lack of visibility over incidents.

The results in Figure 16 show that best-known (surrounding) visibility hardly exists. Three service-teams have no best-known surrounding visibility at all, not on agreed incident handling performance and not on realized incident handling performance of the best-known service-team.

The results are confirmed by respondents *"the own SLA is already hardly known, not to mention the SLA of another"*. Another respondent explains that *"in long complex chains my experience is that different members of the chain cannot find each other. In these cases incidents take weeks to solve which is very frustrating"*. A third shares *"I*

completely have no idea of SLAs from other departments". Another respondent proposes *"a bi-monthly broadcast in the ITSM-system on individual team performance so that all HPSC users can keep track of performance of the incidents allocated by each team; measures could be in terms of % meeting SLA"*. This confirms that incident handling performance is not visible between teams.

The result of the correlation analysis to determine the time constant implies an information freshness of 1.5 months, as the difference in duration between the average of August and September and October is 1.5 months. As the survey was held from the third week of September to the second week of October, the survey covered the reporting period of September. We reason that not all team members were already informed about the performance of September, being the cause for the high correlation between the performance visibility dataset of August and the performance of October. The results seem to confirm that the monthly incident handling performance report has a positive impact on incident handling performance.

Table 10 shows the Pearson correlation analysis between incident handling performance and the four visibility variables. The significance is given between brackets.
The correlation between own realized visibility VRO and incident handling performance is the highest (0.56) with a high significance ($p<0.01$). The correlation between P and VAO is not significant.
The correlation between P and VAS is not significant and the correlation is low (0.13). The correlation between P and VRS is significant at the $p<0.05$ level, which is caused by service-teams that handle incidents quite well and have zero visibility on surrounding nodes, as shown in Figure 17.

Table 10, Correlation matrix of performance and visibility

	P	VAO	VRO	VAS	VRS
P	1.00				
VAO	0.10 (0.33)	1.00			
VRO	0.56 (0.00)	-0.22 (0.13)	1.00		
VAS	0.13 (0.28)	0.45 (0.01)	-0.06 (0.40)	1.00	
VRS	0.41 (0.03)	0.12 (0.27)	0.43 (0.01)	0.43 (0.01)	1.00

High performance seems to be possible without any surrounding visibility. Nevertheless visibility seems to contribute to performance as the non-zero visibility values correlate with incident handling performance. Additional research is required to determine the underlying causes.

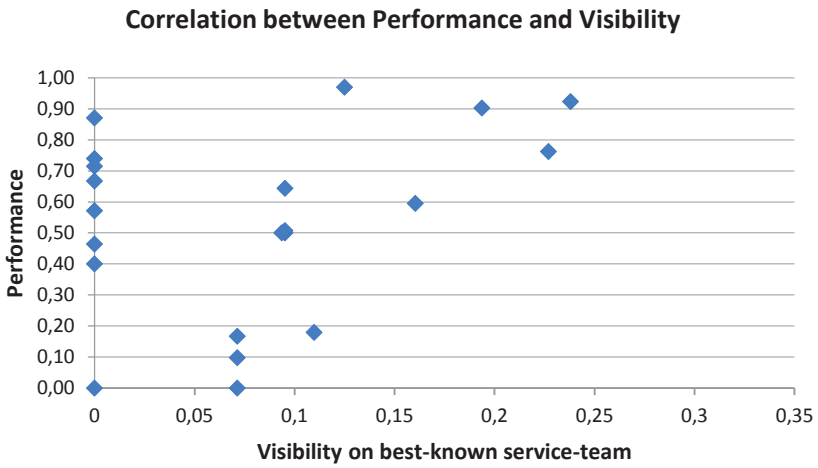

Figure 17, Performance and surrounding visibility

3.5 Visibility Intervention Case Study

3.5.1 Preparation for data collection

As service-team we selected the team that delivers the IT service to the business partner, as this team is has, direct and indirect, interdependencies with all other service-teams in the network (the team labeled "Financial application" in Figure 15). This team also complied with the criteria from Table 11.

Visibility of service-team performance is measured with the first part of the questionnaire as included in the Appendix, and archival record study. The survey measures visibility of agreed and realized service-levels. The answers of each of the respondents are compared with the average realized performance of the last two months. Each answer is scored correct (1) or incorrect (0). Performance visibility of the service-team is evaluated as the average of the scores of all respondents. The pre-condition of the team needs to be set to be able to test the hypothesis. The researcher is involved in setting the preconditions. Table 12 shows the pre-conditions and their rationale.

Table 11, Research service-team criteria

Team criterion	Rationale
Team member cross-location	Cross-location implies limited possibilities for face to face contact and reliance on email, and conference call contact, enabling us to track (the effect of) the interventions.
Service-chain	The service-team is part of a service-chain having interdependencies with other teams.
Accepted services	The agreed services include incident handling used for objective setting.
ITSM application	The team uses an ITSM application to enable measurement and reporting of team performance.
Communicate via email and conference	The team is familiar with email and conference call communication, which implies their usage for the interventions.
Low visibility	Low performance visibility allows us to conduct visibility based interventions and measure their impact on incident handling performance.
Low performance	Low performance allows enhancing service-team performance.

Table 12, Setting service-team pre-conditions

Team condition	Rationale
Objectives	Incident handling objectives are shared to set the reference level for the control cycle. Without set objectives the team members do not understand the objectives and cannot work towards these objectives
ITSM application configuration	The application is preconfigured, such as team names and incident priority definition to ensure that the ITSM application can be used effectively for tracking incident handling performance.
Reporting preparation	The central team of incident managers compiles clear incident handling performance reports. Clear incident handling reports are required to maximize possible effects of the interventions.
Incident coordinator	The incident coordinator role and name is communicated by the team manager. This is required to make team members aware of the role and responsibilities and understand the actions of the incident coordinator.

To measure incident handling performance the duration of each incident is compared with the maximum agreed duration, based on the service catalog and the SLA. The incident duration is defined as the difference between the incident registration and the incident closure timestamp. Incident handling performance of the service-team is determined by the percentage of incidents that have been closed within the maximum agreed duration.

For the measurement of the incident handling performance all incidents that are *controlled* by the software service-team are included. Controlled implies that the team is accountable for handling the incident in time, even when the incident is assigned to a supplying service-team. This is different from the notion of incident handling performance in the first case study, where we only count the incidents actually handled by the team.

Performance data is collected from the ITSM-application. The data collection includes the following information:

- Incident registration timestamp
- Incident closing timestamp
- Priority of the incident
- Service-team that controlled and monitored handling of the incident
- Service-team that solved the incident

Visibility based interventions are used to change the team perception about the realized incident handling performance. The interventions are conducted by the central incident management team by making the realized incident handling performance visible by means of incident handling reports. The report contains, for each incident priority, the total number of incidents and the number of incidents not handled within the SLA (breached); see Table 13 and Figure 18.

Table 13, Sample performance report

Priority	Within time	SLA Breached	Total	Performance (%)	Average duration
1	7	2	9	77	1.2h
2	30	15	45	67	6.7h
3	100	20	120	83	2.8 days
4	45	7	52	86	18 days

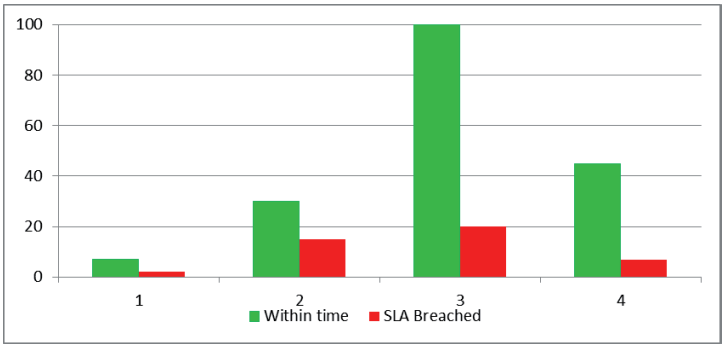

Figure 18, Performance per incident priority

The reporting frequency is increased from monthly to weekly and further increased to a maximum of daily depending on the performance improvement effects. The reporting intensification aims to increasingly challenge the existing incident handling performance perception. The reports are shared with the team manager, the incident coordinator and the other members of the service-team.

Weekly conference calls are held. Participants are the incident coordinator, the centralized incident monitoring representative, the researcher and optionally the team manager. The meetings have a prepared agenda. The topics and agreed actions are recorded in the minutes of the meeting which are distributed to the participants.

During the actual visibility based interventions the IT service-team and the centralized incident management team interact independent from the researcher, notwithstanding that the researcher receives carbon copies of emails. Furthermore the researcher is involved in the weekly progress meetings and if required compiles the minutes to ensure the improvement actions are well recorded. The researcher does not have a further role, such as managing actions to closure.

The empirical research for the second case study started right after the first case study ended, in November, and lasted till October the next year. At the start of the intervention period (November) the team had a performance of <10%, agreed performance visibility of 35% and realized performance visibility of 10%.

Archival email records showed that IT service-team members were informed about the agreed service levels in the service catalog (earlier in the year), as shown in the following snippet[1]:

> *"Main topic of the meeting was to discuss the current SLA and determine to what degree the SLA actually fits current practice and processes. It has been agreed to take more time to study the SLA, Service Catalogue and other relevant documentation in order to be able to define detailed questions which also will be discussed in the light of incident management in a separate meeting with << incident coordinator of the central team>>".*

This pre-condition has therefore been met although the overall knowledge was still quite low.

[1] The italic texts between quotes are the recorded texts in the email communication system. This email system was used for daily ad hoc communication by the involved staff next to the ITSM application. For confidentiality reasons, the actual names of persons are replaced by their roles, put between << and >>.

The second pre-condition, the ITSM application configuration, was also achieved earlier in the year. The application was able to support incident registration, prioritization, control and assignment. The remaining pre-condition were set between November and March of the next year. The third pre-condition was achieved by the centralized incident management team, with the realization of basic incident management reports as shown in the following email:

> *"The reporting instruments have been configured in <<ITSM application>>. Basic reports are now possible, with color codes Green = SLA met, Yellow = SLA in danger, Red = SLA breached.*
> *Everything should be now in place to perform your role as incident coordinator".*

The fourth pre-condition was achieved by assigning the incident coordinator in the service-team. Activation of the role was stimulated by communicating the incident coordinator name to all stakeholders. The incident coordinator was also invited in the weekly conference calls.

3.5.2 Interventions and data collecting

Visibility interventions were performed between March and September.
The incident management reports were provided by the central incident management team on a periodic basis as shown in the following quote:

> *"Please be informed of the periodic progress update: Link or see pics below. Remarks: Limited progress noticeable (1% p/day). Please provide your input how things can be improved and/or let us know what obstacles you encounter(ed)".*

The first reports showed that the number of registered incidents was very low. Reporting the results to clients of the IT service resulted in questions from clients about the number of reported incidents:

> *"We receive questions from <client> about the usage of the ITSM application by the service-team. There seem to be only a few incidents logged".*

This quote shows that staff in the vicinity of the service-team starts to ask critical questions about the low number of incidents after the first report was published. These questions subsequently induced improvement actions within the team.

The resulting analysis showed that a secondary incident backlog was in use, invisible to the environment. This triggered the decision to merge the secondary backlog in the central ITSM application, which resulted in a significant increase of registered incidents in the next months.

The report also triggered action with regard to the role description and reporting line of the incident coordinator. The role description turned out to be in conflict with incident coordinator tasks given by the hierarchical manager. The incident coordinator was discharged from these tasks:

> *"<< Resource manager >> has confirmed that the incident coordinator activities are managed by << functional manager >>. << Resource manager >> will not have an operational role. << Resource manager >> will only take care of the HR-performance cycle based on the input from the << functional manager >>.*

The discharge of these tasks provided a clear set of incident coordinator tasks and a clear reporting line to the functional service-team manager.
Closing the secondary backlog and the discharge of tasks are examples of discontinuous change that broke the inert state and enabled the team to improve incident handling performance.

At a later stage the reporting frequency was increased to weekly and at specific moments even to daily:

> *"For the progress meeting of today herewith the update to reflect the development since yesterday: the number of open tickets increased by 34, the number of close to breach tickets increased from 19 to 23, the number of breached tickets increased from 28 to 29".*

The high frequency of the information, thus high visibility, helped the service-team to recognize the relationship between the incident handling actions of the team members and the incident handling performance of the team.

To enhance understanding of the performance values the full list of incidents was shared next to the incident reports:

> *"As discussed I hereby send you a complete list of all open incidents of the << service-team >> … judging by the contents I see lots of incidents which are no longer an issue/have been fixed. In comparison, << another service-team >> currently has 12 open incidents".*

Detailed information in addition to the standard incident handling reports helped to determine the actions to improve incident handling performance.
The following quote from an email sent by the incident coordinator shows the role of visibility in the mental comparison function of the incident coordinator:

> *"Currently there are 261 open incident registrations for << service-team >>, which is >100% growth in 10 days … What's wrong?".*

This resulted in an analysis to find the causes of the increased number of open incidents. The analysis showed that the queue was not effectively managed:

> *"…to get in control of the backlog the remaining action is to … close/transfer last << old >> 44 incidents in the ITSM application".*

Some of the incidents had a logging date older than a year. The incident coordinator therefore actively chased team members to close the incident in the ITSM application after resolving the IT incident:

> *"… please have a serious go at cleaning up the queue. We should be moving towards increased working from ITSM application and to keep our assignment group clean (i.e. housekeeping) is an important aspect of working well".*

To evaluate incident handling performance and to determine the appropriate action a weekly conference call was held. The meeting was prepared through the distribution of the latest incident management report and the meeting agenda. The meeting results and agreed actions were recorded in minutes and shared with the participants and related stakeholders. Additional stakeholders were added to the distribution list at a later stage to increase visibility of the actions. These stakeholders also received the incident handling reports.

The meeting supported the performance improvements in two ways. First the meeting stimulated the members to compare the incident handling reports with the performance targets and to define improvement actions. Second the distributed minutes engaged additional stakeholders to support the improvement actions.

At the start of the intervention period the incident coordinator executed his role in an reactive way. However after four months of high visibility the incident coordinator executed the role very proactively. The incident coordinator made an inventory of service-team staff that was involved in incident handling activities and sent an instruction to the involved staff. This instruction clarified how to record, prioritize, select, solve and close incidents. The incident coordinator also communicated actively to the involved staff and the stakeholders to handle recorded incidents. Furthermore the incident manager took care of the decommissioning of the secondary backlog and the migration of the incidents to the primary backlog.

The incident coordinator also started to proactively request incident reports to enhance understanding of the incident handling process:

> *"… could you << the central incident management team >> please provide a weekly (probably Monday) copy of the ITSM application reporting for the << service-team >> to me?".*

The results show the importance of visibility in the control cycle. We noticed that motivation and ability also play a role in the control cycle. Motivation determines whether actual action is initiated to move closer to the goal and ability determines the effectiveness of these actions. Incident management reporting was effective only when the report content was accepted by involved staff and staff was able to execute the improvement actions. We concluded that the central incident management team was, organization wise, too far departed from the service-team to effectively manage incident handling. Centralizing incident management to a separate incident management team might remove essential management control causing low incident handling performance.

3.5.3 Reporting

With the above visibility interventions and the consequential social responses performance started to increase, which was noticed by the stakeholders of the service-team:

> *"Good to see the ITSM application has been configured …".*
> *"Good to see things move to the right direction (In all honesty though, the credit is not mine)…".*

The number of tickets dropped between July and August because of a bulk closure:

> *"Bulk closure of tickets was processed this morning. As a result the open tickets reduced from 300+ to 120".*

The bulk closure involved old already resolved incidents that were not closed in the ITSM application. The bulk closure was performed by the central incident management team, in close cooperation with the incident coordinator.
From that moment the number of incidents started to decrease since the service-team started to discover causes of recurring incidents:

> *"…we please ask the help of << member1 >> and/or << member2 >> to assist us in reducing the number of calls".*

This led to less time spent on phone calls and more time spent on resolving remaining incidents, which further increased incident handling performance.

In September the number of new incidents and closed incidents became in balance, implying that the amount of closed existing incidents equaled the recorded new incidents:

> *"Below the update regarding << service-team >> queue. Looks like ticket 'growth' and closure are in balance. Let us agree on goal to reduce backlog before end this week so you/colleagues 'only' face the task to resolve/close the tickets logged per day (between 10-30)".*

The result of the incident performance development of the service-team is shown in Figure 19. The research started in November which is 0 on the x-axis.

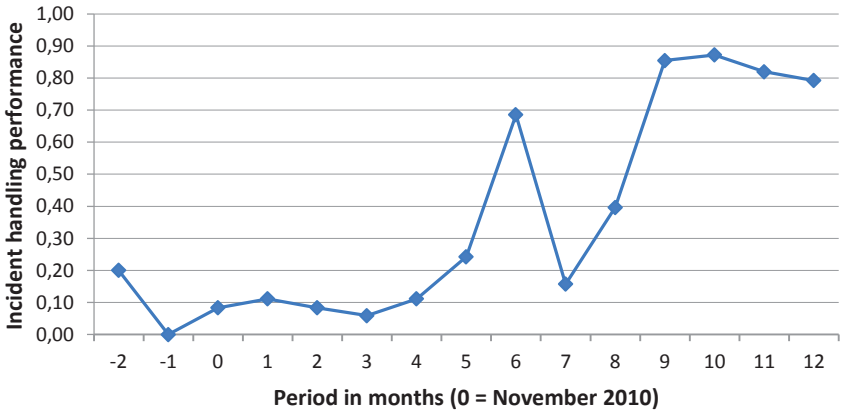

Figure 19, Incident handling performance trend

During the research period, performance increased from below 10% to almost 90% and seems to stabilize at approximately 80% (see Figure 19). The drop in performance between April and May was caused by decreased attention after the initial performance improvement. The performance drop was caused by a lack of closure actions, which was corrected by the bulk closure. After the initial drop the performance increased to the new stable state.

The central incident management team distributed the following text by email:

> *"With these results the team has become an example for other teams. We thank everybody that contributed to achieve this result".*

Figure 20 shows the amount of registered incidents for each month. The figure shows that the low performance was initially caused by a lack of registered incidents in the

ITSM application. Once the visibility increased the number of registrations started to increase, enabling the control cycle.

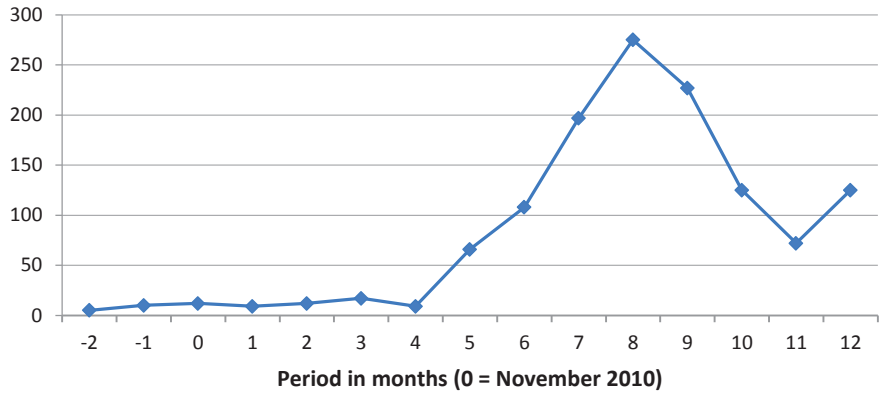

Figure 20, Number of recorded incidents in each month

3.6 Research validity

In this section we discuss the validity of the research. We discuss construct validity, internal validity, external validity and reliability.

3.6.1 Construct validity

During network mapping we validated that the services of the service-teams were defined in the service catalog. We also verified whether the same definitions of incident priorities were used within the full meso-level network. We included a question to verify the involvement of nodes in incident handling to increase population validity.

Understandability of the questionnaire was pre-tested on a service-team of another network, which led to changes in the formulation of questions. The pretest confirmed that visibility of service-team in the network was rather low which led to the decision to only measure visibility of the best-known surrounding service-team.

Archival records were used to triangulate data analysis. A second researcher participated in data analysis to minimize researcher bias. The data collected by the central incident management team to compile the incident handling reports was sample wise verified by the researcher. The visibility based interventions were conducted by the central incident management team to reduce researcher bias.

Construct validity of visibility is limited to the agreed and realized incident handling performance information. Other information, for instance resource capacity planning and service architectures, may also benefit incident handling performance. Another limitation of the construct is the dependency on logged performance information. We used an ITSM repository while some staff members mentioned that not every incident is logged.

3.6.2 Internal validity

The hypotheses with the related variables are built from supply chain management and control theory and subsequently empirically tested. The first study limits the test to correlation analysis. The actual causality of visibility is tested and confirmed in the intervention case study.

The measured visibility of each respondent is limited to the best-known surrounding service-team, which is a rather limited view of incident handling performance of surrounding service-teams. The limited measurement implies that the sum of surrounding visibility on other nodes might be larger than the visibility on the best-known service-team.

3.6.3 External validity

A limitation of the research is the coverage of only one service network in the financial industry. To increase external validity, the research needs to be repeated in other service networks.

3.6.4 Reliability

The researchers have taken several measures to enhance research rigor as explained in the research design. Nevertheless, a researcher bias might be introduced while performing visibility interventions.

3.7 Conclusion

We have empirically researched the relationship between visibility and incident handling performance. Based on existing related literature we built five hypotheses to verify the relationship:

> *[H1] We hypothesize that visibility of agreed incident handling performance values of the service-team positively correlates with incident handling performance of that service-team.*

[H2] We hypothesize that visibility of realized incident handling performance of the service-team positively correlates with incident handling performance of that service-team.

[H3] We hypothesize that visibility of agreed incident handling values between service-teams in the meso-level network positively correlates with incident handling performance of the service-team that has that visibility.

[H4] We hypothesize that visibility of realized incident handling performance of other service-teams in the meso-level network positively correlates with incident handling performance of the service-team that has that visibility.

[H5] Visibility based interventions positively impact incident handling performance.

To verify the first four hypotheses we performed empirical research at seven interdependent service-teams of an internal IT organization of a multinational financial institute.

The results show a significant relationship ($p<0.01$) between realized performance visibility of the own service-team and performance of that service-team in the following 1.5 month, so hypothesis 2 is supported. Visibility of realized incident handling performance seems indeed to influence service-team performance. As the own visibility is low (VRO = 14%) it suggests that enhancing VRO will improve incident handling performance.

The results do not show a significant correlation between agreed visibility and incident handling performance, so hypothesis 1 is not supported.

Surrounding visibility hardly exists; visibility of performance agreements of the best-known service-team is only 11% and realized performance even lower: 5%. This implies that only 5% of the given answers are correct. Given these low levels of visibility we were not able to confirm hypotheses 3 and 4.

Hypothesis 5 was empirically tested, and confirmed, in a subsequent case study within the same environment. This research shows that visibility based interventions can be a useful instrument for performance oriented improvements. In the end state the team actively manages the incident backlog to achieve high levels of incident handling performance. The results indicate that a more prominent role of visibility might benefit performance improvements initiatives.

3.7.1 Future work

Our study is a starting point and one of the future research opportunities is a follow-up study that includes a more detailed analysis, such as correlations per team and incident priority.

Another opportunity is to research the impact of ITSM-applications on visibility and performance.. Research in this area may gain understanding about the impact of ITSM-applications.

We also advocate supplementing the model with capacity. Staff may be unable to improve incident handling performance, due to a lack of staff and/or skills, as was found in the Access service-team. Another research avenue is to study which visible information has the most effect on incident handling performance. This is reported in (Vlietland & van Vliet, 2014c). One type of information might for instance be a dashboard that shows the overall network of interdependent service-teams with existing performance, utilization of resources and planned changes. A fourth research opportunity is to study the impact of information visibility on the performance of development teams.

3.8 Appendix

The appendix contains the questionnaire that was used to survey the visibility.

3.8.1 Part 1.1: Agreed performance of your own group/department

- What (do you think) is the agreed maximum resolution time of a priority 1 incident for your group? (1 hr, 2 hrs, 4 hrs, 8 hrs, 16 hrs, don't know)
- What (do you think) is the agreed maximum resolution time of a priority 2 incident for your group? (1 bus day, 2 bus days, 3 bus days, 4 bus days, 5 bus days, don't know)
- What (do you think) is the agreed maximum resolution time of a priority 3 incident for your group? (1 bus day, 2 bus days, 3 bus days, 4 bus days, 5 bus days, don't know)
- What (do you think) is the agreed maximum resolution time of a priority 4 incident for your group? (3 bus days, 7 bus days, 10 bus days, 15 bus days, 20 bus days, don't know)
- What has been the average number of incidents per month which you have worked on this year? (0-10, 10-25, 25-100, 100-250, 250+)

3.8.2 Part 1.2: Realized performance of your own group/department

- What (do you think) is the average realized resolution time of a priority 1 incident of yourgroup? (1-4 hrs, 4-8 hrs, 8-16 hrs, 16-32 hrs, more than 32 hrs, don't know)
- What (do you think) is the average realized resolution time of a priority 2 incident of your group? (1-2 bus days, 2-3 bus days, 3-4 bus days, 4-5 bus days, more than 5 bus days, don't know)
- What (do you think) is the average realized resolution time of a priority 3 incident of your group? (1-2 bus days, 2-3 bus days, 3-4 bus days, 4-5 bus days, more than 5 bus days, don't know)
- What (do you think) is the average realized resolution time of a priority 4 incident of your group? (3-5 bus days, 5-10 bus days, 10-15 bus days, 15-20 bus days, more than 20 bus days, don't know)

3.8.3 Part 2.1: Agreed performance of your best known group/department

- Select the department/group for which you know the SLA best (other than your own).
- (Infra Server, Unix, Middleware, Sybase, Access, Reporting App, Financial App)
- Do the agreements (SLAs and OLAs) with that department differ from the agreements with your client? (only 0-20% differ, yes 20-40% differ, yes 40-60% differ, yes 60-80% differ, yes 80-100% differ, don't know)

3.8.4 Part 2.2: Realized performance of your best-known group/department

- What is the average realized resolution time of a priority 1 incident of that group? (1-4 hrs, 4-8 hrs, 8-16 hrs, 16-32 hrs, more than 32 hrs, don't know)
- What is the average realized resolution time of a priority 2 incident of that group? (1-2 bus days, 2-3 bus days, 3-4 bus days, 4-5 bus days, more than 5 bus days, don't know)
- What is the average realized resolution time of a priority 3 incident of that group? (1-2 bus days, 2-3 bus days, 3-4 bus days, 4-5 bus days, more than 5 bus days, don't know)
- What is the average realized resolution time of a priority 4 incident of that group? (3-5 bus days, 5-10 bus days, 10-15 bus days, 15-20 bus days, more than 20 bus days, don't know)
- What do you think is needed to increase the performance of incident handling and IT changes? < open question; free text format >