ITIL Based Service Level Management if SLAs Cover Security

Tomas FEGLAR
International Consultant in Information Systems Research and Architecture
Vondrousova 1199, 163 00 Prague 6, Czech Republic
feglar@centrum.cz

ABSTRACT

Current level of information technology creates new perspectives for more IT service oriented market. Quality of these services requires slightly different approach then was applied for products including software. No IT services are delivered and supported in risk free environment. Risks would be considered consistently with IT services quality gaps from Service Level Management (SLM) perspective. SLM is one of ITIL modules that are widely used within the IT service industry. We identified some weaknesses in how SLM is developed in ITIL environment if service level agreement (SLA) has cover Security.
We argue that in such cases Architecture modeling and risk assessment approach let us effectively control analytical effort that relates to risks identification and understanding. Risk driven countermeasures designed in a next step (Risk treatment) have significant impact to the SLM especially from responsibility perspective.
To demonstrate SLM's importance in real practice we analyze SLA synthesize process in CCI (Cyber Critical Infrastructure) environment.

Keywords: Architecture framework, ITIL, Service level management, Service level agreement, Risk analysis and management, Security, CCI.

1. INTRODUCTION

Proportionally increasing importance of a digital economy more and more IT services become specific products that are sold and purchased. This specificity multiplies in a context of CCI, such as power distribution, water supply, national defense, and emergency services, because these infrastructures are managed over increasingly interconnected electronic networks. Mechanisms behind these specific IT service businesses are mostly intuitive; services are non tangible and their influences on business processes are not clearly understood.
Service level agreements between business process owners or customers and service providers have weaknesses that become visible only when something happened and business process is disrupted.
A lot of effort mostly in the area of risk analysis and risk management was spent to avoid such situations. The problem is that methods used by risk analyst are abstract without clear links to something that is more familiar to customers, service providers and suppliers. It was a challenge for us to develop new methodology – CAF (Component Architecture Framework) that allows overcoming gaps between various perspectives.
This paper describes three concepts that can be developed using CAF and that significantly simplify service level management in situations when SLAs deal with security.
Section 2 describes five service quality gaps as were published by Zeithaml and Bitner [20] and Niessink and Van Vliet [13]. These quality gaps are completed with five risks; it allows us better understanding of environment in which services produced by service provides are delivered to customers who purchase them.
Section 3 describes service delivery as a set of ITIL modules that were developed under leadership of the Central Computer and Telecommunication Agency (CCTA). We enhanced 10 originally developed ITIL modules with additional two – RARM (Risk Analysis and Risk Management) module and SECM (Security Management) module. Such modification allows us better understanding of SLM and RARM process relationships.
Section 4 dives into relationships between SLM and RARM modules. We argue that combined approach using architecture modeling and risk assessment stimulates common understanding of all SLM participants. The result is a comprehensive set of service level agreements that corresponds to responsibilities delegated by service provider to suppliers and to responsibilities of own employees.
To demonstrate SLA criticality in real practice we included additional three sections in our paper.
Section 5 describes hybrid enterprise management and control concept, section 6 comments information security and environmental management standards, and section 7 shows an application of architecture and risk assessment modeling based SLM for CCI protecting.
The conclusion and future work are presented in the section 8.

2. HOW RISKS RELATE TO SERVICE QUALITY GAPS

We start with popular gap model [14] and slightly change it with risks (Fig. 1). Now we can describe quality gaps and risks by the similar way.

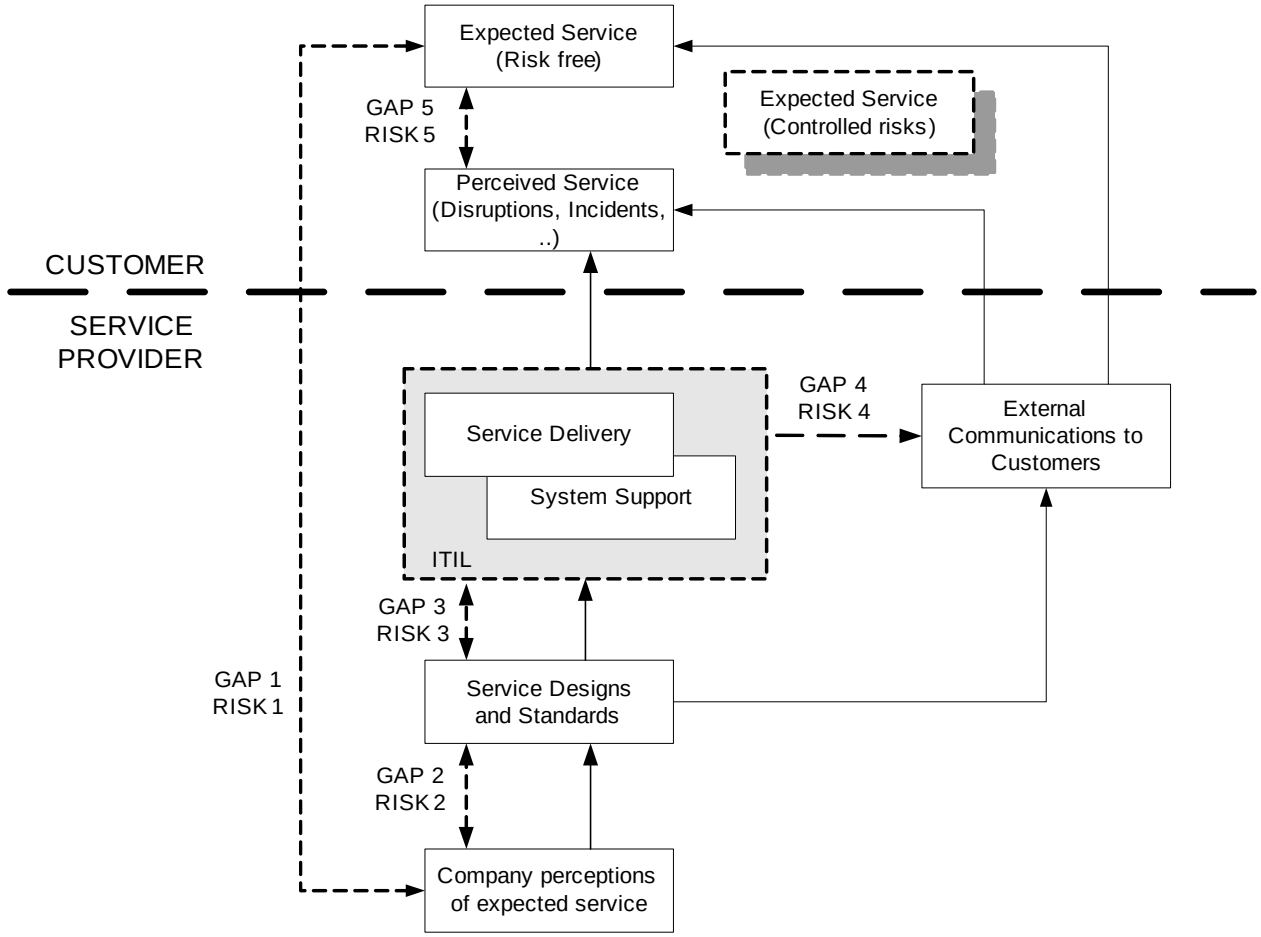

Figure 1: Risk and Service Quality Gaps

The difference between the perceived quality of the service and the expected quality (GAP 5) is a result of four other gaps [20,13]:
GAP 1: The expected service as perceived by the service provider differs from the service as expected by the customer. For example, the service organization aims to satisfy certain availability constrains (e.g. 99% availability), while the actual customer concerns with maximum downtime.
GAP 2: The service specification as used by the service provider differs from the expected service as perceived by the service provider. For example, the customer expects a quick restart of the system, while the standard procedure of the maintenance organization is focused on analyzing the reason for the crash.
GAP3: The actual service delivery differs from the specified services.
For example, customer bypasses the help desk by phoning the maintainer system directly.
GAP 4: Communication about the service does not match the actual service delivery.
For example, a customer is not informed about the repair of a bug he or she reported.

The difference between the perceived risk of the service and the expected risk (RISK 5) is a result of four other risks:
RISK 1: Understanding of impact by service provider differs from customer. Customer usually underestimates dependencies between its business processes and their dependency on IT services.

RISK 2: Caused by a lack of customer-driven security concept, absence of risk assessment method and its regular usage for a periodical risk identification, analysis and evaluation.

RISK 3: Service delivery does not include effective countermeasures that correspond to risks. Some countermeasures are not relevant, some are missing and it's not clear who is responsible for what and what sanctions have to be applied.

RISK 4: Communication by the service provider about its delivered services does not include options that could meet customers' security needs. Cost of these options cannot be compared with customers' impacts (value of business processes) and it negatively influences both sites.
The fifth risk is caused by he four preceding risks. Closing the first four risks we can increase perceived service security (as an service quality enhancement feature), thus bringing the perceived service in line with expected service ("Risk free" property is changed into "Controlled risks").
To close the risks a service provider needs to:

a) Help customer to identify its assets by the way that allows overcoming differences among business process (source of impact assessment), information processes and information technology (RISK 1).
b) Help customer with Security Concept establishment including risk assessment method (RISK 2).

c) Ensure that risk treatment is a part of security concept and allows optimizing countermeasures including clearly specified role based responsibility (RISK 3).
d) Re designing services and modification of SLAs (with customers) and contracts (with suppliers) (RISK4).

3. SLM AND ITIL ENVIRONMENT

IT Infrastructure Library describes a set of well practices organized in modules. The British government through their Central Computer and Telecommunication Agency (CCTA) originally developed them. Five of these modules cover Service Delivery area and other five cover Service Support (Fig. 2). RARM module and SECM module were not developed as separate ITIL modules, but we have included them into our ITIL environment for the following reasons:

– CCTA developed very powerful Risk Analysis and Management Method CRAMM [6] that can be easily integrated into ITIL environment (as a RARM module). Later version of this method was redesigned in accordance with ISO/IEC 17799[1], and BS 7799 Part 2:2002 [2].
– Almost every organization or company maintains information security. Big differences are in how Security Management is applied. SECM module included in our ITIL environment is developed and synchronized with RARM module. Its primary mission is controlling security-operating procedures that relate to System Support.

SLM module [5] helps development relationships between IT Service Section (organization entity responsible for SLM) and end user (customer) and service suppliers and/or maintainers. SLAs relate to users (customers) and describe type of end user services (EUS) delivered to customers and delivery conditions.

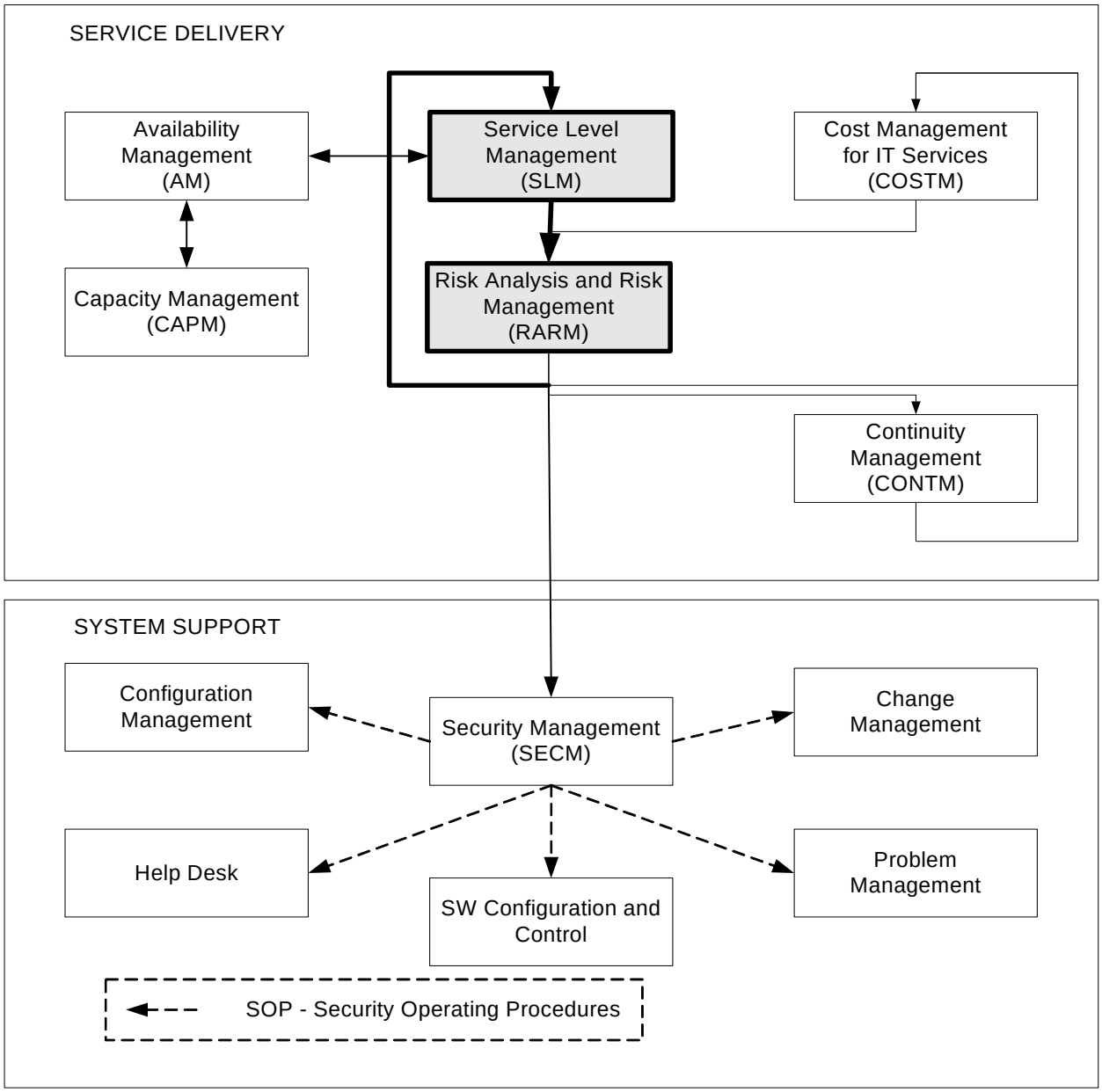

Figure 2: Service Delivery and System Support

Contracts relate to suppliers/maintainers and describe services and/or products needed for EUS delivery. SLA generates requirements to other service delivery modules particularly:

- Availability Management (AM) module [3] covers whole availability lifecycle that has to be established to guarantee SLA availability requirements
- RARM module covers whole risk analysis and management life cycle that has to be established to guarantee SLA security requirements
- Cost Management (COSTM) module [4] allows calculation of incomes (customers payments) versus actual running costs of the IT services

Cost Management development considers additional relationships between ITIL modules:

- EUS delivery infrastructure includes networks (Local, Metropolitan, Wide). Optimal design and planning of this infrastructure significantly influences performance (throughput) / cost ratio. Capacity Management (CAPM) module is responsible for these tasks
- Continuity (Recovery) Management (CONTM) module allows avoiding potential impacts (like loss of revenue, political embarrassment, etc.) of EUS disruptions. CONTM module development uses results of RARM module.

RARM module allows development of security concept on very detailed level. Implementation of such concept through SECM module especially in large organizations requires relatively long time (one year or more in dependency on a security budget).

4. ARCHITECTURE MODELING AND RISK ASSESSMENT

Despite Risk analysis and management process operates with objects – business context, business data, business processes, business applications, business assets [11] - many organizations understand these objects more intuitively then formally. Intuitively based approach isolates risk analysts (responsible for risk assessment) from business owner and information specialist. Risk analysis and management process becomes more tedious, less understandable for businessmen and more expensive.

To avoid these difficulties we developed new methodology – CAF [8] that harmonizes Risk analysis and management process with architecture modeling (Fig. 3). Architecture modeling uses Zachman's architecture framework [19,17].

Six points characterize interaction between both processes. First five points (I1 – I5) deal with synthesis of an Asset Model mapping architecture elements into assets that are familiar to risk analyst. Six's point deals with backward mapping of security operating procedures (generated on the base of identified risks) into "PEOPLE" column of architecture framework with a resolution to a role or a user. Architecture modeling – risk analysis and management interactions can be summarized as follows:

I1 – Impact Assessment controls consistency between Business owner (a person understanding business process), IT staff understanding system process and risk analyst. This assessment is a critical part of assets evaluation step that is a part of risk analysis stage. Our understanding of business influences investigation of an impact from viewpoint of the possible consequences for customers (personal safety, law enforcement, financial loss, commercial and economic interest, international relations, etc.).

I2 - DATA and APPL asset classes correspond to non-tangible assets that relate to system entity and system process. We evaluate both these classes in terms of unavailability (for different timeframes), destruction, disclosure and modification.

I3 - EUS asset class corresponds to functional links that connect source of EUS (site in which application is running) with a point of end user service delivery.

I4 – AC1 – AC3 asset classes correspond to modules and components that are critical for application running and EUS delivery. These classes can include servers, network distributions components (routers, hubs, modems), protocols, etc.

I5 – SITE corresponds to an environment where all modules and components are situated. Fig. 3 illustrates only one such link between AC1 (this asset class represents application server) and a SITE – a place where application server is really placed. We can also change a resolution level (SITE -> BUILDING -> ROOM).

All previous interactions direct from architecture model to risk analysis and management process. It is reasonable to think about opposite direction when we finish with risk analysis (risk treatment) stage.

I6 – A Role and/or a User correspond to responsibility that is one of key results of a risk management. Security Operating Procedures (SOP are synthesized within risk management stage) are assigned to roles (users) in accordance with organization structure. **This process has critical impact to the SLM, particularly:**

- **Suppliers contracts:** SOP responsibilities have to be assigned to external suppliers and maintainers
- **Employment contracts:** SOP responsibilities have to be assigned to employees.

5. HYBRID ENTERPRISE MANAGEMENT AND CONTROL SYSTEMS CONCEPT

Transportation, Water, Emergency Services, Energy, Telecommunication and other sectors mentioned in Presidential Decision Directive 63 (PDD 63) have specific technological infrastructure that includes Cyber Critical Infrastructure (CCI) and technology producing primary products or services (electric power, telecommunication services for example).

The CCI combines three subsystems (Fig. 4):

- Control and Management (CM) sub-system
- Enterprise Information System (EIS) – Strategic Decision and Planning (SDP) sub-system
- EIS – Operational sub-system

CM and EIS Operational sub-systems are distributed across large territory but are functionally coupled with EIS SDP in the Enterprise Management and Control (EMC) node [7].

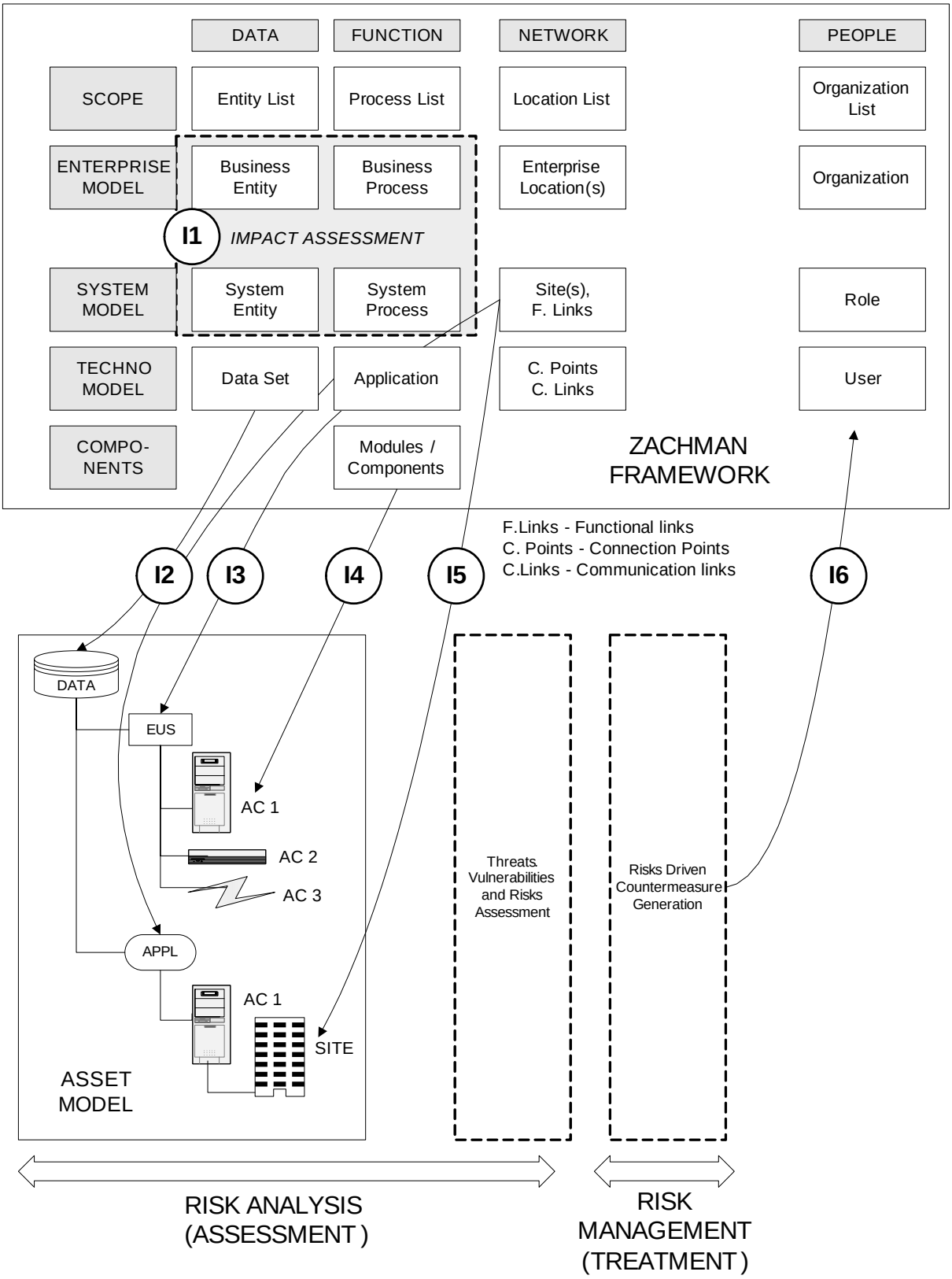

Figure 3: Architecture Modeling and Risk Assessment

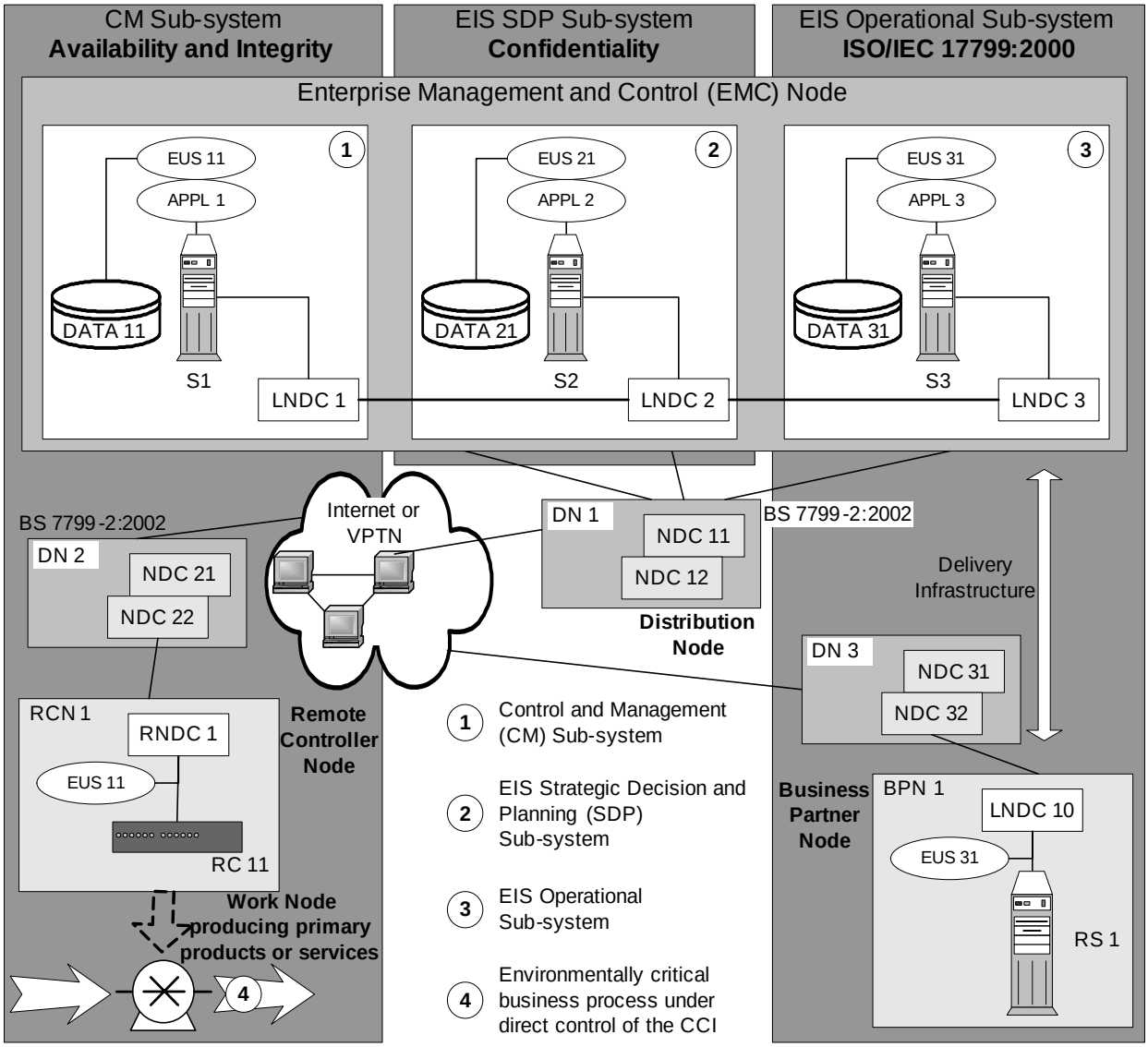

Figure 4: A Hybrid Enterprise Management and Control Systems Concept

CM sub-system consists of:

- Remote Controller Nodes (RCN) that directly control Work Nodes producing primary products or services (air traffic monitoring and control, gas transition and purchasing, radioactive waste processing (in case of the NPS)). Each RCN consists at least from a Remote Controller (RC), a Remote Network Distribution Component (RNDC) and an End User Service (EUS 11) representing a particular functionality managed by a central application (APPL 1).
- Delivery Infrastructure. A part of this infrastructure can be owned and controlled by a company (that provides its key business activities in one of PDD 63 sectors). This part consists of Distribution Nodes (DN); each DN includes at least a couple of Network Distribution Components (NDC) and manages traffic and data flows. NDCs are used in all company's sites that are connected to the Internet. Second part of the Delivery Infrastructure includes Internet or a Virtual Private Telecommunication Network (VPTN); this part is fully transparent for a particular company.
- CM sub-system situated in the EMC node. This sub-system includes running application (APPL 1) with data (DATA 11) that are a source of a particular EUS (EUS 11). A minimal hardware environment includes a Server (S1) and a Local Network Distribution Component (LNDC 1) that connects CM sub-system with DN and with other sub-systems within EMC node.

Work nodes are a part of environmentally critical business process. Well understanding of this criticality is very important for CCI risk analysis and requires special methods allowing explicit description of a criticality in terms of impacts.

EIS Operational sub-system manages supporting activities in which Business to Business transactions become more and more important. This sub-system consists of:

- The Operational part situated in the EMC node. This part includes running application and data (APPL 3 and DATA 3) that produce End User Service (EUS 31). A minimal hardware environment includes a Server (S3) and a LNDC 3.

– Delivery Infrastructure. It is the same infrastructure that is used as a part of the CM sub-system.
– Business Partners Nodes (BPN). These nodes run a particular EUS (EUS 31) that is functionally synchronized with the application running at the EMC node (APPL 3). A minimal hardware environment includes a Remote Server (RS) and LNDC (LNDC 10).

EIS SDP sub-system uses information from other two subsystems and transforms them into a form suitable for strategic decisions. Application (APPL 2) and data part (DATA 21) of this system differs from CM and Control sub-systems and uses On-Line Analytic Processing (OLAP) instead of On-Line Transaction Processing (OLTP). EUS (EUS 21) is a typical service needed by staff responsible for strategic decisions and planning.

The Concept in the Fig. 4 represents high-level view of the Cyber Critical Infrastructures (CCI) that require special protection in accordance with the Department of Homeland Security (DHS) CIP (Critical Infrastructure Protection) strategy [9].

Hybrid Enterprise Information and Control Systems Concept is a new approach. We develop it for following reasons:

– Control systems were understood for a long time as integral part of primary production process that has nothing common with other information systems. Nowadays this standpoint is not appropriate (especially in the CCI context) and too costly - instead of well-structured ISO/IEC 17799 a proprietary approach is more expensive and less effective [1]
– Information security management standardization effort represented by ISO/IEC 17799 becomes more and more important in electronic business but very little attention is given to hybrid systems
– More and more organizations over the world deploy their Environmental management in accordance with ISO 14001 [12]. It is a not easy process; it also in many aspects duplicates effort that has to be spent by organization and deal with ISO/IEC 17799.

6. INFORMATION SECURITY AND ENVIRONMENTAL MANAGEMENT STANDARDS

The Committee responsible for a British information security standardization development identified environmental management standard ISO 14001 uses a model referred to as Plan-Do-Check-Act model or PDCA for short. The newly published revised Part 2 of BS 7799 (BS 7799-2:2002) applied this model also for Information Security Management Systems (ISMS) [2].

PDCA based harmonization between BS 7799-2:2002 and ISO 14001:1996 is great idea that allows organization significantly improve efficiency of its information and environmental management strategy. Overall correspondence between both standards includes nine areas: Introduction, Scope, Normative reference, Terms and definitions, ISMS/EMS requirements, Management responsibility, Resource management,, Management review, and Improvement.

Planning phase is the most critical harmonization part – it influences all other phases that follow. This phase is much better for an ISMS (BS 7799) then for an EMS (ISO 14001) and could be used as an etalon for environmental planning.

The ISMS planning phase consists of five parts.

a) Introduction. The plan activity is designed to ensure that the context and scope for the ISMS have been correctly established, that all information security risks are identified and assessed, and that a plan for the appropriate treatment of these risks is developed.
b) Information security policy. Requires the organization and its management to define the information security policy that includes a framework for setting its objectives and targets, and establishes an overall sense of direction and principles for action with regard to information security.
c) Scope of the ISMS. The ISMS would cover all parts that relate to the CCI. Dependencies, interfaces and assumptions concerning the boundaries CM, EIS SDP and EIS operational sub-systems need to be clearly identified. A concept shown in the figure 1 has to be developed and divided in some way, for example into domains to make subsequent risk management tasks simpler. Primary attention should be paid to the primary business process identification and impact assessment, evaluation of their CCI dependencies and to the CCI asset modeling.
d) Risk Identification and Assessment. The risks assessment documentation should explain which risk assessment approach has been chosen, and why this approach is appropriate to the CCI security requirements, the primary business processes environment and the risks the organization faces. The approach adopted should aim to focus security effort and resources in a cost-effective and efficient way. Primary attention should be paid to the identification of threats and vulnerabilities, assessment of threats exploiting vulnerabilities, calculation of risks based on the results of the assessment, and identification of residual risks.

Risk treatment plan. Organizations should create a detailed risk treatment plan, showing for each identified risk recommended countermeasures including time frame over which they to be implemented, already implemented countermeasures, and role / personal responsibilities. Acceptable level of risk needs to be identified.

Scope description and asset identification and valuation have to be developed in close contact with business owners who are familiar with business processes. In practice business owners are not experts on a business processes environment (IT infrastructure and its environment). Threat / Vulnerability assessment and risk analysis is abstract job usually under responsibility of Risk Analyst. Risk Manager uses risk profiles (outputs from risk analysis) for a design and implementation of the most effective risk treatment strategy.

The Hybrid Enterprise Management and Control Systems concept is appropriate architecture approach to the CCI scope definition and asset modeling. It can be used as a starting point of a CCI security project.

7. AN APPLICATION OF ARCHITECTURE MODELING AND RISK ASSESSMENT BASED SLM FOR CCI PROTECTION

The Concept in the Fig. 4 also includes basic recommendation concerning of a strategic security decision:

– CM sub-system processes small amount of timely sensitive data that could have critical impact on Work Nodes. The level of impact is tightly coupled with primary products and services and could be very large in

dependency on circumstances. Availability and Integrity are key security features that have to be guarantee in this system.

- EIS Operational sub-system has to be acceptable by all business-to-business participants on the base of a unique set of criteria. ISO/IEC 17799 standard is just a way to achieve this kind of security.
- Automation of a primary and supporting business processes accelerates accumulation of business information and allows its transformation to enterprise knowledge that is a subject of interest of competitors, foreign intelligence and so on. Confidentiality is a key feature that characterizes EIS SDP sub-system.

Last year GAO expanded high risks areas monitored since 1997 with risks of information systems that support American nation's critical infrastructures such as national defense, power distribution, telecommunications, and water supply [10]. This effort was a reaction to significant information weaknesses identified in 24 agencies in the year 2002. The analyses showed that weaknesses were most often identified for security program management and access control. In accordance with NIST a successful IT security program has to be based on an effective risk analysis and management (RARM) process [18].

RARM process for CCI described in the figure 4 is usually very complex and time consumption. To achieve appropriate modeling performance we have chosen CRAMM – CCTA Risk Analysis and Management Method /CCTA/ [6]. This method is very powerful from modeling point of view and allows generation security products in accordance with ISO/IEC 17799[1], and BS 7799 Part 2:2002 [2].

Left site in the figure 5 describes CM sub-system that is mapped to the Asset – Threat - Risk Model.

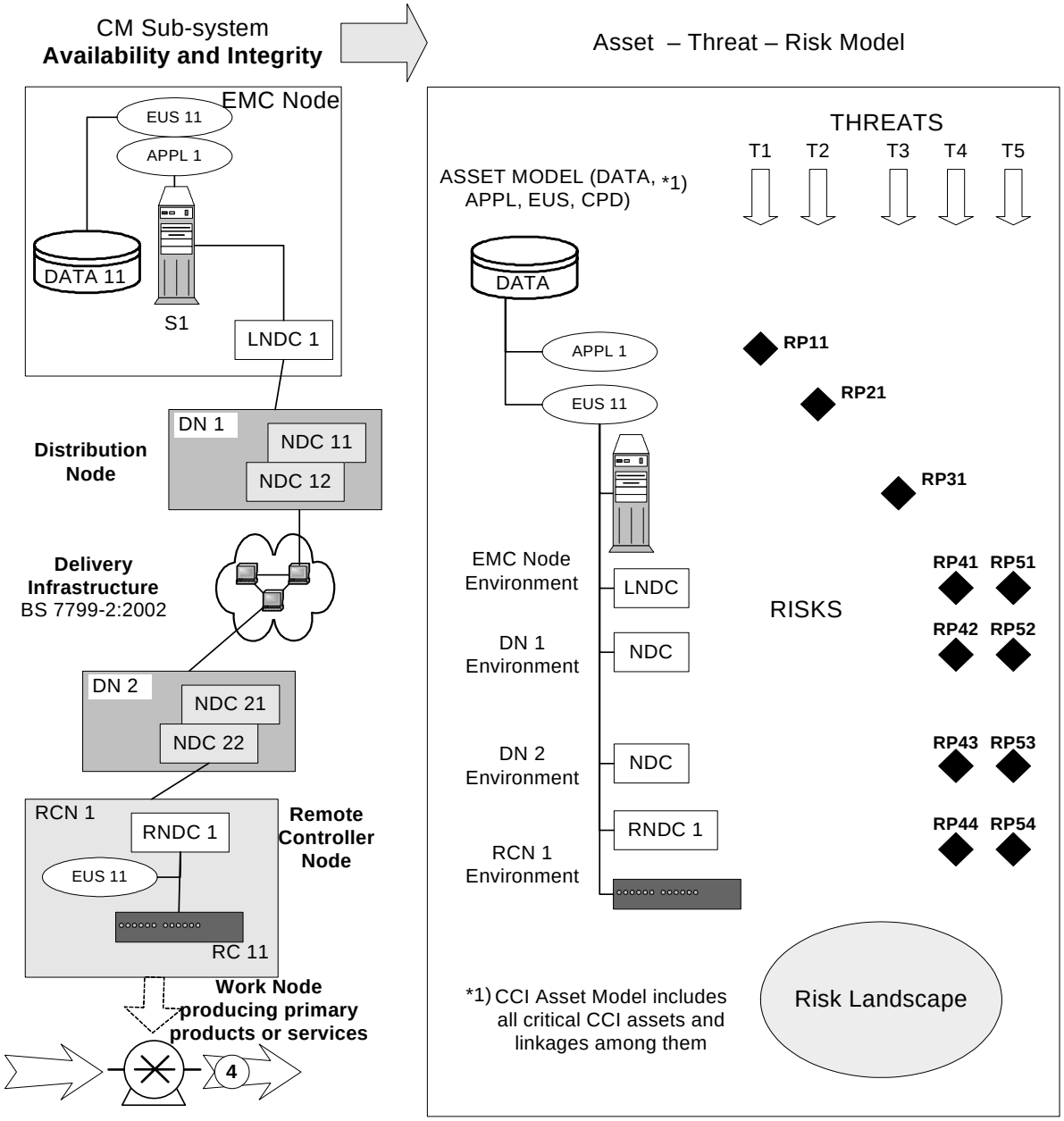

Figure 5: CCI / Asset – Threat – Risk Model Mapping

A mapping in the figure 5 integrates three parts:

- All critical components necessary for controlling of a Work Node, particularly data, application, end user service and CCI critical path delivery (CPD) components.
- Threats (T) include analyzed threats, particularly T1 – Unauthorized Use of Application, T2 – Communication Infiltration, T3 – Technical Failure of Server, T4 – Floods Damage, T5 – Terrorism.
- A Risk landscape that captures risks combining the level of threats / vulnerabilities with possible loss which may result from accident, attack or disaster.

Left site in the figure 6 describes the same CM sub-system as in the figure 5; it is mapped to the Asset – Countermeasure Model. Because Asset model is the same for both, Risk Landscape in the figure 5 and Countermeasure Landscape in the figure 6, it allows easy monitoring how risks are covered by countermeasures. Both, risks profiles and risk driven countermeasures are associated with the same assets. Model mapping in the figure 6 integrates three parts:

- All critical components necessary for controlling of a Work Node, particularly data, application, end user service and CCI critical path delivery (CPD) components.
- Countermeasures recommended for a protection (RC) on the base of a risk landscape, particularly system testing, data integrity over networks, accommodation moves, terrorist / extremist warnings and many others.
- A countermeasure landscape in which beyond each RCD symbol (Recommended Countermeasure Description) detailed description of countermeasure is placed (including its effectiveness, cost, and so on).

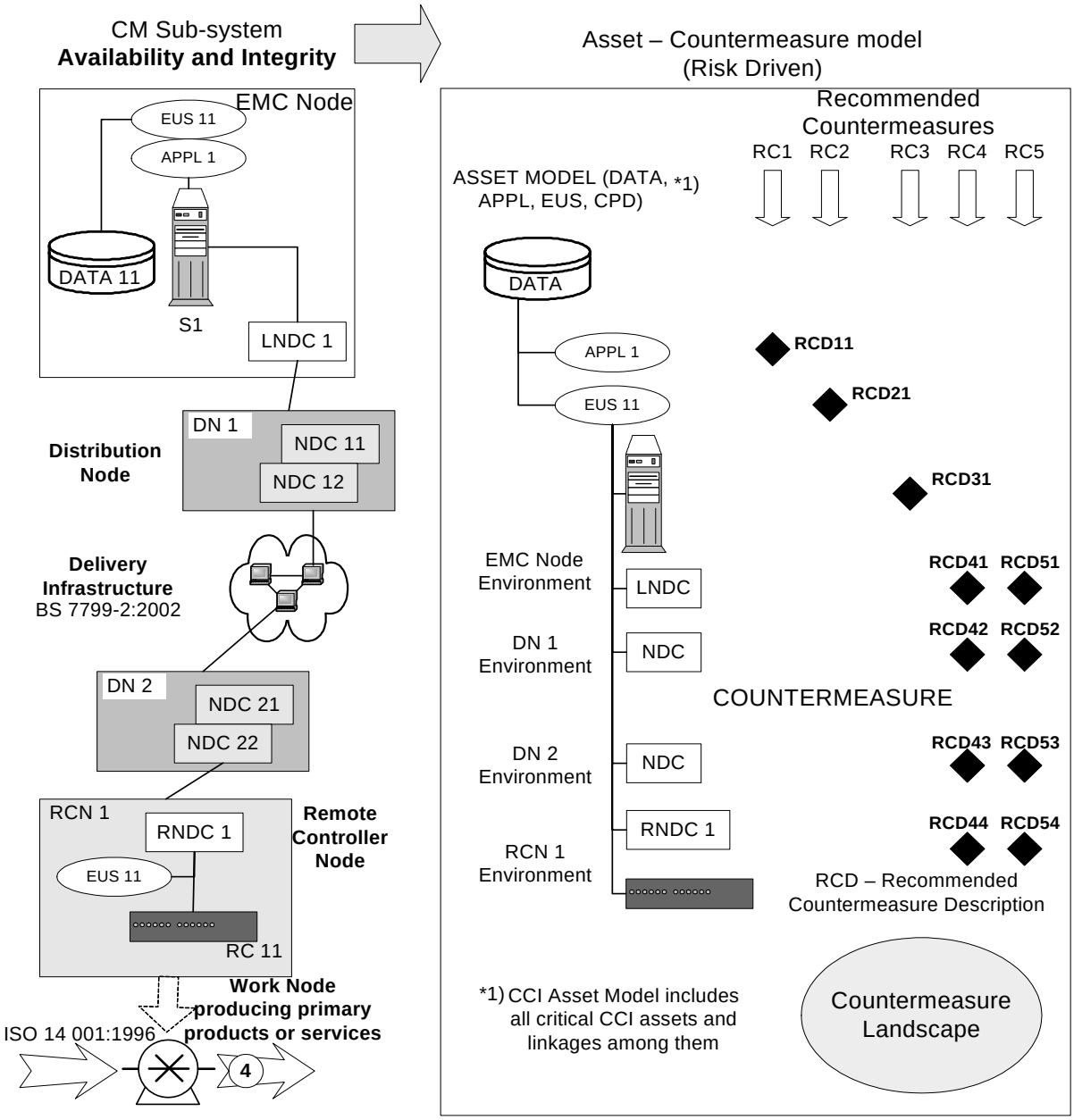

Figure 6: CCI / Asset – Countermeasure Model Mapping

CCI – Asset – Threat – Risk Mapping and CCI – Asset – Countermeasure Mapping allows strong engineering based approach to the SLA synthesize (figure 7):

a) A Scope Definition is based on the common Hybrid Enterprise Management and Control Systems Concept – this approach directly influences a design of an asset models.
b) Impact assessment that is a key part of Asset Identification and Valuation consider as a main source of impact disruption of a primary production process through work nodes managed by remote controllers.
c) Threat – Vulnerability Assessment consider a relationships between potential threats and asset model that replaces a real CM sub-system.
d) All three steps mentioned above create a risk landscape (output from Risk Analysis step) that can be used for specific decision making (for example acceptable risks). Well understandable risk landscape allows starting risk management, oriented to the decreasing of detected risk into acceptable level with an optimized set of countermeasures.
e) Outputs from Risk Analysis and Risk Management steps are further processed in a Responsibility Assignment step, which associates acceptable risks and risk management / treatment tasks with responsibilities. Responsibilities are further split among companies (for example power distribution company that is in a position of business process owner) and company's staff and external suppliers like telecommunication operators, application service providers, and so on.

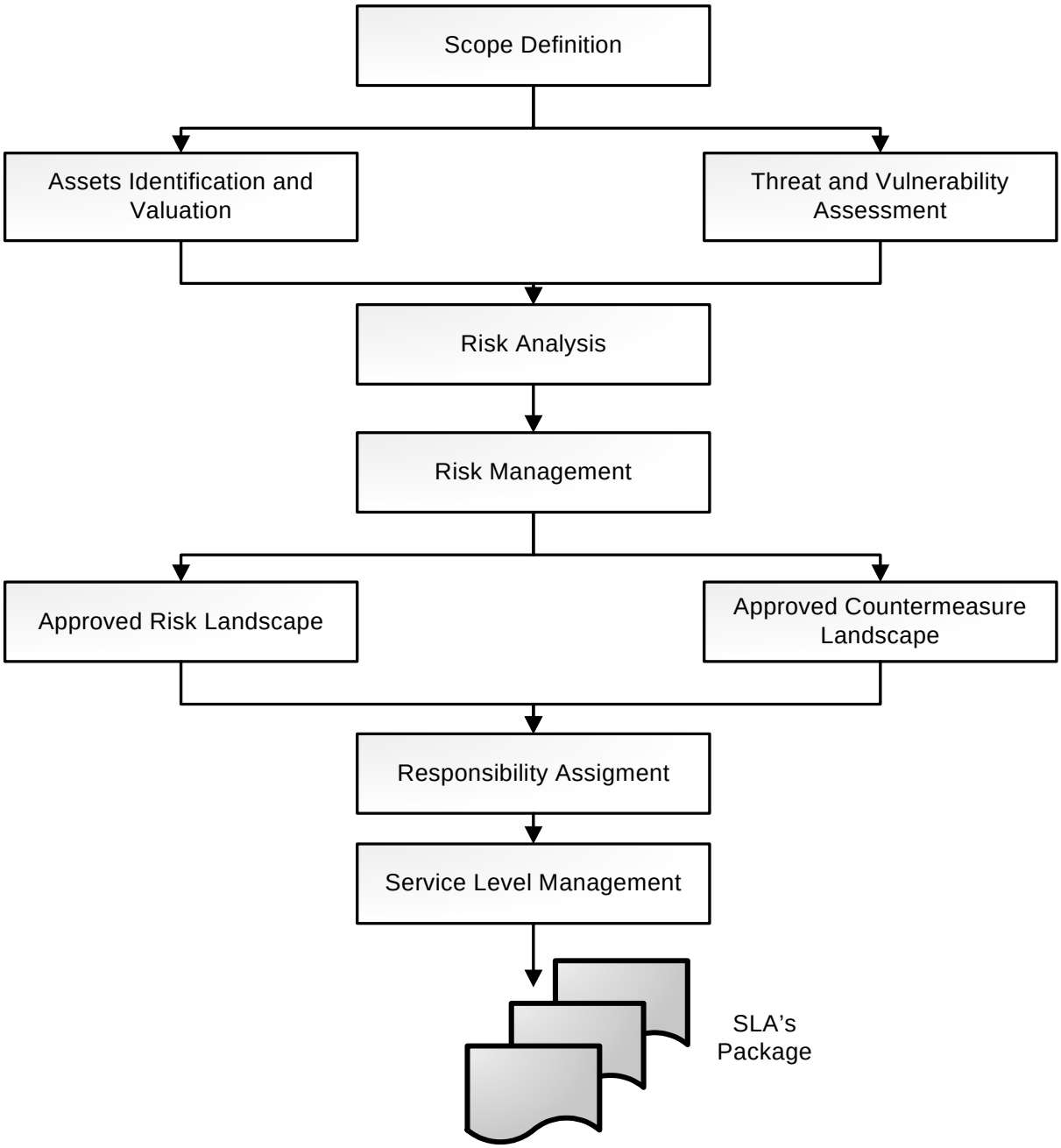

Figure 7: Synthesize of SLAs Considering Risks Threaten Business Processes in CCI

f) Service Level Management is a final step in the whole process; it generates an SLA's package using results of a Responsibility Assignment step.

8. CONCLUSION AND FUTURE WORK

Presented topic illustrates very flexible modeling that could be easily customized for broad ranges of SLA synthesize scenarios. From this perspective following topics seems to be interesting for further research:

a) Development of CAF techniques allowing business process owners better understanding of dependencies of their core business activities on IT services and IT infrastructure. These methods must involve them into the process of impact assessment, the process of a residual risk landscape understanding and making decisions concerning acceptable risks and in the process of active participation in responsibilities assignment and SLA specification.
b) Development of CAF techniques allowing IT service providers better and more precise threats / vulnerabilities identification and evaluation, risk landscape modeling and countermeasure landscape optimization.

There is also broad area for particular topics like "Assurance/Cost dilemma" and "Recovery Strategy establishment" (see figure 2).

Assurance/Cost dilemma needs systematic investigation. ITIL based concept does not include mechanism that allows controlling a process of continual improvement of an assurance like CCM and SSE CCM [15,16].

Recovery strategy, recovery options, backups, insurance and continuity planning represent a group of countermeasures that relate to CONTM module (figure 2). Continuity Management establishment has direct impact to a cost (COSTM module).

REFERENCES

[1] **BS ISO/IEC 17799:2000**, Information technology Code of practice for information security management.
[2] **BS 7799-2:2002**, Information security management – Part 2: Specification for information security management systems.
[3] CCTA, **Availability Management,** IT Infrastructure Library, ISBN 0 11 330551 6
[4] CCTA, **Cost Management for IT Services**, IT Infrastructure Library, ISBN 0 11 330547 8
[5] CCTA, **Service Level Management**, IT Infrastructure Library, ISBN 0 11 330521 4.
[6] CCTA, **The CRAMM Risk Analysis and Management Method**, Crown Copyright, CCTA IT Security and Privacy Group, London, 1991, 245 p.
[7] R.F. Dacey: Critical Infrastructure Protection. **Challenges in Securing Control Systems**, www.gao.gov/ogi-bin/getrpt?GAO-04-140T
[8] T. Feglar, **Component Architecture Framework (CAF) Methodology and Tools**, 2003.
[9] GAO."Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues", **GAO-03-1165T**, http://www.gao.gov/cgi-bin/getrpt?GAO-03-1165T
[10] GAO: "Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures", **High Risk Series,** January 2003, GAO-03-121
[11] ISO 13335-1:1996 **CMITS - Concept and models for IT security**
[12] ISO 14001:1996: **Environmental Management Systems: Specification with guidance for use**.
[13] F. Niessink, H. Van Vliet, Software Maintenance from a Service Perspective, **Journal of Software Maintenance: Research and Practice**, Vol. 12, N. 2, March/April 2000, pp. 103 – 120.
[14] A. Parasuraman, V.A. Zeithaml, L.L. Berry, A Conceptual Model of Service Quality and its Implication for Future Research, **Journal of Marketing,** Vol. 49, pp. 41-50, 1985.
[15] SEI, The Capability Maturity Model: Guidelines for Improving the Software Process, Software Engineering Institute, Carnegie Mellon University, **SEI Series in Software Engineering, Addison-Wesley Publishing Company**, Reading, Mass., 441 p. 1995.
[16] SEI, **Systems Security Engineering Capability Maturity Model SSE CCM**, Version 3.0, Software Engineering Institute, Carnegie Mellon University, 340 p., June, 2003.
[17] Sowa, J., F., Zachman, J.A. Extending and formalizing the framework for information systems architecture, **IBM Systems Journal**, Vol. 31, N. 3, 1992.
[18] Stonebuner,G., Goguen,A., Feringa,A.: „**Risk Management Guide for Information Technology Systems**", NIST Special Publication 800-30.
[19] Zachman, J.A., A framework for information systems architecture, **BM Systems Journal**, Vol. 26, N. 3, 1987,1999
[20] Zeithaml, V.A., Bitner,M.J., **Service Marketing**, McGraw-Hill, New York, NY, 700p. 1996.