Bundesamt für Sicherheit in der Informationstechnik

E-Government Phase Plan

Phase 3 “Analysis”

This text is a module of the

E-Government Manual

http://www.e-government-handbuch.de

Editorial staff: E-Government Project Team
Federal Office for Information Security (BSI)

Contact details: egov@bsi.bund.de

Contents

Information on this module

Status	BSI contribution
Authors	Belz, Dr. Mrugalla et al. (BSI)
Point of contact / contact details	Rainer Belz (BSI), egov@bsi.bund.de

Amendment History

Date	Name	Change
18.03.2004	Horn	Some changes incorporated
16.12.2002	Dr. Hauschild	Integration of recommended changes by the authors of the module "Authentication in E-Government" – further revision to follow in connection with the publication of Phase 5 or 6.
13.02.2002	Horn	Editorial revisions
19.12.2001	Belz, Mrugalla et al.	Version 1 completed

3 Phase 3 – "Analysis"

Phase 3 of the e-government implementation process entails making the organisational preparations that are necessary for the identified online-capable services. The activities are centred around the capture of information about, and optimisation of activities in, a business process analysis. After this, constraints such as the protection and security requirements for the planned services are determined. The approach presented also includes essential elements of an overhead-value analysis. All work operations are investigated here with a view to their later mapping onto IT procedures.

A review of the examination of feasibility and cost-effectiveness begun during Phase 2 and a preliminary check of the legal situation are also carried out. It is then planned to review and enlarge the selected e-government strategy.

To guarantee later implementation of the innovations, the new tasks are designed jointly with the staff affected. The approach requires close co-operation between the Organisational and IT Departments, which present the results of their work to senior management for decision-making. An open information policy should ensure acceptance within the agency of the changes associated with the introduction of e-government.

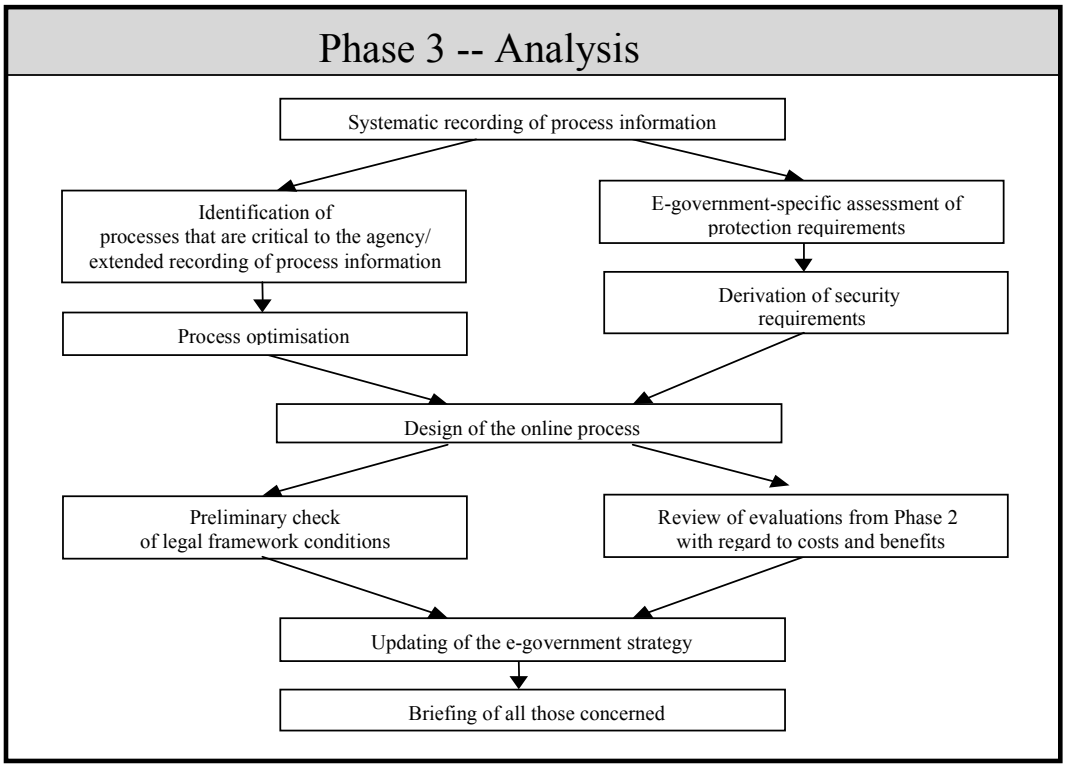


Figure 1: Flowchart illustrating Phase 3 – Analysis

3.1 Activity "Systematic recording of process information"

Initiation responsibility: Team leader

Implementation responsibility: Core team, Organisational Department, staff representatives (support)

Recording of process information in e-government

Design framework, points of emphasis

In the public service, the framework for the formulation of agency objectives is normally defined by the existing laws and the specific functions of the public agency. The financial framework is also controlled by the public budget. Compared with business and industry, it is a system feature that it is not possible to optimise existing procedures by moving closer to the customer and increasing customer acceptance.

If, moreover, one assumes that the public, as customers of public services, above all else expect the services to which they are legally entitled to be available quickly, at a low price and reliably, then it becomes clear that the necessary e-government analysis will primarily be aimed at increasing efficiency. A more or less extensive process analysis and optimisation is generally unavoidable.

Approach

The recording of potentially online-capable services in Phase 2 was carried out on the basis of existing working papers originating from the existing organisational and operational structure of the agency. To deal with the above requirements of e-government, however, it is necessary to adopt a process-oriented approach. This requires that there is a description of the workflows (including information flow) which makes it possible to identify weaknesses and the potential for improvements in the conventional procedure as well as possible uses for electronic workflow management. This process documentation also serves the purpose of identifying and eliminating media discontinuities.

If it is clear already at the end of Phase 2 that a workflow management system should be used across the agency, then it is beneficial to keep down the effort spent on the "classical" recording of process information in favour of the desired optimisation for an IT process in Phase 4. "Classical" recording of process information here refers in particular to the part of describing and optimising paper-supported processing and of transportation within the necessary sub-processes.

Involvement of staff representatives

It is imperative here to involve the responsible staff representatives from the start, as the results could be used to draw conclusions about the people holding each job (i.e. monitoring of performance and conduct would be possible). This applies irrespective of with which recording procedure the investigation is carried out (interview technique, observations at the workplace, flow diagrams, questionnaires, workshops). In the case of automated data capture methods, it is always necessary to involve the staff representatives early on.

Process analysis for modern state

Process-oriented analyses, unlike functional or task-oriented analyses, offer good opportunities for continual improvement. The employee is actively involved in the procedure of designing and optimising processes. The fact that the employee is encouraged to consider his work from the point of view of the internal or external customer creates greater mutual understanding and in the longer term greater employee satisfaction. Through the basic idea of modelling sizes of object over which it is possible for a process owner to have an overview, process analyses also constitute the basis for dealing with tasks in flat hierarchies. Generally this is also in line with the desires of customers/members of the public for a lean, efficient and low-cost administrative structure.

Use synergy effects

Results obtained by the Organisational Department from past investigations that had similar objectives can be used for the process analysis and process optimisation. For example, it could be the case that small sections of the agency have already been examined using time-and-motion analysis requirements and methods or that standardisation approaches similar to the DIN/ISO standards (9000, 9001 ff.) have already been developed for the implementation of effective controlling. As a rule it is also a good idea to make use of the know-how gained by staff from previous analyses.

Consider new control instruments

Before recording information about processes it is necessary to clarify what organisational goals have led to organisational changes in the past. For example, the priorities for the implementation of agency objectives that were ascertained in Phase 2 with regard to financial and personnel resources could lead to conflicts of interest if at the same time measures are planned for increasing employee motivation or for controlling.

Usually the e-government analysis and the use of new control instruments (instruments for raising efficiency and quality control, e.g. cost and performance calculation, controlling, agreeing objectives, suggestion systems, concepts for increasing competence) may be expected to complement each other. The new control instruments primarily serve to optimise the pure decision processes. At the same time the e-government analysis strives above all to improve efficiency within the individual services and thus constitutes the precondition for the online provision of services. If IT procedures for the use of new control instruments have already been implemented within the agency, steps should be taken during modelling of the e-government services to ensure that interfaces to these procedures are opened to ensure that none of the procedures planned turn out to be incompatible or difficult for users to use.

If nevertheless, incompatibilities should be identified between the objectives of e-government and new control instruments, then it is extremely advisable to discuss and clarify these before starting to record information about processes.

Factors relevant to the scope of the analysis

Even if organisational analyses have been carried out in the past which could be used to get up to speed with the problem area, there is no mistaking the time and staff resources that are needed, nor the elapsed time involved in carrying out an analysis at process level. Projects aimed at extensive restructuring and optimisation usually last several years and are very labour intensive. The scope of the studies depends heavily on the existing extent of IT penetration in relation to the number of planned online services. The effort necessary for the analysis depends critically on the depth of detail envisaged. The approach described below

is appropriate for analyses of intermediate depth of detail. If the strategic requirements are such that a highly detailed analysis is necessary, then the approach must be modified. This subject will be examined in more detail in the next activity, "Identification of processes that are critical to the agency, extended recording of process information".

Project management with software support

Even analyses of intermediate size should generally not be carried out without the support of relevant software products, as otherwise the amount of effort required for later IT design becomes unmanageable. If the total effort does not warrant the purchase of special analysis software, then it is recommended at least using some project flow software. If processes have already been redesigned for parts of the agency (especially Human Resources and Cost Management) using special modules or program packages, use of these products should be considered for the e-government analysis as well for reasons of economy.

Assignment of services to processes

Processes

The online-capable services selected in Phase 2 are assigned in this activity to the top-level agency tasks as processes. Compared with the activity "Identification of required infrastructural procedures" carried out in Phase 2, the concern here is to group together services that have similar workflows (e.g. all requests for advice). The aim is to identify activity chains (processes) which *one* member of staff (the person responsible for the process) can if possible process from start to finish alone. In this way it is desirable that the work outcomes achieved within such a process are not produced by several persons and then signed off by a line manager, but that instead responsibility for the result of carrying out the process lies with one person only.

The aim of identifying processes is to establish a basically object-oriented organisation, so that as a result a qualitative improvement of services can be achieved. There is an obvious point of contact for external customers, line managers are relieved of routine work and can concentrate fully on their management and co-ordination functions.

If delegation possibilities are exhausted in the course of process modelling, efficiency can be improved. Performance-specialised service pools should not be excluded as a possibility, but their cost-effectiveness must be examined in detail.

In the course of identifying processes and without putting a lot of effort into it, existing activities should be assigned to "virtual functional units". This promotes awareness of the theoretical restructuring possibilities, detached from existing hierarchical structures. In reality, it will generally not be feasible to implement such a radical redesign of the hierarchies within a public agency.

1. Break down every online-capable service at activity level. Activities include, for example, advising, checking, analysing, researching, making decisions (define sub-processes).
2. Group together the activities noted during step 1 into groups with identical activity content, independently of the organisational unit (department) that produces the service. Functional content depends on the person at whom the service is directed (member of the public, public agency, business).

Example. All advisory services of the agency in which advice is given to members of the public constitute one group (Subject 1, ..., n). All the services in which only complete work outputs are communicated to the public as information are assigned to the Public Relations group.

If grouping on the basis of output is not possible, then it should be done according to content.

Example. All services of the agency which require contact with law courts are assigned to the Legal Department group.

Process types

The processes of the agency are classified into

- core processes (primary tasks of the agency)
- support processes (internal administrative tasks)

Dividing line for comprehensive process analysis

Restructuring, possibly into steering processes (tasks of decision-makers, e.g. Human Resources) or by customer role is not necessary from this point of view for the objectives of the e-government analysis. Support processes should only be investigated in individual cases as they are not at the forefront of the e-government initiative. Nevertheless, it can be useful and necessary to examine them in case it should become apparent that a standard workflow system needs to be used right across the agency.

Graphical presentation of processes

Graphical presentation in flow diagram

In parallel to the recording of detailed information about processes and sub-processes, it is useful to present the logical connections between them in graphical form. This graphical presentation makes it possible to grasp the important sequences and links in actions at a glance. It should be quite clear which decisions are made and which actions (have to) follow these decisions.

A major source of branches are Yes-No decisions and Or decisions that entail different actions. To later determine the best approaches, it should also be possible to detect when decision-makers change and how information is transported. The start and finish of a diagrammatic chain of events should be delineated by identified sub-processes. Interfaces between processes should have their content explained.

Generally, the sub-processes that are urgently required in order to initialise the next process must be marked as a minimum.

Example of a process / definition sub-process

Product certification

Process – sub-process

Sub-processes of the process **Product certification**:

Order confirmation
Functional check
Check for adherence to tolerance limits
Patent research
Preparation of a report
Generation of certificates
Publication

Content of sub-processes, definition

Sub-processes are presented at the level of "milestones" for the achievement of the process objective, not at a level of detail that approaches the activity level (activity in the sense of individual performances, chores). Sub-processes are processes whose boundaries can be set by the creator and which have a clearly delineated input and output. The following must be derived from the individual sub-processes:

Collection of information about sub-processes

- Name of the sub-process e.g. order confirmation
- Brief workflow description of the work steps. Where does media discontinuity exist?
- Who is responsible for creation, who owns the sub-process? A role should be assigned here e.g. technical officer, computer scientist or legal adviser, rather than a specific individual.
- Work equipment/medium used for the output, e.g. word processing program xy, spreadsheet xy or paper and pencil.
- Tools/medium needed, e.g. collection of statutes/regulations xy (paper version), address directory xy (file/table format xy), exchange-rate table (HTML internet), telephone or fax.
- Statement of effort required for the sub-process, e.g. average time it takes to process the sub-process and average frequency. If appropriate, assign to cost centres.
- Recipients of copies of the output, e.g. persons working in purchasing, Legal Department, divisional archive Z.
- Weaknesses from the point of view of the owner of the sub-process, e.g. frequent delays due to non-availability of customer hotline, (excessively) long internet connection time.

3.2 Activities "Identification of processes that are critical to the agency", "Extended recording of process information"

Initiation responsibility: Team leader

Implementation responsibility: Core team, Organisational Department, senior management of the agency

Determine processes that are critical to the agency

To determine which processes are critical to the agency, the processes captured in Activity "Systematic recording of process information" (Activity 3.1) are assessed in order to identify processes that are of elementary importance from a financial or strategic point of view. It is up to each agency to decide for itself which processes are critical. These could be processes which, because of their frequency or complexity, tie up a lot of personnel resources, or they could be processes which, due to their financial or political importance, are essential to the existence of the agency. Processes that are critical to the agency because of their quantitative importance can be deduced from the recording of process information (effort for the sub-process, processing duration).

Qualitative evaluation criteria can be derived from the activity "Determination of quality requirements for online services" (Phase 2) e.g. the specification of a very short reply response time. Additional clues as to the qualitative assessment of processes that are critical to the agency (e.g. high or very high requirements for confidentiality, integrity and availability) can be obtained from Activity "E-Government-specific assessment of protection requirements" (Activity 3.4), which is initiated in parallel.

Detailed analysis necessary?

A decision must be made as to whether process information should be gathered to a greater level of detail compared with Activity "Systematic recording of process information" (Activity 3.1) for the processes identified as being critical to the agency. A higher level of detail might be considered, especially for the description of the workflows and for the processing duration and frequency within the sub-processes. The more critical the importance of the process, the greater the level of detail that should be applied.

Criticality

Where the analysis is to proceed to a greater level of detail, it is necessary to identify which *work operations* within the sub-processes are critical to the assessment that a given process is critical to the agency, whether on account of the frequency of the process or its qualitative importance. "Work operations" are individual processing steps (recording of process information includes a workflow description of the work operations for each sub-process) within sub-processes.

Data gathering techniques

Quantitatively important work operations can be gauged from organisational data gathering methods/observation techniques. These include techniques such as work sampling. These techniques should not be used without theoretical and practical knowledge of suitable procedures (e.g. time and motion methods – for further information see

http://www.refa.de). If necessary, key figures which can be used for subsequent benchmarking can be calculated using these methods.

Examples

1. Process critical to the agency because of its qualitative importance

Process "Product certification" consists of seven sub-processes. The process occurs around 60 times per year. The total processing time for the sub-processes is around 2 million minutes of work per year. At present 33 employees (out of a total of 120 in the agency) are employed at different levels of the hierarchy to deal with the process. On the basis of its quantitative importance, the agency's senior management decides to classify the process as one that is critical to the agency. One of the agency objectives from Phase 2 is to develop rationalisation potentials. Two of the sub-processes account for over 50% of the processing time for the entire process. These sub-processes are to be investigated further, in addition to the staff interview carried out. The decision is taken to describe these workflows precisely and to evaluate them individually using the work sampling data gathering technique, so as to provide the level of detail needed to derive possible optimal approaches for the sub-activities.

2. Process critical to the agency because of its quantitative importance

Approximately 1,500 staff are employed in agency XY. The authority has a division in which 400 members of staff process applications from members of the public/customers, with 350 out of the 400 staff employed to perform the routine clerical work. 22,000 applications are handled per year, and the customer file covers 130,000 customers. The customer applications all concern the same area of law, and the notifications that are issued are based on *one* law only. Processing of applications is performed using a word processor. The average processing time is 28 calendar days from receipt of the application through to sending out the written notification by post. The customer does not receive any interim notification even where processing takes longer.

In Phase 2 it was decided to make the service available online. Senior management has specified as a quality feature that a member of the public should receive an acknowledgement of receipt of his application no later than within five calendar days. The total elapsed time to process an application should not exceed 21 calendar days.

On the basis of the large numbers of cases handled, the agency's senior management decide to classify the process as one that is critical to the agency. In addition it is decided to carry out a detailed analysis of the work operations. In connection with the "electronification" of the procedure, a review is to be carried out of the content of the work with a view to increasing the quality of the procedure. The decision taken is to be made more transparent to the public. The content is to be made more uniform.

3.3 Activity "Process optimisation"

Initiation responsibility: Team leader

Implementation responsibility: Core team, Organisational Department, Human Resources

General optimisation approaches

The activity begins with analysis of the results of the process of recording information about processes. Obvious objectives for optimisation approaches can be worked out from the activities completed in Phase 2, "Determination of evaluation criteria for online-capable services" and "Determination of quality requirements for online-services".

No radical redesign

From the limited objectives of the e-government initiative, and given the existing time and cost pressures, there will generally be no question of radically redesigning processes.

Vulnerability analyses

It is useful to have an expert systems analyst indicate at the outset where weaknesses exist in the identified sub-processes. Typical weaknesses include, for example:

- Long processing time
- Long wait times
- Frequent alternation of personnel within a process
- Media discontinuities within processes

Quantitative optimisations through use of IT

In the first stage of optimisation, basic, predominantly quantitative opportunities for improvements through the use of IT resources should be considered. These include in particular speeding up processing due to the elimination of transport times, to electronic forwarding, shortening of wait times, central data keeping, archives, follow-up reminders and filing. Moreover, the gradual removal of media discontinuities should be checked, taking into account the associated effort.

Participation of staff in workshops

The *causes* of suspected weaknesses should be identified with the aid of workshops or employee surveys. As modern communication platforms, workshops are an effective investigatory tool because they provide a means of accessing directly the competence and expert knowledge of the workforce so that ideas as to possible solutions can be generated rapidly and with comparatively little effort. To obtain high value results, workshops must be well prepared and moderated in a purposeful fashion. They should be attended by the people who actually work on the sub-processes as opposed to the persons who are responsible for the processes. In this way, the staff concerned will gain the opportunity to express their opinions. This is important if they are to be motivated and also for the generation of creative ideas for solutions, both of which are essential for a continuous process of improvement. Criticism of the way things are done, or "process criticism", and restructuring exclusively by line managers or "technical experts" has in practice proved ineffective. Staff and the responsible staff representatives should be informed in advance that process criticism and/or identification of weaknesses

will only be used for the purposes of the e-government analysis and not to check up on staff performance. Accordingly, access to the data collected must be protected. This data must be treated as confidential.

Qualification of the moderator

The workshops should be moderated by an organiser capable of assessing the potential utility of approaches to solutions put forward by employees. His job is to identify areas in which standardisation would be appropriate (customer contact, letters, reports, statistics) and to refer to them in a purposeful way. As the aim is the online provision of the service, he must be in a position to present to the parties involved the basic improvements that might be possible with selective use of IT that have been worked out during the first stage. In the long-term the aim is to integrate as many tools and resources as possible without media discontinuity.

Process criticism vital

Process criticism enables the persons involved in the sub-processes to develop improved ideas for dealing with tasks in the future. Discussion in process criticism is centred around the workflows identified within the sub-processes and the weaknesses from the point of view of the user. The following issues should be considered:

- How can a sub-process be simplified (forms, standard text) or standardised?
- Where is work being duplicated (entered more than once)?
- Has all the potential for delegation (signatory authorisation) been utilised?
- What errors have occurred in practice?
- Do any standard procedural specifications exist? Is it possible for the same initial situation to produce different results, especially as a consequence of unclear, missing or contradictory procedures? Does this result in uneven treatment, especially in the legally relevant sense?
- How much time is invested in preliminary work? Are all the resources and tools available locally and when needed?
- Is the person responsible for the work satisfied with the procedure and the outcome of the work?

Design of new tasks

When designing the new tasks, the qualification and capabilities of the workforce must be considered. The moderator of the workshop should initiate the development of ideas for improvements and enhancements through organisational or electronic procedures:

- Create pools of knowledge and competence.
- Use benchmarking for identical activities.
- Present opportunities for reporting, monitoring and controlling. Determine the process owner.
- Speed up procedures through parallel sub-processes.
- Consider possible applications for project work.
- Eliminate routine work through the use of IT.

If possible, all the changes and suggestions for changes should be noted down in the workshop. If necessary, key points which can be refined as to content later on can be noted down.

Qualification concept

After the tasks in the optimised sub-processes have been designed, it is necessary to clarify whether the role of the person performing the work has significantly altered. If the resulting profile no longer matches the qualifications of the workforce, then a staff qualification plan must be prepared, and this should be expanded and refined in the course of the e-government analysis. It is sensible for the Organisational and Human Resources Departments to work together on this. If appropriate, opportunities for outsourcing should be checked, e.g. if any exotic knowledge or capabilities are required only to a very small extent.

All measurable differences, e.g. as a result of speeding up procedures (time gained), should be documented and assessed. The same applies to any effort expected to be spent on optimising procedures.

3.4 Activity "E-Government-specific assessment of protection requirements"

Initiation responsibility: Head of E-Government Team

Implementation responsibility: Core team, IT Security Officer, Data Protection Officer, Legal Department

Introducing protection requirement

In the course of introducing e-government, existing services should be transformed so that a significant proportion of the necessary communications between customers and the public agency are carried out over the internet. The aim of this activity is to define for each online-capable service identified in Phase 2 the protection requirements of the underlying communications. The main security objectives that have to be considered here are the confidentiality, integrity and authenticity of both data and communication partners. Moreover, the functioning of e-government depends on the technical systems required (e.g. web servers) being available in the agency.

The procedure presented here, the "e-government specific assessment of protection requirements", considers exclusively *communication* between customers and the agency and hence the interfaces of the online service. An extensive assessment of protection requirements, e.g. to IT Baseline Protection standard (IT Baseline Protection Manual, http://www.bsi.bund.de/gshb , Section 2.2) is undertaken in Phase 4. This is based on the IT resources used and takes into account the client PC, the technical implementation of the communication channel and also the IT resources at the public agency (web servers, background system).

Protection requirement classes

Protection requirement classes are defined below as an aid to orientation. As the protection requirement cannot normally be directly quantified, the definition is limited to a qualitative statement. On the basis of the IT Baseline Protection Manual, five[1] protection requirement classes are defined.

Protection requirement class	Variations in protection requirement class
None	No particular protection is required as no impact from loss or damage is expected.
Basic	The impact of any loss or damage is strictly limited
Medium	The impact of any loss or damage is limited.
High	The impact of any loss or damage may be considerable.
Very high	The impact of any loss or damage can attain catastrophic proportions which could threaten the very survival of the agency/company.

Table 1: Protection requirement classes

[1] The IT Baseline Protection Manual does not distinguish between "Basic" and "Medium". Hence, only four classes are defined in the manual. Because of the large number of possible authentication mechanisms, it makes sense to have a more precise subdivision here for this protection objective.

Damaging effects

The damaging effects that are of interest here refer on the customer side primarily to damage to the **social standing** or the **financial situation of the customer** (e.g. impairment of the right of informational self-determination, impairment of personal freedom from injury, financial consequences etc.).

On the side of the agency, the main concerns are that **administrative acts should remain within the law** (e.g. not violate laws, regulations or contracts) and that no **loss of image** should occur (e.g. due to negative consequences). Other consequences (e.g. **impaired performance of duties, financial consequences**) are conceivable. It is not normally possible to quantify the financial consequences in absolute figures.

Assessment of protection requirements

In order to assess the protection requirements for communication in a particular transaction, the possible damage scenarios must first of all be analysed and the potential damaging effects assigned to the individual protection requirement classes (Table 2, further more detailed information is provided in the "Authentication in E-Government" module). The higher the protection requirement class, the more important it is to have protection from the relevant damage scenario.

Protection requirement class **Impact of** **loss or damage**	**None**	**Basic**	**Medium**	**High**	**Very high**
For the customer:					
"Social standing"					
"Financial situation"					
For the agency:					
"No legal violations"					
"Loss of image"					
"Impaired performance of duties"					
"Financial consequences"					

Table 2: Assessment of protection requirements

Information and examples are provided below for the relevant security objectives as to how to ascertain an appropriate protection requirement class for online services.

Protection requirement for transmitted data

The security objectives listed above refer to the data that is passed, both from the customer to the agency (input) and from the agency to the customer (output). In the case of a complex service, a number of transmissions can take place in each direction. In a first step, a separate assessment of protection requirements should be carried out for each transmission, as often no single level of protection

requirement will apply universally. In particular there will usually be a difference in requirements between the input and output phases.

Confidentiality (of transmitted data)

If data is exchanged between customers and agency, then in many cases it is necessary to ensure that this cannot be read by unauthorised third parties; the *confidentiality* of the transmitted data must be protected. In the conventional paper-supported approach, confidentiality is normally safeguarded by the use of envelopes.

The following examples provide the rationale for each possible classification:

> **None**: general information; conventional communication entails publishing in brochures / newspapers / generally accessible media or sending out by postcard.
>
> **Basic:** person-related or company confidential data (e.g. marital status, dates of birth) requiring little protection; conventional communication is by postcard or letter.
>
> **Medium:** person-related or company confidential data (e.g. marital status, dates of birth) requiring a limited amount of protection; conventional communication entails sending in a sealed envelope.
>
> **High:** person-related or company confidential data (e.g. tax affairs, default summonses); conventional communication entails sending in a sealed envelope.
>
> **Very high:** person-related or company confidential data requiring special protection (e.g. medical data about patients, correspondence regarding bankruptcy, seizure of chattels); conventional communication normally entails sending by registered post or handing over personally.

The generic term "binding force" of data covers the following aspects: **data integrity** (protection against alteration of data), **data authenticity** (ability to attribute the data to the originator); **non-repudiation** (protection against subsequent denial of authorship), **legally binding nature** (in the sense of having concluded a contract), **fulfilment of the requirement for the written form** (as required by law), and **unequivocal mapping to the data records**.

Integrity (of transmitted data)

If data is transmitted, it is necessary to ensure that this data cannot be modified en route; its *integrity* requires a certain degree of protection. Changes to data could occur here either as a result of technical errors (unintentional) or through deliberate manipulation (intentional). The first type of change applies if the data altered by transmission errors is no longer meaningful (e.g. it comprises a series of random character strings).

Strictly speaking it is always important that data cannot be modified[2]. It is necessary here to assess on the one hand the possible effects that changes could

[2] This applies not only to the actual transmission but also to storage of the data before or after transmission.

have and on the other hand the probability that this data will be deliberately manipulated.

The question of data integrity plays only a very small role in paper-supported procedures, as generally it is not possible for changes in the content of a written document to go unnoticed. The risk potential in this case is quite different from that in an IT-supported procedure.

All data which needs to be kept in a condition such that it could be produced in court must have the classification category of at least "High" against the "Integrity" protection requirement.

The following examples are intended to explain the various classification possibilities:

> **Basic:** general information (e.g. procedures regarding performance of services, opening times).
>
> **Medium:** information for a restricted user population (e.g. changes of dates of meetings).
>
> **High**: tax return, tax assessment notice.
>
> **Very high**: data which leads to automatic actions or to the deployment of emergency services (alarms to emergency services / the THW emergency organisation), data relating to police investigations.

Authenticity and non-repudiation (of transmitted data)

It is also necessary to check to what extent it is a requirement that the transmitted data can be attributed to its originator. This relates to the *authenticity* of the communicated data, i.e. the ability of the recipient to reliably attribute the data to the supposed originator, and its *non-repudiation*, i.e. the ability to prove the attribution of data to third parties. Once again, both directions of communication must be considered, i.e. both from the customer to the agency (input, e.g. customer application, customer request) and also from the agency to the customer (output, e.g. notice, reply or request by the agency).

In paper-related procedures, authenticity and non-repudiation are normally established by a signature or an official stamp.

Legally binding nature

The implementation of a legally binding, technical equivalent (qualified electronic signature) requires extra expense on the part of the customer. It should therefore be checked on a case-by-case basis whether a signature is in fact necessary.

All data which needs to be retained in a condition such that it could be produced in court must have the classification category of at least "High" against the "Authenticity of data" and "Non-repudiation" protection requirements.

The following examples explain the various classification options:

> **None:** it is possible to use the service anonymously or without giving one's name or other authentication data, e.g. request for opening hours of an office, notification of rubbish collection dates, publication of the results of an election, retrieval of information brochures.

Basic: the communication can be made informally in writing (i.e. not on a specific form) or verbally (to be written down), i.e. normally without a written signature, e.g. when arranging an interview with the Planning Office.

Medium: the communication can be made informally in writing (i.e. not on a specific form) or verbally (to be written down), e.g. filing a report with the police.

High: the communication has to be made in writing, i.e. including signature or official stamp or other distinctive features, e.g. tax return, tax assessment notice.

Very high: the written form is not sufficient for the communication, it must also be countersigned by an official office (e.g. appearance in person), e.g. the issue of personal identity papers.

Fulfilment of the requirement for the written form

The requirement for the written form can only be fulfilled by a qualified electronic signature

If a law or regulation requires the written form and this requirement cannot be dispensed with, the only way to fulfil this obligation electronically is by means of a qualified signature. The mechanism of using a qualified signature has the effect of giving a protection level of at least "High" in terms of the authenticity of the signatory.

If there is no such legal basis, but a signature is normally required under the conventional procedure, the reason for having the signature needs to be examined. It is possible that the signature can be dispensed with in favour of a different authentication mechanism.

Unequivocal mapping to the data records

Unequivocal mapping to the data records

If data records should be or have to be accessed, the authentication data must be suitable for finding the data records, either directly or in combination with identification data.

This is particularly important if access to customer data records is required in order to perform the particular service. The identification and authentication data must enable unambiguous attribution. Steps must be taken to ensure that:

- the data records possess some characteristic enabling them to be distinguished (called the *principal*).
- there is a rights check (*reference monitor*) to decide whether the subject's access request to the object can be allowed (under the *access control policy*); however, this is not a question of authentication in the sense of unequivocal mapping.
- access is not granted until authentication and the rights check have been successfully completed.

Protection requirement for communications

As well as the protection required by the data, in the e-government-specific assessment of protection requirements further security objectives relating to the

communication that takes place must be considered, i.e. the authenticity of communication partners, the requirement for ex-ante authentication (authentication before performance of the service) and system availability.

Authenticity of communication partners

The use of online services often presupposes that agency and customer are able to "recognise" each other. On the one hand, the agency wants to be sure prior to sending out documents that the customer is really the person he claims to be. On the other hand, it must also be possible for the customer to be certain that his communication partner (e-mail address or web address) really is the desired agency.

Once again, this task is less difficult in the paper world as the majority of data exchanges are carried out by post, and postal addresses, unlike web and e-mail addresses, cannot generally be chosen freely and cannot be rapidly altered.

On the agency's side, the technical component which mediates the exchange of data between customers and the agency's background system plays a central role. This component is the agency's (web or mail) server, which, for example, can be implemented in the form of a "virtual mail room". It is therefore necessary, depending on the online service to be provided, to clarify how authentic this electronic incoming mail room has to be.

If the *confidentiality* of the transmitted data is "High" or "Very high", then this classification also applies to the authenticity of the public agency or the "virtual mail room" which in the online service ultimately receives the customer's data.

The following explanations and examples are intended to explain the classification options:

> **None**: the communication partners can remain anonymous.
>
> **Basic:** the identity claimed is accepted, e.g. a simple statement of the name and address of the communication partner or a print of the logo of a public authority (e.g. general information provided by the agency, simple requests which could also be made over the telephone).
>
> **Medium**: plausible verification of identity must be possible, e.g. by giving further information such as file reference or reference to previous communications.
>
> **High**: authoritative verification of the identity of communication partners must be possible.
>
> **Very high**: the identity of communication partners is unequivocally verified in advance (e.g. through submission of personal ID or registered delivery).

Requirement for ex-ante authentication

In some transactions it is of relevance

- whether the identity of the customer can be determined "ex ante", i.e. before performance of the service (it may also be necessary here to distinguish between whether determination of identity is merely possible or actually has to take place) or
- whether it is sufficient that the identity of the customer can only be determined "ex post", i.e. subsequently.

This is particularly important if there is the possibility of irreparable damage arising as a consequence of performing the service (e.g. disclosure of information regarding serious illnesses or previous convictions to third parties). In practice, though, this aspect is only relevant if the protection requirement is "Medium" or "High". If the protection requirement is "None" or "Basic", the question of "before or after performance" does not arise. If the protection requirement is "Very high", determination of identity must inevitably be "ex ante".

Availability (of technical systems at the agency)

Online services can only be used if technical systems at the agency are available. For each service it is necessary to ascertain how long it is acceptable for systems to be down in the event of failure. The following classification system is recommended:

None: not applicable

Basic to medium: it is acceptable for the online service to be out of action for more than 24 hours.

High: it is acceptable for the online service to be out of action for between one and 24 hours.

Very high: the maximum time for which it is acceptable that the online service should be out of action is less than one hour.

Example

An example will illustrate this type of assessment of protection requirements.

Submission of a tax return and return of the tax assessment notice

Input (tax return)

Confidentiality: "High", as the document contains person-related data that has to be kept confidential.

Integrity: "High", as changes to the data could have significant effects.

Authenticity, non-repudiation and legally binding nature: "High", as a manual signature is necessary.

Fulfilment of the requirement for the written form: Yes.

Authenticity of the public agency as recipient (e.g. "virtual mail room"): "High", as personal data is passed to the server with the tax return.

Authenticity of the customer: "None", as the originator of the tax return is irrelevant as long as the tax return is in writing (e.g. qualified signature).

Requirement for ex-ante authentication: Yes.

Availability (of the receiving mail room): "Basic" to "Medium" (rising to "High" in the run-up to deadlines for submission), as normally it does not matter if a tax return is submitted few days later.

Output (tax assessment notice)

Confidentiality: "High", as the assessment notice contains person-related data that has to be kept confidential.

Integrity: "High", as changes to the data could have significant effects.

Authenticity, non-repudiation, legally binding nature: "High", as the tax assessment notice is subject to special characteristics.

Fulfilment of the requirement for the written form: Yes.

Authenticity of the public agency as originator: "None", as the tax assessment notice already satisfies the written form requirement (for example, it is signed by the agency).

Authenticity of the customer as recipient: "High", as personal data is communicated with the tax assessment notice.

Requirement for ex-ante authentication: No.

Availability (of the outgoing mail room): "Basic" to "Medium" as normally it makes no difference if delivery of the tax assessment notice is delayed by a few days.

Protection requirement → security requirements

In the next activity, based on the assessment of protection requirements, the (security) requirements of the transaction that is to be implemented online are examined for both the input and output phases. Requirements which are derived from processing within the authority are not considered at this point, as they are not part of the actual communication.

Additional resources provided in the E-Government Manual:

- Module entitled "Resources for e-government – toolbox" (further information on the assessment of protection requirements is provided in Section 2.2 of the IT Baseline Protection Manual).
- Module entitled "Encryption and Signature"
- Module entitled "Authentication in E-Government"
- "Guide to the Introduction of Digital Signatures and Encryption in Government Administration" (toolbox)

3.5 Activity "Derivation of security requirements"

Initiation responsibility: Team leader

Implementation responsibility: Core team, IT Security Officer, Data Protection Officer, Legal Department

Following the previous activity, it is now necessary to collect data about the protection requirement of the data transmitted and the communication partners involved in relation to the generic protection objectives of the individual communication phases. This sets the limits for the degree of security that is necessary for secure communication between customer and agency. It is then necessary to incorporate this protection requirement into specific security requirements placed on the partners involved and the safeguards that they need to implement. The requirements regarding the procedures and data formats used or the organisational constraints will then become apparent, enabling the categorisation of possible solution mechanisms for the implementation of the online services.

The security requirements of the individual services can be deduced from the protection requirement class using the following rules:

Input

- Confidentiality

  If the protection requirement regarding confidentiality is "Basic" or "Medium", then it is desirable but not absolutely necessary to encrypt data sent by customers to the agency.

  If the protection requirement regarding confidentiality is "High" or "Very high", then it is imperative that data transmissions from customers to the agency are encrypted.

- Authentication of customer application

  If the protection requirement regarding the authenticity and non-repudiation of a customer application is "None", then no authentication of the customer is required.

  If the protection requirement regarding the authenticity and non-repudiation of a customer application is "Basic", then an authentication procedure that plausibly identifies the customer is required. This can be done, for example, by stating an e-mail address or a residential address.

  If the protection requirement regarding the authenticity and non-repudiation of a customer application is "Medium", then an authentication procedure in which the identity of the customer is confirmed by an independent entity is required.

  If the protection requirement regarding the authenticity and non-repudiation of a customer application is "High", then an authentication procedure which makes it possible to verify the identity of the customer beyond all doubt is

required. However, this does not necessarily mean that the evidence has to be supplied at the time at which the application reaches the agency.

For example, the customer could add a qualified electronic signature to the application. This would make it possible after the event to unequivocally attribute the transmitted document to this customer, with reference to the certification service provider who issued the certificate used. However, it will only be possible to attribute the application to the customer at the time at which it is received by the agency (ex-ante authentication) if such data is stored in a root certificate or attribute certificate which permits unequivocal identification.

If the protection requirement regarding the authenticity and non-repudiation of a customer application is "Very high", then an authentication procedure which makes it possible to verify the identity of the customer beyond all doubt is required. However, here the evidence must already be available at the time at which the application is processed.

- Authenticity of the agency

  If the protection requirement regarding the authenticity of the agency as recipient is "Basic" or "Medium", then the agency should provide the means by which the customer can verify its authenticity.

  If the protection requirement regarding the authenticity of the agency as recipient is "High" or "Very high", then the agency must provide the customer with the means to verify its authenticity. However, this must be based on confirmation by independent third parties.

  For example, a public agency could use a certificate issued by a trusted certification body.

Output

- Confidentiality

  If the protection requirement regarding confidentiality is "Basic" or "Medium", then it is desirable but not absolutely necessary to encrypt data sent from the agency to the customer.

  If the protection requirement regarding confidentiality is "High" or "Very high", then it is imperative that data transmissions from the agency to the customer are encrypted. If encryption is not possible, then a conventional communication channel (post, formal delivery etc.) must be used.

- Authenticity and non-repudiation of agency services

  If the protection requirement regarding the authenticity and non-repudiation of an agency service is "Basic" or "Medium", then an authentication procedure which makes it possible to identify the customer or have him identified is required.

  If the protection requirement regarding the authenticity and non-repudiation of the agency service is "High" or "Very high", then an authentication procedure which makes it possible to verify the identity of the agency beyond all doubt is required.

For example, the agency could append a qualified electronic signature to the notice.

- Authenticity of the customer

  If the protection requirement regarding the authenticity of the customer as recipient is “Basic” or “Medium”, then it is necessary to ensure during the electronic transmission that the customer can be addressed.

  If the protection requirement regarding the authenticity of the customer as recipient is “High” or “Very high”, then it is necessary to ensure during the electronic transmission that the customer can be reliably addressed. However, this can be based on confirmation by independent third parties.

If the requirements regarding the authenticity of the customer differ as to input and output, then it can be appropriate to adopt the higher authentication requirement right from the input stage in order that the agency can then apply this to the output.

It is only necessary to work out the availability security requirements from the protection requirements for classes “High” and “Very high”. It is not possible to say any more about these security requirements without knowing the details about a particular transaction.

No separate derivation of security requirements is undertaken with regard to the integrity aspects of a protection requirement, as the same protection mechanisms (electronic signature) are used as for authentication of the transmitted data.

This means that the security requirements regarding the interface between customer and agency that have to be considered during implementation are now known for every online service.

Additional resources provided in the E-Government Manual:

- Module entitled “Encryption and signature”
- Module entitled “Authentication in E-Government”

3.6 Activity "Design of the online process"

Initiation responsibility: Team leader

Implementation responsibility: Core team, Head of Organisational Section, Head of IT Division

The purpose of this activity is primarily to prepare the envisaged optimisation possibilities within the individual processes from the previous activities and to bring them together into planned IT projects. In addition, a basic feasibility check should also be carried out now.

The changes to workflows in the design of the new tasks that either were jotted down using keywords or were written out in full (following the workshop) must be expressed in a form which can be modelled onto the use of IT resources. Blocks of tasks for implementation, responsibilities and time targets must be assigned accordingly. For this procedure it is strongly recommended using appropriate tools (forms, To Do lists etc.). To retain a general view and also to keep processing costs down, it is recommended using a powerful tool on larger projects.

The flow diagrams must be modified accordingly. The extent to which work operations can sensibly be brought together into new sub-processes and, if appropriate, automated through the use of IT resources must be clarified. During modelling, customer-friendly additional options (automated incoming messages or similar) involving the use of IT should be considered.

The IT procedures in operation should be listed. After that, the optimisation approaches from the newly designed tasks which have interfaces to existing IT procedures or which make new IT procedures necessary are collected together and summarised accordingly.

Questions to be clarified

The following points should be clarified in a workshop involving participants from the Organisational Department and IT experts:

- Online suitability of old procedures
- Requirements profile for "new" IT procedures, taking into account the previously identified agency-wide infrastructural procedures (agency-wide use of electronic signatures, encryption, workflows, document management etc.)
- Identification of the additional IT procedures to be modelled
- Boundaries of feasibility of new IT procedures
    - Estimate of the effort required for IT modelling and programming
    - Requirements arising from the assessment of protection requirements and security requirements which cannot be modelled or can only be modelled at a disproportionately high effort.

- Standard products or solutions for partial implementations that are not on the market, so that the costs cannot be estimated.

Elucidation of the problem through "elimination of media discontinuity" example

1. Within a sub-process, laws and ordinances are used in paper form by 15 persons. It has been established that it is very effort-intensive to administer and update these paper versions. In the workshop on the conceptual design, preference was therefore expressed in favour of eliminating the media discontinuity through the use of IT. As the workstations under consideration are basically equipped with the necessary IT and are also networked, implementation of this requirement is not particularly costly. In the list of tools used by *all* the sub-processes concerned (check), the media format is changed from paper to electronic file. It must be stated in the task list for the IT Division that it is responsible for the provision and implementation of access. The Administration Division is responsible for the altered procurement and usage arrangements. (All the other details, such as data format, access rights, backup, interfaces to databases and similar are modelled in Phase 4).
2. The outcome of the work produced by one sub-process is printed out and transported from person A to person B for the next sub-process by in-house messenger. Printing and transportation result in a delay in the processing chain of two days, including idle time. It was established in the workshop that it is not possible for a single person to complete all the work relating to both sub-processes as they require different roles. As an alternative, it was agreed to eliminate the media discontinuity so that the relevant data could be passed on electronically. The possibility of a separate IT procedure has been ruled out as it is not a process that is critical to the agency (it ties up less than 3% of resources). Since up to now customer documents have been passed from sub-process to sub-process, this must now be taken into account from the very first sub-process where the customer's documents arrive. It is necessary to check whether a central online IT procedure or, possibly, a "virtual mail room" is planned as control instrument for all online inputs and outputs. If this is not the case, then first of all a new sub-process must be generated in the sub-process chain to carry out checks for completeness, digitise data and pass it on to the first employee mentioned. The sub-process should be identified as a generic IT process. An agency-wide list should be created for similar cases of document digitisation. Note: as far as the BundOnline 2005 initiative is concerned, a procedure that was entirely online would be preferable, as the interim stage of document digitisation combined with the issue of paper notifications once again involves media discontinuities. At the same time it is necessary to document how the documents received from the customer will be archived and put with the final notice at the end of the process chain. Again, time schedule and responsibilities should be specified in the task list. Outside of the IT modelling, standard organisational procedures and approaches must be

devised (IT procedural rules: co-signature, deputisation etc.). All connectors between sub-processes must be modified accordingly (electronic transfer).

3.7 Activity "Preliminary check of legal framework conditions"

Initiation responsibility:	Head of E-Government Team
Implementation responsibility:	Technical Manager, Legal Department, Data Protection Officer, officer for the Budget Department

Special importance of legal standards in e-government

The provision of e-government services is regulated by laws, directives and other legal standards to a far greater extent than corresponding projects in the free economy. The possibilities of and restrictions on their provision are essentially defined by legal framework conditions. A review of the relevant legal situation will prevent the redesigned service from violating any legal requirements or from failing to use to a reasonable extent any legal freedoms that exist. Such a *preliminary* check must be supplemented at the end of the implementation process by a final and complete legal check of the new service, taking into consideration the legal situation applicable at that point.

The preliminary check of the legal framework conditions should capture both the technical laws that are relevant to a service (the information that is collected during the activity "Collection of information regarding online-capable services" can serve as the basis here) and also the general framework of the administrative process. The general laws that need to be considered typically include the following:

- **Federal Data Protection Act** (BDSG) (and equivalent regulations issued by the German states): the BDSG requires in a large number of cases that adequate *encryption* is carried out on person-related data wherever this is stored, processed or transmitted electronically. The information rights of the citizen vis-à-vis government agencies are also regulated.
- **Procedural requirements**: As a result of the adoption into German law of Directive 1999/93/EC on a Community framework for electronic signatures, numerous procedural requirements are being added as amendments both in private law and also public law, to the effect that under the provisions of the **Digital Signature Act** a qualified electronic signature can replace a manual signature and hence the written form. Of paramount relevance here are the amendments to the **German Civil Code** and the changes to the **Law relating to administrative procedure** (only available in draft form at the time at which this document was created).

Also requiring consideration are regulations such as staff representation rights (e.g. as contained in the Federal Staff Representation Act (BPersVG) and the Employees' Representation Act (BetrVG)), the Distance Selling Directive, the Teleservices Act, the Teleservices Data Protection Act, the Telecommunications Act, the German Interstate Treaty on Media Services, the Information and Communication Services Act, the Interception of Telecommunications Ordinance, the Federal Budget Ordinance etc.

Standard questions

The review of the redesigned service should include consideration of the following questions:

- Is the intended degree of automation of the service compatible with statutory requirements?
- Do the mechanisms envisaged for safeguarding the confidentiality of (person-related) data satisfy the statutory requirements?
- Is data archived for a sufficiently long period and providing the required degree of legal certainty?
- Are the information rights of members of the public to their data guaranteed?
- Will the provision of the service in electronic form create special requirements with regard to encryption and authentication of the data communicated?
- How are procedures to be assessed in which both electronic and also "classical" communication paths are used?
- ....

New law for e-government

During evaluation of the legal framework conditions, it should in any case be borne in mind that a large number of legal provisions that are relevant to e-government are currently being revised (e.g. as part of the BundOnline 2005 initiative). In many cases new possibilities for e-government services are being created as a result. Information on amendments to laws that are either planned or have already been implemented can be retrieved from these URLs: *http://www.bundonline2005.de*, *http://www.bund.de*, and *http://www.staat-modern.de*. Information can also be requested from the ministry responsible for a particular technical law.

It should also be noted that e-government by its nature touches on topics relating to administrative law, for which in many cases no legal precedents yet exist. To avoid the possibility of the agency acting in an improper manner, both regular and event-triggered checks should therefore be carried out as to whether previous evaluations of the legal situation still apply.

Legal Department, staff representatives

To conclude the legal preliminary checks, the agency's Legal Department should be asked to approve the planned implementation of the service. In this way formal certainty of planning can be obtained for the next stages.

Additional resources provided in the E-Government Manual:

- "Legal Framework Conditions for E-Government" module
- Section VII "Legal basis" (loose-leaf collection)

3.8 Activity "Review of evaluations from Phase 2 with regard to effort required and benefits"

Initiation responsibility: Head of E-Government Team

Implementation responsibility: Core team, Technical Manager

Target conformity?

After the form of the planned online process has been provisionally specified in Activity "Design of the online process" (Activity 3.6), checks should be carried out to ascertain to what extent the service to be set up still addresses the public agency's original objectives and whether its introduction in the planned form is justified when examined from a cost-effectiveness point of view.

When reviewing the target conformity, the following questions should be answered amongst others:

- Are those services to which a high priority has been assigned (best) suited to contribute towards achieving the primary agency objectives?
- Have the assumptions which formed the basis on which priorities were set been confirmed in the course of specific planning?
- Have any significant constraints and difficulties or opportunities that are linked to the implementation of the online service been overlooked?
- Can the planned optimisation steps be implemented in the envisaged time schedule?
- ....

The aim of the (provisional) cost-benefit analysis is to find out whether the benefits of the new online service justify the expected cost of designing the associated online processes, viewed against the background of the agency's objectives.

Benefits

On the **benefit side**, it is necessary to check whether the conclusions which formed the basis for assigning priorities between services are still valid, bearing in mind the extra knowledge gained in the meantime and the more detailed planning that has been carried out, and whether, in particular, the agency objectives defined in Phase 2 can in fact be achieved through the services to which priority has been given. If any evaluation forms were completed in Phase 2, then it is recommended critically re-examining the entries made on them.

Effort required

As detailed technical planning of online processes has not yet been performed, it is not yet possible **on the cost side** to undertake any serious monetary analysis at this point. Typical aspects to be covered here would, however, be:

- The extent of redesign that is necessary (especially on the organisational side; on the technical side only in so far as such a judgement is currently possible), taking into account the infrastructural procedures identified in Phase 2.
- Training requirements on the part of the staff affected
- (Relatively great) complexity of the service on the user side

- Dependence on legislative procedures whose timing is difficult to determine
- ....

Additional resources provided in the E-Government Manual:

- Module entitled “Evaluation Criteria for Potentially Online-Capable Services”

3.9 Activity "Updating of e-government strategy"

Initiation responsibility: Head of E-Government Team

Implementation responsibility: Core team, senior management of the public agency

Better knowledge leads to a new strategy

In Phase 2 of the Phase Plan an *e-government strategy* for the agency was drawn up through specification of the agency's objectives with regard to e-government, along with selection of suitable services and the drawing up of a high-level resource plan. However, as this is only based on the results of a data-gathering exercise, it cannot consider either functional or technical details of the newly designed services. It is therefore recommended critically viewing the strategy at the end of this third phase and, if appropriate, revising it. In particular, the results of the preliminary check of the legal framework conditions and of the provisional cost-benefit analysis should flow in here.

Typical results

The deliberations typically result in one (or more) of the following conclusions:

- **The strategy determined in Phase 2 does not require any modification.** All the underlying assumptions have been confirmed in Phase 3. The timetable can be adhered to.
- **The process modifications required to implement the online service will cause delays to completion of the project.** In this case the timetable will have to be modified accordingly. If rapid implementation of the online service is still desired, consideration can be given to implementing transitional solutions, taking into account the relevant cost-benefit considerations.
- **Certain services selected for priority implementation do not contribute to the required extent towards accomplishment of the agency objectives or in fact are proving to be restricting.** In principle, there are two possible responses here:
  - The corresponding services are given a lower priority in the implementation plan or even cut right out, or
  - The agency objectives must be revised. However, this option should only be used in case of "emergency", i.e. if, for example, no online-capable services can be found which are really suitable for achieving the objectives.
- **Some of the planned online services are too effort-intensive to implement.** Possible responses:
  - The corresponding services are given a lower priority in the implementation plan, e.g. moved back until certain unfavourable framework conditions have changed or have been completely eliminated, or
  - A check is carried out to ascertain to what extent transitional or partial solutions can be implemented for a limited period at lower effort.

- **Some planned services cannot be implemented at all due to legal restrictions or else they can only be implemented to a limited extent, e.g. with less automation.** Depending on whether changes in the legal framework conditions can be expected in the foreseeable future, plans for the services concerned must be modified, cut out or temporarily set back. Here again the possibility of implementing transitional solutions should be considered.
- **Through changes in the legal situation that have either come about or are expected in the foreseeable future, certain online services can either be offered as extras or their scope can be expanded.** These "new" services must be checked in accordance with the suggestions made in Phase 2 and should be integrated into the implementation plan, to the extent that this is possible with the resources available.
- **Certain services can be carried out on the back of other services with which they can be "bundled" relatively cheaply.** These services should be included in the implementation plan for the purpose of rounding off the service portfolio of the agency.

Approval by senior management of the agency

The results of the review of e-government strategy must be presented to senior management for approval. Senior management must then decide whether and to what extent publication of a new set of e-government guidelines is necessary and desirable. The E-Government Team should draw up a proposal on this matter.

It is essential that the staff representatives are included in these activities. The Staff Council is involved firstly in connection with the rights of co-determination under the Federal Staff Representation Act and the Employees' Representation Act, but in any case it should be involved in good time prior to the introduction of new technologies and procedures, to eliminate the possibility of unnecessary hurdles raising their heads due to any failure to have kept the Staff Council informed or allowed it to become involved.

3.10 Activity "Briefing of all those concerned"

Initiation responsibility: Head of E-Government Team

Implementation responsibility: Core team, Public Relations, senior management of the agency

Keep talking

As a result of the functional design of the planned online services and the associated review of e-government strategy, the agency's e-government plans will have gained significantly in binding force compared with the situation at the end of Phase 2. As well as providing fresh information to the staff and staff representatives about the stage reached in the implementation plan, the question of to what extent customers and partners affected are to be given more information should also be considered during this phase. These activities should be co-ordinated with the general public relations work and must ultimately be approved by the head of the agency.

Realistic expectations

When relatively large user groups are to be informed, it is essential precisely at this early phase of the project to avoid arousing expectations through premature promises or over-ambitious timescales which later on may be disappointed and thus in the long-term do more harm than good to the image of the agency. Such negative effects should be avoided by exercising a reasonable amount of caution both in form and content. For this purpose it is helpful if the E-Government Team prepares an estimate of the remaining project risks.

Objectives

Several objectives can be pursued through briefing of those concerned. These include:

- **"PR effect"**: the agency shows the outside world that it is actively taking on board the requirements and possibilities of internet technologies. As well as press releases, attendance at trade fairs and public lectures, the agency's existing website is naturally particularly well suited for this form of public relations campaign. The risk of a negative effect from arousing excessive expectations is of course especially high here.
- **Feedback, active participation of outside parties**: the agency should now, if not before, be in a position to discuss its e-government plans in detail with the parties involved, to respond sensibly to their suggestions and, if appropriate to consider these in further stages of planning. Depending on the scope and composition of the customer and partner groups, different approaches are recommended. While the establishment of e-mail and telephone hotlines allows large numbers of members of the public to get involved, in the case of small groups of users who are mostly known to the agency it may also be appropriate to hold workshops or to set up appropriate working parties in some cases. Inclusion of trade associations, political committees or attendance at technical conferences etc. can deliver valuable information. The web pages need to be reviewed for accessibility; user tests must also be carried out with disabled users[3].

[3] See "Accessible E-Government" module, Chapter 5.

- **Planning security on the user side**: in a few cases there will be a desire or even a necessity for external users to enlarge or safeguard the value added by the new service using its own technical and organisational measures (e.g. through the procurement of signature smartcards, registration with providers of online payment methods, modification of internal IT processes or formats on the side of the users etc.). By providing information to customers and partners early on regarding the forthcoming changes, the planning certainty is increased and hence, ultimately, the willingness and ability of those parties to accept the services online.

7 Checklists

The following checklist can be used to ascertain whether all the essential results of the present phase are available. It can also be used where the above activities have been carried out in a different order or in a different form.

7.3 Checklist for Phase 3

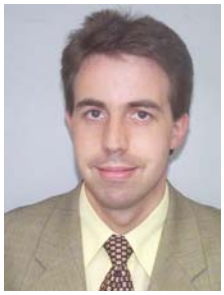
Outcome(s)	**Who?**	**When?**	**Done?**
Processes have been recorded			
Processes have been optimised and designed			
Protection requirement has been determined			
Legal framework conditions have been checked			

9 Author Profiles

Rainer Belz, BSI

After obtaining a degree in Public Administration, Rainer Belz worked for several years as an administrator in personnel and organisation at the alternate site of the highest constitutional organs of the Federal Government (government bunker). On the basis of his expertise in information science, he performed numerous functions in the areas of IT security and IT co-ordination. He was responsible for the introduction of IT resources, the technical and organisational measures that had to be taken and their planning and implementation at the highest federal authority. Since 1999 he has been employed at the Federal Office for Information Security BSI as an IT security consultant, concentrating on technical infrastructure and communications technology. He is responsible for IT security analyses at medium-sized public agencies and is also involved in the development of new security analysis methods and procedures. As one of the authors of the E-Government Manual, he is responsible for the model projects of the BundOnline 2005 initiative.

Dr. Christian Mrugalla, BSI



After obtaining a first degree and PhD in Physics from the Technical University of Clausthal, Christian Mrugalla joined the German Information Security Agency in 1998 as a section head. As well as providing general IT security consultancy to (federal) public agencies and involvement on the continued development of the IT Baseline Protection Manual, he is heavily involved with the BSI "Digital Signatures" project office, providing consultancy on e-government projects in which this technology is used. As an advisory member of the "Digital Town Hall" subgroup of the Deutscher Städtetag umbrella organisation, Dr. Mrugalla also supervises the implementation of e-government initiatives in local government.