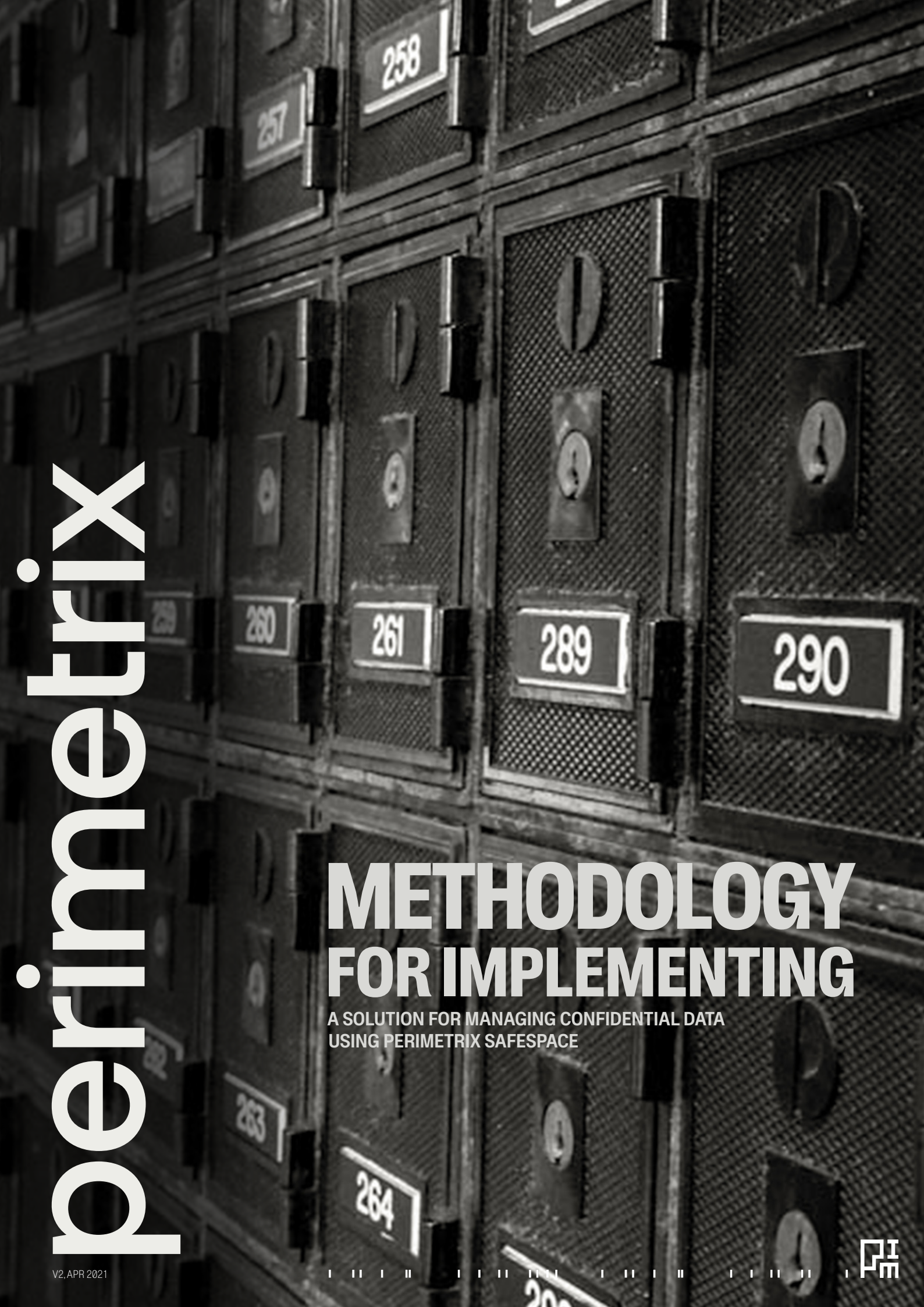
perimetrix



METHODOLOGY FOR IMPLEMENTING

A SOLUTION FOR MANAGING CONFIDENTIAL DATA USING PERIMETRIX SAFESPACE

V2, APR 2021

Contents

Abstract

Any business, regardless of its size and/or complexity, operates within the framework of a particular business model. The business model, in turn, is dependent on a set of instruments which enable the organization to succeed when competing against similar organizations. Together, the business model and the associated tools form a symbiotic relationship. Because of this symbiosis, it makes little sense to consider the two elements individually.

In terms of digital tools, companies do not usually create or implement them by themselves, but often involve specialists from the IT industry. When implementing out–of–the–box solutions, consultants from either the vendor or one of its partners are often used.

As within any sphere of business, the IT industry has its peculiarities and works according to its own set of rules. Given the particularities of project work, a business can usually get a much better result when taking into account these industry–specific practices rather than by ignoring them.

The Perimetrix SafeSpace solution is also a digital tool, one designed to classify and manage confidential data. Successfully managing confidential data is achieved by applying restrictive data storage, processing, and transmission policies that are configured to meet the organization's requirements.

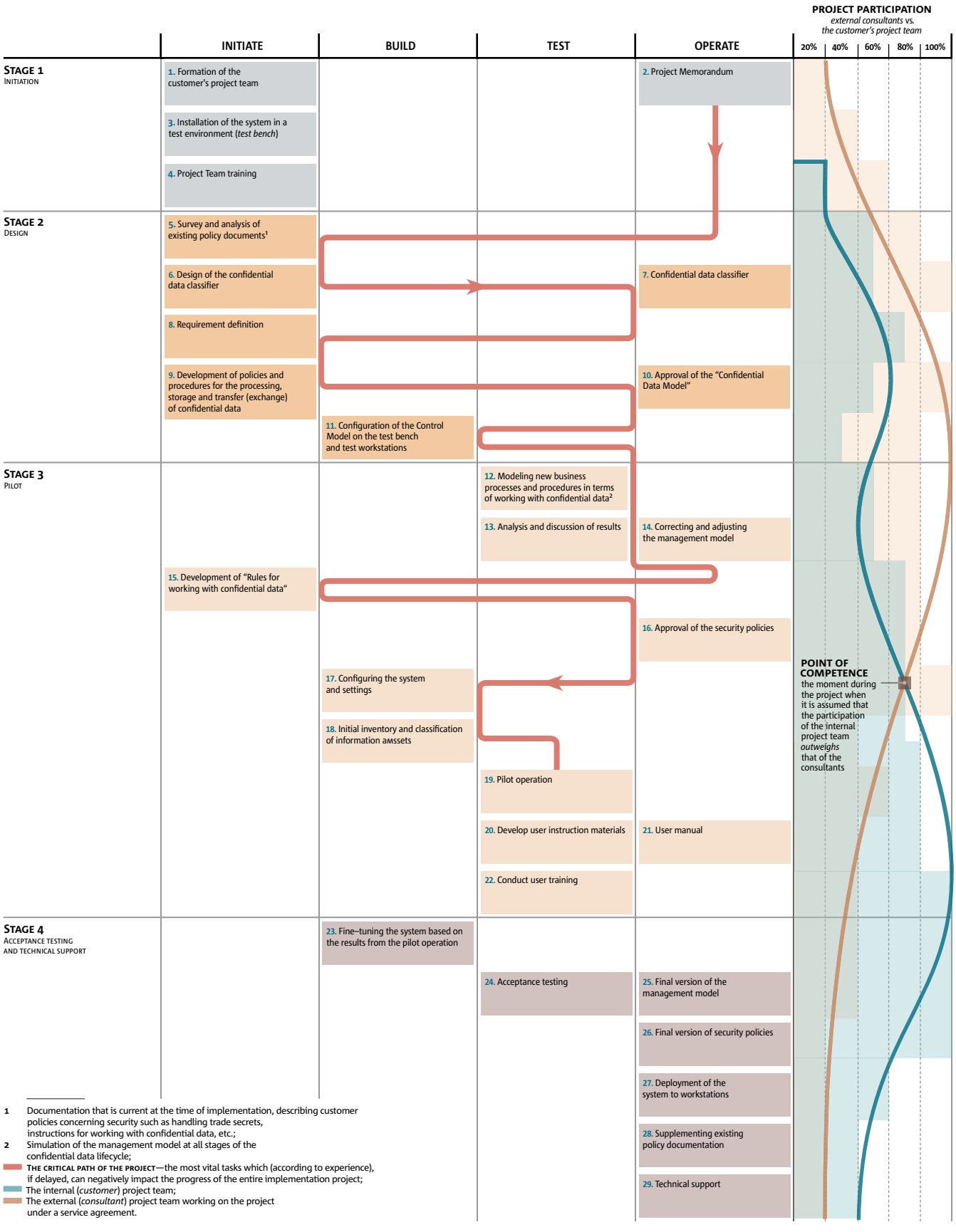
Even though Perimetrix is a readymade solution, using it does, however, require a certain number of preparatory procedures, activities, and documents. These are necessary in order to configure the system so that it meets the needs of the customer. All of these things combined make up the methodology for implementing Perimetrix, which is described in this document.

This document summarizes the basic principles for implementing Perimetrix. These principles are *based on actual projects completed* for clients representing a wide variety of different industries. Moreover, this document provides organizational and methodological recommendations in order to organize activities in the most effective manner possible.

It is assumed that the approaches and guidelines described in this document will be understood as general recommendations. It is anticipated that these recommendations will be in great demand by both customers and partners when developing effective and feasible implementation plans.

Implementation Roadmap

Typical structure and sequence of project activities



1 Documentation that is current at the time of implementation, describing customer policies concerning security such as handling trade secrets, instructions for working with confidential data, etc.;

2 Simulation of the management model at all stages of the confidential data lifecycle;

THE CRITICAL PATH OF THE PROJECT—the most vital tasks which (according to experience), if delayed, can negatively impact the progress of the entire implementation project;

The internal (*customer*) project team;

The external (*consultant*) project team working on the project under a service agreement.

Data Management Model

The confidential data management model

The Perimetrix SafeSpace confidential data management system includes a set of pre–designed and tested solutions and programming components. The suite of components and their configurability define the overall capabilities of the solution.

Configuring the Perimetrix solution follows a process using a predefined set of parameters. The values of these parameters must be established at the very beginning of the project, during the pre–project survey. The settings are formalized in the form of a document called the *"Confidential Data Management Model"*, subsequently referred to simply as *"the data management model"*.

Model (French *modèle* from Latin modulus meaning "measure, analog, sample")—is an abstract representation of reality in some form, designed to represent certain aspects of this reality and allow you to get answers to the questions you are studying.

The data management model is a document and plays a key part in the implementation of the Perimetrix solution. The data management model document interprets the configuration settings in terms of the business environment as well as the existing customer policy documentation.

It describes the lifecycle of confidential data in Perimetrix terms. The main goal of its devel-

opment is *to reduce uncertainty* in the implementation of the solution. The ultimate goal, of course, being to deliver the exact results that the business is expecting to get from using Perimetrix products.

Of great importance here is not only acknowledging that uncertainty exists, but also in understanding where in the project uncertainty is located or can manifest itself. In this context, it can be argued that the data management model, when developed with the required level of detail, actually minimizes uncertainty, thereby reducing overall risk to the project.

And here we are talking primarily about the organizational side of the issue. This includes things like getting a clear set of requirements for the system as well as resolving various issues related to finding qualified specialists for the internal project team.

The data management model is a key instrument for designing the system prior to its implementation. If an error is detected during its preparation, the consequences will be significantly lower than if the issue were only discovered during the actual implementation phase. Figuratively speaking, it is better to discard lots of bad ideas than to jeopardize the final product.

Here, the primary role is played by business representatives (i.e., the data owners). If we neglect the business during the design phase of the project, then instead of receiving well–developed project documentation, the customer risks getting a fragmented set of functional requirements. This fragmented set of requirements is very often interpreted as a simple set of "technical tasks".

Goals and objectives

The data management model is designed to address the following objectives:

Define the content of confidential data assets, identify any existing security policies, and describe existing processes for handling confidential data;

Classify data assets according to customer requirements using Perimetrix notation;

Develop access policies for handling confidential data, including policies related to the storage, processing, and transfer of confidential data;

Describe the workflows for creating, storing, processing, and transmitting confidential data, including:

1. a list of workstations that can process the data in any given category;
2. a list of users (user accounts) that are allowed to access the data;
3. a list of applications that are allowed to process the data;
4. a list of acceptable file formats for storing the data;
5. a list of acceptable locations for storing the data, including server locations (network folders, DBMS, etc.);
6. a list of permitted peripheral devices;
7. a list of printers that are allowed to print the data;
8. business process diagrams for data processing, including permitted storage locations, allowed applications, etc.;
9. procedures for disclosing confidential data to third parties.

The Data Management Model addresses three key aspects related to confidential data: *what*, *who*, and *how*. First, what is protected; second, who can access what is protected; and third, how access is managed. In other words, how we control the processing, transmission, and storage of confidential data. The model describes in detail what "access" means for users, applications (and application processes), devices, as well as the confidential data that is under the control of the system. Ideally, this document should serve as a supplement to any policies that the customer already has regarding confidential data such as trade secrets. It should further support any other policies related to handling electronic data that may contain confidential information.

Typical structure and content of the data management model

Below is an example of the content of the data management model, divided by section.

Section 1: "Project Information". Defines the goals and objectives of the project; describes what information is to be considered confidential data and provides a high–level definition of current threats to the security of confidential data.

Section 2: "Baseline information regarding confidential data". Classifies the types of confidential data by function (for example, corporate document management, business development and planning, personnel management (HR), etc.) and by corresponding information systems (accounting systems, databases, etc.). In addition, for each of the classified data types, a description of the handling process is made which includes all stages of the data lifecycle (creation, use, transfer, storage and retirement).

Section 3: "Organizational structure for processing confidential data". Defines a list of business units (e.g., divisions, departments, etc.) and the confidential data that is processed within each unit;

Section 4: "General principles related to the build of the system".

Section 5: "Assets to be safeguarded". Contains a register of all information systems involved in the processing of confidential data, including the corresponding classification

code of the asset defined earlier in "baseline information".

Section 6: "Classification dimensions and levels". Introduces the concept of data classification *(see box below)*, classification dimensions, and classification levels. These are based on the project goals and objectives, information security policies, and customer rules and regulations.

Section 7: "Permissible storage locations and transmission channels". Generates a register of classified data using the following notation: *name/allowed storage locations/allowed transmission channels*.

Section 8: "Software tools and applications that are allowed to work with confidential data".

Section 9: "User roles and permissions". Introduces the concept of a user category for the system. This provides a detailed description of the work scenarios that involve classified data for each user category.

Section 10: "Data Management and Processing Policies". A supplement to existing internal policy documents, which defines the administrative and technical rules for data storage and processing. This is implemented through the installed and operational Perimetrix system.

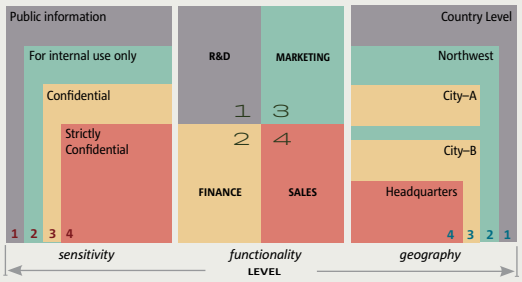
Section 11: "Process description for handling confidential data". A functional scheme for the system that is to be implemented. The scheme contains descriptions of the processing sequence for each category of classified data and the corresponding information system included in the functional and technical scope of the project.

Data Classification In Perimetrix

The Perimetrix security doctrine is based on the Data Centric Security Model **(DCSM)**. It was first defined[1] in 2007 and proposes the idea that data should classified based on its importance to the relevant business processes. In practical terms, this means that the level of security assigned to data must be appropriate given its business value.

This approach makes it possible to establish a solid link between the technical competence of information security specialists and the knowledge of data owners regarding the role that information plays in achieving business objectives.

It does not replace, but rather complements the traditional, "flat" classification applied in the context of "trade secrets", "confidential information", "personal data", etc. All confidential data is classified in such a way so as to ensure the necessary *granularity* needed when managing access permissions. For example, managing access by defining the level of confidentiality (*sensitivity*) and the actual contextual meaning of the data (*thematic*). The latter allows you to classify information using the *business context* and to manage data access permissions accordingly. Access is controlled for users, applications or IT devices that are involved in the corresponding business process.



Example 1: Multi–level classification.
An example of a three–level data classification model categorized by *sensitivity*, *functionality*, and *geography*.

More information on: https://www.perimetrix.com/

1. "*Elevating the Discussion on Security Management—The Data Centric Paradigm*" by IBM Research, IBM Security & Privacy Services, Zurich Financial Services; "*Enterprise Security: A data—centric approach to securing the enterprise*" by Aaron Woody

Rules and Regulations

Rules and regulations for working with confidential data

This document, as well as *the data management model*, is a guideline. It is developed during the third stage of the project in parallel with the configuration of the test system. It contains a description of the rules, policies, restrictions and instructions regarding the processing, storage and transmission of confidential data. It also describes which data is to be safeguarded and under the control of the data management system based on the Perimetrix SafeSpace solution.

Its purpose is to provide a detailed description of how users interact with the solution, depending on the defined and implemented classification and security policies.

In particular, it describes in detail the procedure for executing work activities related to the processing, storage and transmission of data that is managed by the Perimetrix solution.

It contains a description of the rules (policies and restrictions) and instructions regarding the processing, storage and transmission of confidential data that comprise the customer data to be safeguarded.

The starting point for developing the regulations document are the design results obtained during the 2nd stage of the project, as well as any existing policy documentation from the customer.

Policy documentation can include "policies regarding trade secrets", "classification of data containing confidential information" and other local policy documentation regarding information security of the customer.

"User rules and regulations" is the final decomposition of the system design. This includes everything from the level of security policies approved in the data management model, through the workflows of data storage, processing and transmission, down to the level of users, applications and the technical means involved in the handling of confidential data.

Typical rule content

The developed and approved rules and regulations should contain, as a minimum, the following (**stage 3**):

- *confidential data,* its composition and classification;
- *rights and responsibilities* of the system's users;
- *general requirements* concerning user activities;
- *user modes of operating* with confidential data;
- *configurable policies* for working with confidential information;
- *description of user operations* when working with files in the system. This includes detailed scenarios for interacting with the system at each stage of the confidential data lifecycle (reading, writing, storing, moving, etc.), specific to the particular system installed and specific business processes of the customer.

The Project Team

The role of the internal (customer) project team

The project team is, first and foremost, a group of professionals who are able to translate business requirements into the appropriate language describing the functional and technical requirements for the Perimetrix system. This team of specialists acts as a single entity, which not only has all of the qualifications required, but also clearly understands current and future business needs.

However, if the complexity of the solution, or more precisely the IT systems underlying the solution, were equal to the sum of its parts, then the level of expertise needed wouldn't be so high.

The complexity of the system, however, is actually not determined by the parts but by the relationships between the parts. And in order to properly define these relationships instead of allowing them to develop chaotically, there is a clear need for an internal project team.

Its task is to find the best way to organize the system, taking into account both the available technical capabilities and limitations of the out–of–the–box solution, as well as the customer's business requirements combined with specific business expertise.

Another important factor highlighting the importance of the internal project team is the ability to derive the maximum capabilities from the implemented system. This should be done within existing project management guidelines and also by attracting qualified external experts.

The most common way of working, that of freelancing, is gradually losing its ability to effectively solve many business problems that arise. The level of professional competence required from all project team members far exceeds the skills and experience typically possessed by an external project manager. As a result, both the business and the project team members are forced to interact in ways that overly simplify the

issues discussed.

Neither the precise definition of goals, nor the thorough design of a well–developed security model, can eliminate the fundamental source of uncertainty, namely, the actions of the people involved in the project and in deploying the system on the ground. Ultimately, the success or failure of the project depends on the decisions the project team makes. Therefore, the formation of a project team is one of the key factors determining the success or failure of an implementation project.

All of the above should make it clear why an internal project team is critical to the success of the project. This applies equally to technical solutions, user interface solutions, and business scenarios.

Sometimes a bad situation can be salvaged by having the necessary expertise on the side of the company providing the consulting services. This expertise can come from the vendor itself or from a partner company. Ultimately, however, in order for the project not to rely on chance, the business itself must understand both the criteria and the method for selecting suitable specialists.

Ideally, on the business side, there should be people who understand both the project activities as well as having good IT knowledge. The consequence of not having this expertise is that the customer can become a hostage to the goals of the consulting company, overpaying for the time of external consultants.

Almost every IT product evolves along with the business. When a business is established and operating, changes in the external environment require constant updates within the company. Such updates are often evolutionary in nature. For example, when tools and business processes develop gradually over time to meet business needs. In many cases, the actual business model itself does not significantly change.

If the circumstances are such that minor adaptations are not enough to continue to support the business, then significant changes may be required both to the business model as well as the tools that support it.

In both situations, the internal project team plays a leading role in this process, adapting the Perimetrix products to the changing needs of the business.

Approaches to setting up the project team

Anyone who has ever organized a project understands that simply hiring the right specialists is not enough to get the desired result. It is necessary to establish rules and to structure project tasks in such a way that each member of the project team has both the motivation and opportunity to realize their professional potential. As soon as more than one person is involved, the question arises of how the team will interact and which principles should be used to build the project as a whole.

The choice of specialists should be determined by objective needs driven by the project goals, the type of project, as well as the technological specifications of the system to be implemented.

An important aspect of any project is the role played by the cohesiveness of the project team. Only amateurs structure projects purely based on roles, not taking into account the particular characteristics of the team members. They often don't realize that people will sometimes spend more effort on competing with each other, rather than on achieving team, and subsequently, their own objectives.

Last but not least, one must consider the level of trust that the business has in the members of the project team. Without a high level of trust, the business will be forced to limit, possibly through official policies, the project team's freedom to act. Only with sufficient trust will the project team be granted the authority which is essential to achieving their full potential.

The role of the internal project manager

There must be *one person* on the project team who has the authority to make final decisions. We are certainly not talking about someone who makes arbitrary and irrational decisions, nor someone who rejects common sense and project goals.

However, when the situation arises where the project team members cannot agree, someone is needed who can take responsibility for making decisions.

The absence of a strong project leader is no less risky than the other factors mentioned earlier *(more details in the section on project risks)*.

As with any project, during implementation, a large number of issues, of varying degrees of importance, regularly come up. Some of the issues are technical, some are related to clarifying requirements, while others concern organizational issues.

In any case, if the issue is not resolved in a timely manner, then the internal "debt" of the project increases along with the issue itself. For example, if functional requirements for the system are not defined on time and work progresses, then at some point it may become impossible to fully implement and integrate all of the necessary functionality. Consequently, the overall cost to the business can be significantly higher than the cost of a few more months of project work.

It may seem logical for a business representative to assume the leadership role of a project. The problem with this approach is that even though the person may have the authority, especially due to the client–customer relationship, they may not be willing to accept responsibility for project decisions.

Furthermore, many issues are usually related to the technical aspects of the project, and cannot be resolved without specific technical knowledge. Nor is it possible to rely only on administrative tools.

Therefore, the role of a project leader requires someone with both responsibility and authority to resolve issues, as well as sufficient technical competence. The leader should be able to essentially work in the aria where all aspects of the project intersect.

Project Risks

In this section, we have tried to summarize some of the most common uncertainties and their associated risks. This list is certainly not exhaustive since every customer is unique. Therefore, we highlight only those risks that, in our experience, are most likely to arise and which have the highest potential to negatively impact the project.

Project goals and objectives

The main source of risk and uncertainty in any project is the lack of clear project objectives. Historically, many projects implementing out–of–the–box IT solutions, have been viewed by the business as a way of solving all of their problems at once. A kind of magic pill to cure all of their ills, including organizational ones.

The Perimetrix solution certainly is a powerful IT tool. But a tool remains a tool and must be eventually used in order to get any benefit from it. It makes no sense to expect developers to be able to implement business logic if the customer is not able to formulate it themselves. In turn, the business is more likely to get the desired results if the goals are clearly communicated at the beginning of the project. Therefore, it is important that these goals are defined at the very beginning of the project. Moreover, the goals should be articulated using language that accurately and unambiguously reflects the expectations of the business and can be clearly interpreted by all project participants.

Of course, the Perimetrix solution, like any digital product, can be implemented based solely on formal business concepts, but that means that it will only perform functions that meet formal, rather than actual business goals. In other words, it will not be very effective. Therefore, when designing a solution based on Perimetrix SafeSpace, the key task is to not only find the most appropriate solution for safeguarding confidential data, but also to understand, in principle, what the actual requirements for working with confidential data are. Moreover, having clearly defined requirements will facilitate any future efforts to evaluate the effectiveness of the implemented solution, especially in terms of its ability to meet those very requirements.

Engaging the business and managing expectations

A complex product, such as the Perimetrix solution, is like a plant that needs to be grown and cared for in an environment where it can thrive. Organizations work in symbiosis with digital tools, relying on them to implement specific business models to support their activities.

Therefore, implementing such a system should involve gradually adapting and fine–tuning both the company's business processes as well as the supporting technical products and solutions.

The situation is quite different when a company expects to get everything all at once. This “big bang” approach has the disadvantage of depriving the project team of the opportunity to test hypotheses during implementation. Not being able to test the workability of the design at different stages in a real environment leads to the accumulation of uncertainty for both the project and the business.

In the majority of cases the initial requirements for the project are usually based on assumptions about how the company operates. The requirements can come from either management or regular employees. However, neither sees the whole picture because a representation, regardless of quality, is still only a simplified model of reality. And even if we assume that the original model is correct, there are some aspects which are bound to change during the time when the project is being executed.

This approach is also fraught with risk since the business, by delaying hands–on experience with the actual product, tends to over inflate expectations and consequently considers the solution a panacea for all problems. That is why it is often the case that during the course of a project, long before its completion, a large number of additional functional and “nice to have” feature requirements magically appear. This of

course, only exacerbates the growing discrepancy between the actual needs of the business and the final results that the project delivers.

A good illustration that the business does not always understand its responsibility for the results of the project is a situation where a practically completed system is presented to business leaders.

In real life, company executives often consider themselves entitled to give an assessment and express their desires about how an almost finished product needs to be finalized. This happens despite the fact that they likely never paid any attention to the project while it was being developed or implemented.

Obviously, by the time the solution is presented to the customer, the project has already gone through every stage from concept, to design, development and finally, testing. The number of interconnected elements in such a complex solution are enormous. Any attempt to make changes, regardless of how insignificant they may appear, requires a review of all of the decisions made previously. As a result, it will be necessary to go through the entire project lifecycle again.

Businesses traditionally believe that responsibility for these issues lies with the implementation team who did not notice "obvious mistakes" and consequently failed to address them. The implementation team, in turn, appeals to the fact that the "missing functionality" being demanded was never defined in the original requirements.

To avoid such a situation, the business needs to accept equal responsibility for the final results and to ensure that it actively participates throughout the lifecycle of the project. Managers should be involved in making policy decisions throughout the course of the project so that risks do not accumulate unseen. By the time the project is completed, it is already too late to address many issues that were not identified earlier. By engaging the business at every stage of the project, the final operational product will be the result of a joint effort involving all parties. The biggest advantage of this being that it will not require additional resources to be completed.

The participation of *data owners* in making fundamental decisions on the project is key. This will help to ensure that the implemented system adequately reflects the customer's requirements. The earlier the business begins getting acquainted with the system, the lower the risk of deferred requirements either for the system itself or for any implemented functionality.

Responsibilities of the internal project manager

Each of the project team members, looking at the project from the perspective of their specific role, makes decisions based on what they believe needs to be done. This perspective naturally restricts decision making to limited parts of the project.

What is needed within the project team, therefore, is someone who can view the entire system as a whole and make decisions accordingly. This applies to all aspects of the project, especially when we consider the Perimetrix system as an integrated part of the company's business model.

If a person with the appropriate level of responsibility joins the project only at the very end, it will mean that work performed and decisions taken throughout the project were based on unconfirmed hypotheses. Consequently, when testing begins, many decisions will have to be revised, impacting the results from the work that was done previously.

Another important aspect concerning the responsibilities of the project manager is the preparation and coordination of project decisions within the company. Experience shows that with insufficient responsibilities, the implementation of key decisions is often delayed. This inability to make timely decisions relevant to the project is not usually a matter of malicious intent.

As a rule, this is due to the fact that several divisions or department within the company are engaged in the requirements approval process. Since each group has its own business objectives, it is unlikely that they will easily be able to reach an agreement on requirements, and may even choose to postpone decisions indefinitely.

What is needed here is someone who sees the whole picture; someone who can imagine what the final product will look like and focus on getting it launched into operation. At the same time, this person must have administrative skills and a sufficient level of responsibility to coordinate and, if necessary, accelerate the adoption of management decisions within the organization.

Business Consulting

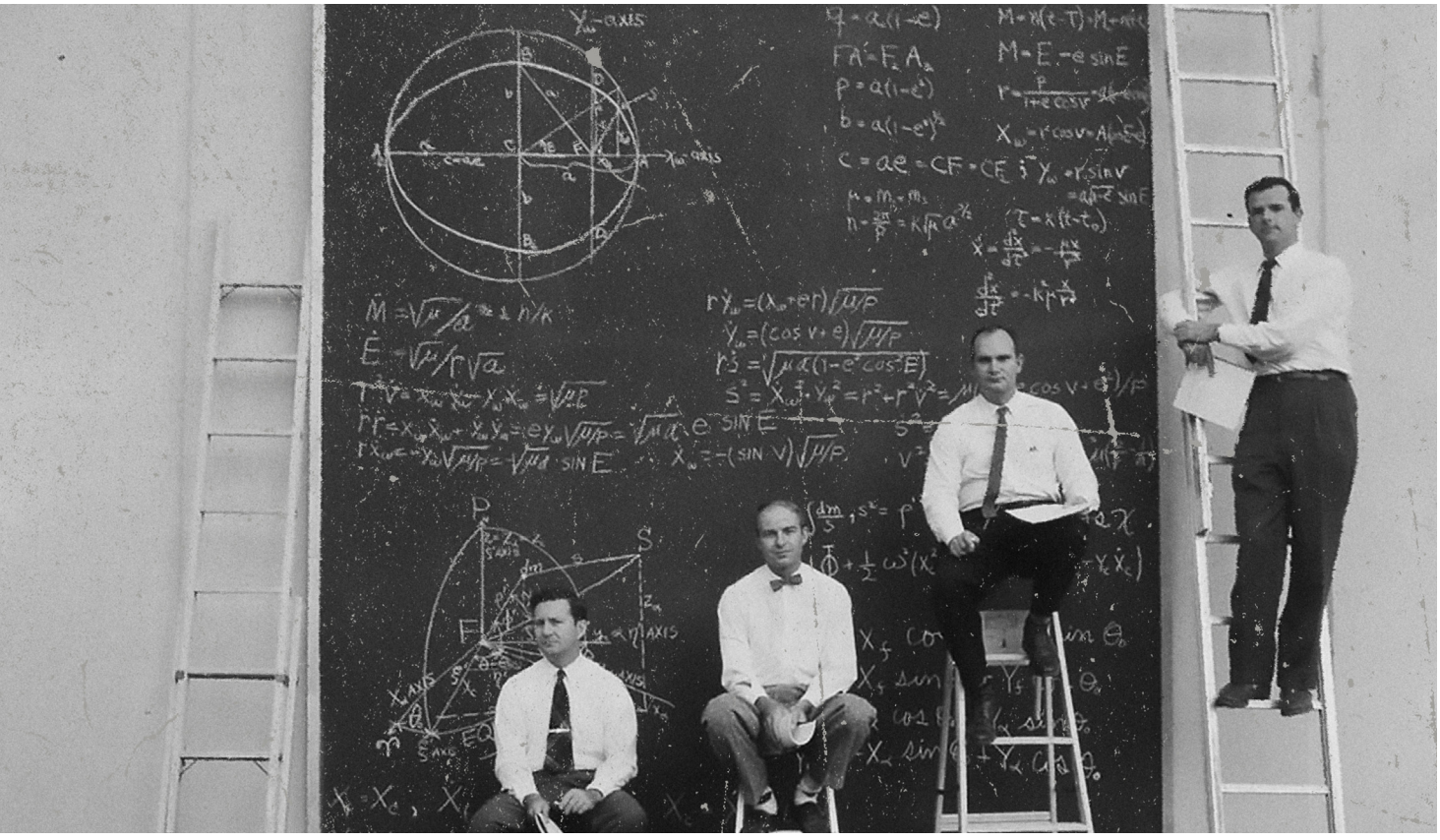
In today's business world, the leading companies are those that are able to connect their business models with the right digital tools. However, in order for such a strategy to succeed, it is not enough to follow a "business as usual" model where IT is seen simply as auxiliary infrastructure similar to office space or communication tools. Moreover, the value derived from IT should be significantly more than increasing the relative speed at which business processes are executed.

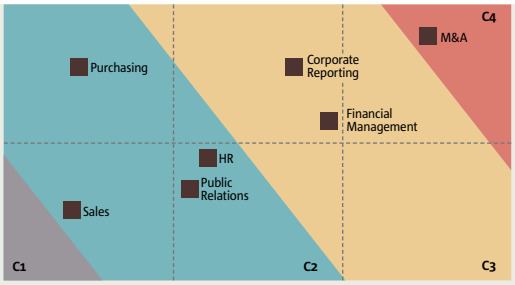
Digital systems are the very heart of today's business. They are the foundation, the skeleton upon which the business model is built. These are not merely the latest buzzwords and phrases, but the reality in which we live.

The external environment in which a company operates is constantly changing. And in order to survive, the company itself must continuously adapt to change. This means that businesses are continually updating their processes and infrastructure, including their digital infrastructure.

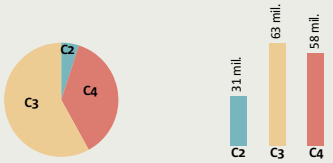
Creating effective digital solutions that can be woven into the business model requires clarity about the model itself. Additionally, modern digital systems are no longer simply the basis for automating existing processes. While automation does make everything run a little "more efficient", modern digital solutions, in a way, are the very structure upon which the entire business is built.

In the context of information security, questions are often raised regarding the point where business and digital technologies intersect. For example, how effective are the implemented security measures when looking at the company's long–term development strategy? Or to what extent does the existing IT portfolio, specifically products related to data security, meet business objectives? How do data security solutions support current and future business activities





Example 2: Classification of business processes and data.
A data classification model from a telecom/mobile operator company. The model is divided into levels C1—C4, depending on the value of the business processes with which the data is associated. The horizontal axis indicates the estimated damage in absolute terms from a data breach. The vertical axis indicates the probability of such an event occurring given the existing organizational and technical security measures implemented at the customer.



Example 3: Distribution of classified objects by levels of confidentiality and cost of compromise.
Referencing the same customer, here data assets are divided by their level of confidentiality and the business processes that they are associated with. On the left the data assets are distributed by level of confidentiality. On the right, data assets are distributed in terms of the financial damage resulting from a data breach (the value of assets "at risk").

such as sales given an ever–changing competitive environment?

These and other issues are addressed within a separate category of work, usually referred to as *"business consulting"*. Business consulting may include, for example, some of the following activities:

—Developing *a set of criteria* for evaluating the effectiveness of the implemented confidential data management system;

—Developing *a methodology* for analyzing the feasibility of implementing the system, including activities such as:

1. determining the value of information assets which are at risk and any potential damage resulting from their compromise (AVR, assets value at risk);
2. calculating the total cost of ownership of the system (TCO);
3. calculating the return on investment of the system (ROI);
4. recommending metrics that can be used to assess the effectiveness of an implemented confidential data management system. ■

The above list is not intended to be comprehensive and is provided here for *illustrative* purposes only. The above activities are not included within the framework of a standard implementation and are outside the scope of this document. They can, however, be provided *upon request* by Perimetrix partners who are experienced in business consulting and have all of the necessary qualifications.

perimetrix © 2021 Perimetrix LLC

A Russian company founded in 2007, whose products have been trusted for more than 10 years to protect the confidential data of organizations such as AvtoVAZ, Gazprom Energoholding, the Federation Council of the Federal Assembly of the Russian Federation, TVEL and others. The company has a network of partners in Russia and abroad. The company's headquarters are located in Moscow.