An Internal Control Framework in a complex organization

René s'Jacob RA
is head of Planning & Control of the Dutch Police Service Centre.

Claudia Voll
is a senior consultant at KPMG IT Assurance & Advisory.

An example from the unruly police practice

Complex organizations need insight in their system of internal control. Based on this insight, the operation of that system can be tested periodically and continually adjusted to changing circumstances. More and more there is a call for compiling a so-called Internal Control Framework. In this article we discuss an example from the unruly practice of the most complex and largest business management service provider of The Netherlands: the Politiedienstencentrum (PDC, Police Services Centre).

Of lees dit artikel in het Nederlands op www.compact.nl:

THE POLITIEDIENSTENCENTRUM (PDC, POLICE SERVICES CENTRE)

The assignment of the Politiedienstencentrum (PDC, Police Services Centre) is to facilitate the entire Dutch police force (Regional units, National Unit, Police Academy and Landelijke Meldkamer Samenwerking [LMS, National Control Room Cooperation]) with high quality business management. The position of the PDC in the force is depicted in Figure 1. This is how the PDC contributes to sound police work. The PDC regulates Payroll, Purchasing, Housing, IT, Vehicles & Vessels, Weapons & Ammunition, Clothing & Equipment and External Communication, including the production of TV programs. To this end, the PDC houses seven departments: Purchasing, Finance, Facility Management, Human Resource Management, Information Management, IT and Communication. Over 7,000 colleagues work at the PDC on a daily basis. The PDC has an annual budget of nearly EUR 6 billion. The organization is relatively young, established in 2012 from the merger of the regional police forces into a single national police force.

TWO APPROACHES OF AN INTERNAL CONTROL FRAMEWORK

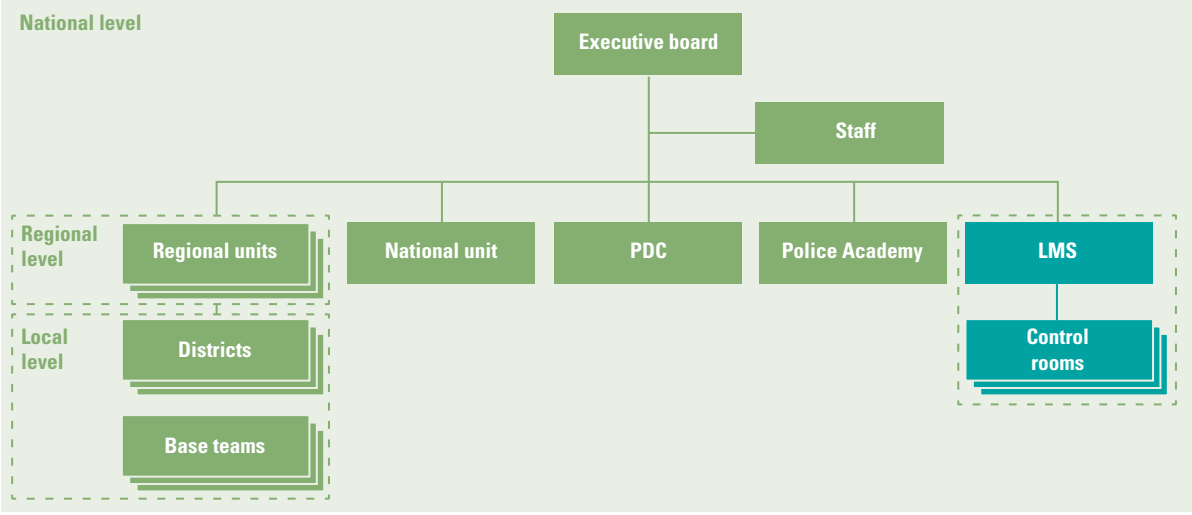
An Internal Control Framework (ICF) is a generally applicable framework in which all types of controls are displayed in interdependence. The most well-known model is the COSO framework that focuses on the entire internal control system, known as COSO II or Enterprise Risk Management (ERM) Framework.

But what is the impact of an ICF for a complex organization such as the PDC? At the beginning of 2021, that assignment was given by PDC management to the Planning & Control unit. We asked ourselves a practical question: what does the ICF look like? Is it a document and if so, how thin, or thick is it? And how is it structured? To provide an answer to all these questions, we have had many conversations, within and especially outside the police organization. Because why would we want to reinvent the wheel? A surprising result: a tour along a number of large private and public organizations did not deliver one useful ICF sample that the police could use. However, there appeared to be two trends:

1. an ICF is the sum of the description of all controls in the processes, or
2. an ICF is a document in outlines with a description of the way in which Internal Control within the organization has been designed.

The PDC has made a choice, a pragmatic approach that fits the current level of control within the PDC. The ICF has become a document in outlines for the PDC which describes how Internal Control is designed for the entire organization. It provides an overview and insight into its coherence, creates a common language with terminology and refers to sources within our organization for more details. And with that the ICF document is also eligible for discussion at executive level. The ICF contains the leading principles of Internal Control within the PDC and is setting the frame for all types of business processes: whether it concerns the development of real estate, the management of clothing and equipment or the production of TV programs. The ICF focuses primarily on business management that is responsible for Internal Control and secondary on controllers that support business management. Finally, the ICF is of value to our internal and external auditors.

Figure 1. Main structure of the police organization.



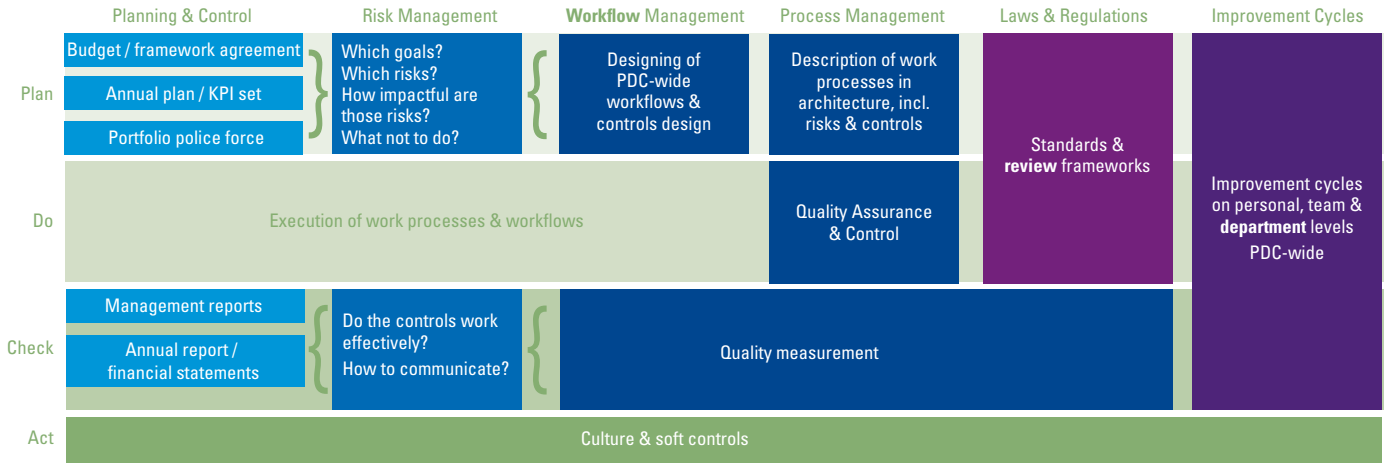


Figure 2. Major components of the ICF.

OBJECTIVE OF CONTROL

The central theme of the ICF is control. Control is primarily about achieving the set objectives within legal and budgetary restrictions, despite the risks that could obstruct or prevent this. These can be operational goals, compliance and regulatory goals, financial objectives and accountability goals or policy objectives and development goals. Control does not solely serve the reliability of the financial accountability; it also serves a sound balance between the going concern activities and the renewal of services.

THE FRAMEWORK

It took us a little over six months with a small group of professionals to prepare the ICF for the PDC, to tune in with a representative group of colleagues (business management, controllers, staff) and to take a well-considered decision at board level. De-facto the alignment process was the first step to get the document alive within our organization. After formal decision-making, many discussions followed at all management levels within our organization. The fact that the ICF is mainly a description of what has been arranged organization-wide for Internal Control but has never been mapped in conjunction helped us tremendously. Only a few new parts need to be implemented.

All-in-all, after one year the PDC has a working and alive ICF for its entire shared services organization. Our aim was to deliver an accessible document of up to 20 pages. Ultimately, we have shaped the description of Internal Control of our organization in 7 chapters and 30 pages ([sJac21]). Figure 2 shows a rough sketch of each of these components / chapters. Especially the framework is a description of how things are organized at the moment and only to a very limited extent a target image. This is emphatically not a model that needs to be implemented. It brings things together, consolidates, makes transparent and gives direction.

1. Typology of the PDC

It may sound a bit old-fashioned, but Starreveld has helped us again after all those years ([Berg20], [Leeu14]). The typology of the business functions of the PDC is diverse and the nature of the control is therefore also diverse: from the processing of salaries to fleet management, the logistics of weapons, the development and the management of police-specific IT systems and the production of a TV programs. We sketch the PDC in its context, the typology of the various business functions, the culture, the tension between going concern and renewal, the strategic developments, and the developments in the area of IT.

2. Planning & Control

For the PDC, the Planning & Control cycle is the core of Internal Control. From budget to annual report. Our cycle is anchored in that of the force as a whole and the annual reports connect to the further development of our strategic vision. Especially the preparing of the annual plan of the PDC is extremely complex, where all portfolio plans of the operational portfolios come together with a need for going concern. Renewal of the police force namely works along the line of portfolio management and practically every renewal in our operational process impacts the business processes of the PDC. Insight into that impact prior to the annual plan process is essential. Over the past years, the Planning & Control organization of the PDC has been busy with a catching up a relatively large backlog in the area of professionalization, organizational design, and staffing.

3. Risk management

Risk-based working is anchored in the genes of operational police work. That's what we do. But risk management in the supporting business has been left behind corps-wide. That is why in our framework explicit attention has been given to the risk management process, the risk-based working, the typology of risks, the method of assessing risks, our risk appetite, and the different roles in the risk management.

4. Process control

From the start in 2012, the PDC has been organized in business operation columns. Each department (HRM, Finance, Facility Management, etc.) had the primary task to get its own processes in order. However, many processes no longer take place in only one department these days. We distinguish the well-known chains such as Procurement to Pay (P2P) and also Police specific chains such as Competent to Skilled and Equipped when it comes to means of violence (standard weapon, baton, pepper spray, etc.). Managing the improvement of the PDC-wide workflows is becoming more and more important. In our ICF we pay attention to het way in which we do so, for which workflows and what are the roles of workflow owner and work process owner.

5. Controls in the processes

Especially for our service, this is the most important part of the framework. We describe our system of controls in the processes that underlie the products and services of the PDC. We record our processes under architecture in BizzDesign. The aim is also to record all key controls of the main processes under architecture. We have started with recording all key controls focused on financial accountability and now we expand that to all processes that are primarily directed to the delivery of our products and services. Regretfully, BizzDesign does not contain a Governance, Risk & Compliance (GRC) module. We are still struggling with that; the way in which we need to model the key controls is not optimal yet. In the ICF we explain the coherence between process control, quality assurance, quality measurement and service, because there is a lot of overlap there. Both worlds contain methods and techniques for the controlled delivery of products and services that comply with predefined KPIs. We strive to make them come together and to integrate them in the organization, if only by creating one language. Finally, using the models developed by Quinn and Cameron ([Came14]) and of prof. Muel Kaptein ([Kapto3]; see also [Bast15]), we give an outline of the influence of culture and behavior on our internal control. Quin's model helped us to design controls and to implement them, matching our dominant culture. The Soft Controls model of Kaptein helped us to gain insight in the potential effect of soft control instruments to the desired behavior of employees.

6. Complying with laws and regulations

The PDC has to do with a large diversity of laws and regulations. Whether it concerns all regulations in the area of working conditions, financial management, privacy or the Weapons and Ammunition Act, the ICF provides general tools on how to deal with this. The ICF does not contain concrete integration of all laws and regulations, it is too generic for that.

7. Improvement cycles

The police invests heavily in being a learning organization. This is necessary to achieve the goals. To this end, multiple improvement cycles have been designed for this that are closely related and coordinated. Development on a personal level and within the team or the network structure is the basis of the improvement cycles. At sector level or service level, we work with a quality management system to test, measure and optimize the quality of the servicing. And our system of regular Control Self-Assessments (CSAs) is an important improvement tool (see Figure 3). As part of the two key questions of the CSA ("Are we doing the right things?" and "Are we doing things right?"), the following questions are being addressed:

- Are all critical risks controlled sufficiently?
- Are we adhering to criteria and norms?
- Do we steer on the desired behavior-risk ratio?
- Do we use the right management and accountability reports?

The CSA system is the basis for the annual In-Control Statement of the police, as recorded in our annual report. At the level of the PDC as a whole, the improvement of the servicing is secured in the Planning & Control cycle.

NECESSARY IN-DEPTH IMPROVEMENT OF THE IT ORGANIZATION

The police is increasingly becoming an IT-driven organization. The IT part in the total business and in the total police work increases every year. That justifies separate attention for the control in the area of IT. Our ICF is too generic in nature to be directly applicable to our IT organization. That is why we have developed a specific framework for the development of our police systems and why we have begun with the

Figure 3. Objects of the Control Self-Assessment.

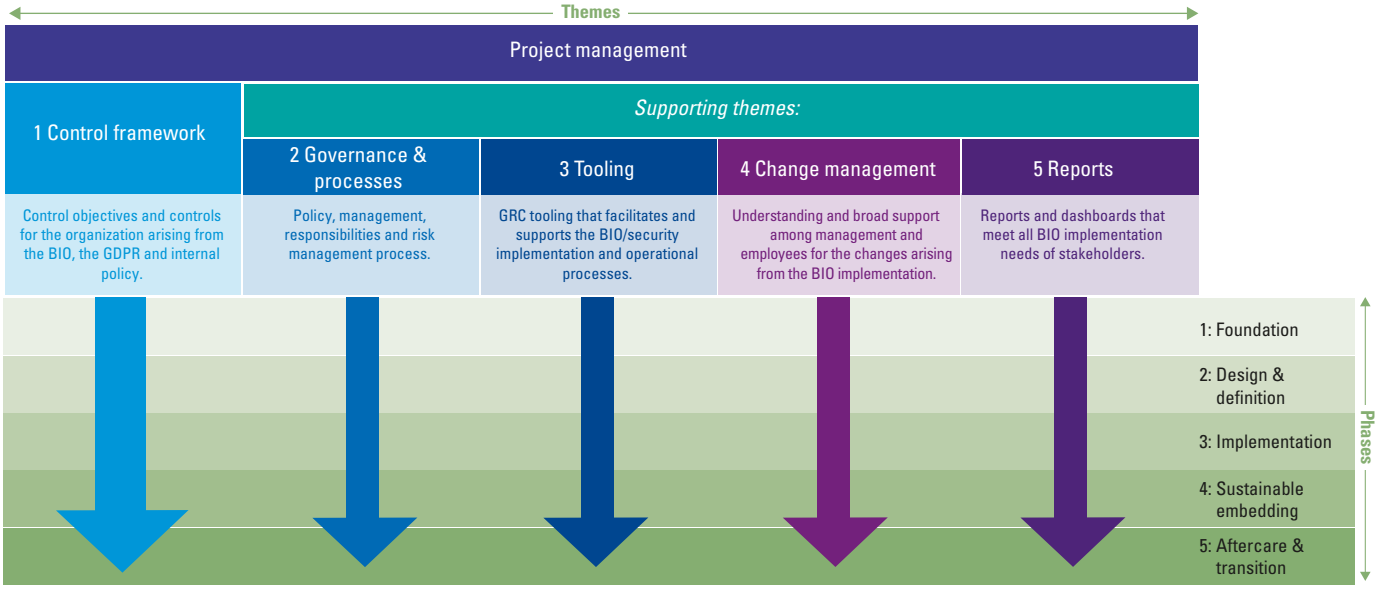
implementation of one framework for IT management processes. The goal is to identify and control the risks of the IT organization within the entire IT landscape (and the associated IT layers) by appropriate controls, considering applicable laws and regulations. As framework for the management of the IT processes the police has adopted the Government Information Security Baseline (Dutch: BIO). The BIO ([BIO20]) concerns a standardized framework based on the international ISO standards NEN-ISO/IEC 27001:2017 and NEN-ISO/IEC 27002:2017 for the Dutch government to protect all its information (systems). The BIO provides direction for the concretization of the ISO standards into concrete control measures.

KPMG best practices for BIO implementations at governmental organizations prove that the first step of the implementation roadmap includes the formulating of the objective by top management and the need to translate the degree of control into the annual internal control statement in the annual report, specifically for our IT processes. The desired scope of that internal control statement determines the scope of the implementation process, which is usually carried out in phases. After the scope has been determined, a link is made per IT process to the BIO security framework in order to take inventory which BIO security controls minimally need to be implemented.

Subsequently, a gap-analysis is used to assess to what extent the current controls are in line with the desired controls from the BIO Security standard. At organizations with a limited degree of maturity levels in the area of IT control, it often is a major challenge to map existing controls and the BIO Security standard in practice. In addition, we often see that the ownership of the controls and the responsibility for the testing thereof are not unambiguously designed and implemented. In order to considerably reduce the complexity of the mapping between existing controls and the complying with the BIO Security standard, a GRC tool can offer a solution. A precondition is to handle a simple structure in the arrangement of this tool in the recording and documentation of the control measure, including a linkage to relevant BIO and ISO standards, upon which the controls are based. This mapping is important because one control measure can affect multiple BIO and ISO standards.

Figure 4 shows in outline the KPMG approach of the BIO implementation; subdivided in five phases and five themes, of which the theme “control framework”, or rather the actual ICF for the IT management environment, is the most important theme.

Figure 4. Phased implementation method of the BIO.



The implementation of the BIO is a complex process, the duration of which is influenced by for example:

- The desired scope of the roadmap (entire PDC, entire IT organization, specific IT parts, etc.)
- The maturity of the IT environment and the quality of the design and implementation of the IT processes with the enclosed controls
- The degree in which the existing controls already comply with the BIO Security standard and whether they are periodically tested
- The knowledge of and experience with the design, implementation and testing of controls in general within the organization and especially the BIO Security standard.
- The degree to which a contribution is made to the implementation roadmap, also outside the IT organization
- the available resources (staffing and budget).

In addition to the BIO, it is necessary to control specific IT risks. In strictly regulated organizations we see that specific internal control frameworks are being developed and implemented for certain IT processes and/or parts of the IT infrastructure, to control specific IT risks. For example, for the process of the transfer of changes to the product environment with deployment tooling, such as Azure DevOps or AWS or for that part of the IT network along which traffic in and out is regulated.

CONCLUSION: WHAT IS THE CONTRIBUTION OF AN ICF TO THE DUTCH POLICE?

For the police the ICF is an instrument to take Internal Control to the next level. The Planning & Control organization offers the ICF as a menu list. There are large differences between and also within the departments of the PDC when the typology of the business functions is at stake and when it affects the degree of maturity in the area of internal control. Every PDC department chooses, also based on their own Control Self-Assessment, one or more subjects from the ICF with which they can further improve their internal control.

The ICF is a police-specific framework. Each of the parts need in-depth understanding. This is how the control of our processes truly gains meaning when the key controls have been accessibly recorded per business process. For our IT environment it is important that we further develop the ICF based on the BIO Security standard and make the link to the various layers in the IT infrastructure and in the specifically high-risk IT processes. In that way we keep on controlling the risks adequately.

For the executive management of the PDC, the ICF offers overview and insight, and it is an aid in the steering towards improvement of Internal Control. And, we now have a common language where internal control is concerned. This creates rest, regularity and (administrative) cleanliness.

References

[Bast15] Basten, A.R.J., Bekkum, E. van & Kuilman, S.A. (2015). Soft controls: IT General Controls 2.0. *Compact 2015/1*. Retrieved from: https://www.compact.nl/articles/soft-controls-it-general-controls-2-0/

[Berg20] Bergsma, J. & Leeuwen, O.C. van (2020). *Bestuurlijke informatieverzorging: Typologieën* (Management Information Systems: Typologies). Groningen: Noordhoff Uitgevers.

[BIO20] BIO (2020, 17 June). *Baseline Informatiebeveiliging Overheid*, versie 1.04zv (BIO Baseline Information Security Government version 1.04zv). Retrieved from: www.bio-overheid.nl.

[Came11] Cameron, K.S. & Quinn, R.E (2011). *Diagnosing and changing organizational culture – Based on the competing values framework*. Jossey Bass.

[Kapt03] Kaptein, M. & Kerklaan, V. (2003). Controlling the 'soft controls'. *Management Control & Accounting, 7*(6), 8-13.

[Leeu14] Leeuwen, O.C. van & Bergsma, J. (2014). *Bestuurlijke informatieverzorging: Algemene grondslagen Starreveld* (Management Information Systems: General Principles). Groningen: Noordhoff.

[sJac21] s'Jacob, R.A. (2021). *The Internal Control Framework PDC*. [The ICF document is public and available upon request, only in Dutch.]

About the authors

René s'Jacob RA is head of Planning & Control of the Police Service Centre (PDC). He also contributes to combating serious internationally organized crime as a financial detective. René started his career at the Automation and Control Group of KPMG, the current KPMG IT Assurance & Advisory. He then fulfilled various functions in advice and management at CMG, KPN, Logica, HEC, Amarantis, Xerox, Conduent and PBLQ. He uses, amongst others, the ICF of the Police as teaching material for his (guest) lectureship at the EMFC/RC training of the TIAS School for Business and Society, Tilburg University.

Claudia Voll works as senior consultant at KPMG IT Assurance & Advisory. She is employed for internationally (listed) clients within the Financial Services sector. Claudia has extensive experience in auditing cloud infra and networks, testing and assessing privacy controls and the implementation of the BIO standard. She has a background in Finance & Control, Accountancy & Control and Digital Auditing.

René and Claudia happen to be father and daughter.