Summary: Has Public Administration Used All Opportunities for Efficient Management of ICT Infrastructure?

Riga, 2019

Latvijas Republikas
Valsts kontrole

Dear reader,

We have completed a performance audit on the efficiency of public ICT infrastructure. The purpose of the audit was to verify whether public administration has a unified approach to the efficient management of ICT infrastructure and whether the institutions have assessed the benefits of ICT centralisation.

Centralised management of ICT services and infrastructure would allow the institutions to optimise in long run their resources – financial, human, material and technical. However, we observed during the audit that the move towards ICT centralisation and single data centres has ceased. The different ministries and even the institutions subordinated to the same ministry do not co-operate sufficiently with each other regarding the ICT management, maintenance, and infrastructure placement. They rather choose to maintain their own, sometimes even several, data centres.

The main difficulty to introducing centralised ICT infrastructure management is linked not to the insufficient technical capacity but to the weak motivation. The institutions simply do not feel comfortable to place their ICT infrastructure with another institution - fearing of losing control of the resources or compromising accessibility to the systems.

The reluctance of the authorities to manage ICT infrastructure centrally, at least at the level of one ministry, has led to a number of server rooms being established in almost every institution, thus significantly increasing the maintenance costs. During the audit, we witnessed situations where information systems of significant, even national, importance, are placed in the premises of insufficient security level. Optimising the number of server rooms would allow not only to reduce ICT placement expenses, but also to provide a sufficient security level at a lower cost.

At the same time, there are high-security level server rooms already available in some institutions, which are not used to their full capacity. These server rooms could host the ICT infrastructure of other institutions, provided there is a centralised ICT management and planning in the ministries.

We express our gratitude to the Ministry of Environmental Protection and Regional Development for a good cooperation during the audit, as well as to other ministries and institutions we visited in order to assess the ICT infrastructure management.

Respectfully yours,

Ms Zita Zariņa,
Department Director

Summary

Motivation

Modern public administration is unthinkable without the use of information and communication technologies. With public administration becoming more modern, not only the amount and convenience of services available to the residents but also the amount of information processed and stored in the provision of services increase. Investing not only in the development of new information systems (hereinafter referred to as IS) but also in the procurement and security of ICT infrastructures, which must ensure the continuity of the systems, is carried out to enable institutions to deliver better quality services and to provide daily support functions. Although institutions have the opportunity to interact and develop interinstitutional sharing services, there is a situation developed historically where institutions take care of their ICT activities themselves according to their understanding, skills, and capabilities, which results in fragmented national ICT infrastructure and insufficient security solutions being ensured during its maintenance.

The problem of ICT fragmentation and more efficient potential use of the existing ICT infrastructure in public administration through interinstitutional cooperation and thus promotion of more rational and efficient public administration is also highlighted by the responsible authority for eGovernment (Ministry of Environmental Protection and Regional Development, from now on - MEPRD):

> *"In the case of modern, rational, and efficient public administration, ICT should support not only the co-operation of one institution, but of all the institutions of public administration by implementing the public administration policy in accordance with the principles set out in the Public Administration Structure Law and the National Information System Law on cooperation of state institutions as a whole."*

Problems in ICT resource and infrastructure management and trends of increasing overall ICT costs are identified in the country since 2010, and there have been attempts to address these problems at least once per every three years (by integrating potential solutions into sectoral policy planning documents*), but overall institutional ICT maintenance costs is still growing. Between 2011 and 2017, total ICT maintenance costs of the institutions** have risen from 17 million euro to 20 million euro per year. Total ICT maintenance costs for institutions include expenditure on ICT infrastructure maintenance, information system maintenance, software rental, and communications services for computer network operations. One cannot define from the existing ICT expenditure accounting data directly how much and to what extent the institutions spend directly on ICT infrastructure maintenance. In addition, there is no practice introduced in the institutions to carry out regular evaluation of what costs cheaper - to maintain ICT themselves or to cooperate with another institution to maintain ICT. Therefore, the State Audit Office pays attention to the question, "Has public administration used all opportunities for efficient management of ICT infrastructure?"

* Given that the information reports contain some of the features of policy planning documents, in the context of this audit, the informative reports[1] and the concept[2] are considered the sectoral policy-planning framework and will be marked as "policy planning documents".

** Institutions - Institutions included in the audit sample.

Main conclusions

Public administration has the potential to optimise ICT, but there is no specific action plan to use this potential. One can find opportunities both within a single ministry and, looking through a broader lens, in interinstitutional cooperation. ICT optimisation is a well-known objective, but its implementation disappears in the routine of daily duties. The tasks for ICT optimisation contained in policy planning documents are more defined in the form of 'intentions' and do not have specific deliverables and criteria to be met in order to identify progress. While ICT optimisation is not defined as a specific task with a responsible person appointed and execution deadlines in the ministries, optimisation is more like a slogan used in institutional strategies, ICT project applications and funding requests, but without a realistic action plan that would allow implementing the intentions and according to which the progress could be measured.

There is a good potential for ICT optimisation; however it is not made use of due to the lack of unified plan.

As responsible authority for ICT management policy development, the Ministry of Environmental Protection and Regional Development (MEPRD) is looking for solutions to promote efficient ICT use. However, this task is not simple at all given the continuous development of technology and the challenge of defining a common direction for the ministries which emphasise the uniqueness of the ICT infrastructure, solutions used, the systems developed, and the data being processed they have created.

One finds it positive that there is a recognition at the national level for several years that centralising ICT service management is one of the elements of good ICT governance and management, which would provide financial benefits in the long run. The MEPRD has provided a common vision for ICT management transformation, based on which the ministries and institutions should plan and implement the measures tailored to the particular ministry and authorities. **However, it unacceptable that the ICT optimisation policy launched in 2010 has not resulted in significant progress** because only one of the audited ministries (Ministry of Justice) has managed to succeed the most in centralising ICT, and it continues further optimisation of ICT within the ministry consistently. **In contrast, ICT optimisation in other ministries included in the audit launched 8 years ago has come to a standstill**. The ambiguous optimisation objective set in policy planning documents - the decrease in ICT spending - has also not been achieved. The situation is opposite because **ICT spending can increase with the development and commissioning of new information systems** and electronic services, as well as with the increase in outsourcing prices.

Consistently year after year, there is a lack of calculation of ICT maintenance costs, and the institutions do not assess alternative solutions for the provision of ICT services or ICT infrastructure management. One has also failed to address the challenges of ICT resource accounting and compilation of data for evidence-based policy-making in ICT governance, which would allow the setting and definition of measurable, realistic indicators for achievable targets by abandoning the overall objective of reducing ICT maintenance costs.

In the audit, we confirmed that data on how much, for example, the maintenance of their server rooms costs are not identified and maintained in the institutions consciously. There is no analysis of alternatives and benefits if the practice of ICT infrastructure provision historically established in the institution would change.

Thus, **in the opinion of the State Audit Office, we reach one of the preconditions for the optimisation of ICT resources that is the competence in the overall planning of ICT management (for example, the accounting of the ICT services used and the costs of ICT infrastructure) should be strengthened in the ministries.** To facilitate this, the State Audit Office calls on the MEPRD to develop the methodology for ICT resource optimisation and to organise training so that the ministries would be able to take decisions related to ICT optimisation independently justified with clear financial benefits and improving the level of ICT security at the same time.

In order to move towards optimisation purposefully, the fact that the MEPRD develops ICT policy planning documents is not enough, as one also requires the MEPRD to monitor how the ministries are implementing the ICT optimisation plans.

For the national ICT policy to be efficient it needs: :
- Comprehensive data for informed decision-making;
- methodology on further actions for t institutions;
- Monitoring the actual execution of the plans.

Three attempts to settle the ICT infrastructure management challenges in the country

The beginnings of single management and optimisation of ICT infrastructure can be found in policy planning documents starting from 2010 when Latvia experienced a significant financial crisis. Since then, three major policy-planning documents have been drafted, providing progress towards ICT optimisation.

Each of them identifies the same problems in ICT management (fragmented management of ICT services and infrastructure and lack of information on ICT resources). The MEPRD has offered new and potential solutions to address the identified problems every time ranging from performing ICT optimisation in the ministries, arranging ICT organisational management itself in the ministries to the definition of the general principles of ICT resource formation and use.

ICT optimisation through the introduction of a single data centre principle is the first attempt to arrange ICT infrastructure management

In 2010, the policy-planning document that the MEPRD had developed set the objective of performing ICT optimisation in the ministries by introducing the principle of a single data centre. The ICT optimisation should be provided according to the action plans developed by the ministries themselves.

When evaluating the implementation of the policy, the situation found by the auditors today does not differ from the conclusions of the MEPRD in 2012 much:

- The ministries optimise ICT infrastructure according to their understanding and capacity leading to the situation when there are ministries that continue implementing ICT optimisation plans set in the ministry consistently, and there are ministries that do not take any measures to optimise ICT;
- Optimisation solutions in the ministries differ, and nobody envisages interinstitutional cooperation in ICT management optimisation, for example, individual ministries plan to use the outsourced data centre as a primary data centre, while other ministries plan to develop their own data centres, but no one is considering an alternative to place their own resources into the data centres already established in other ministries thus making optimal use of the resources existing in the country.

Even today, the level of ICT optimisation is different across the ministries ranging from complete centralisation to a decentralised ICT governance model. The operating environment, technology, capacity, and the level of electronisation vary in every ministry, so the introduction of good governance and management can be different in each ministry, but in all cases, it must rely on research and analysis. **The State Audit Office considers that setting the objective of complete centralisation or decentralisation as an end in itself would not be correct, as one must emphasise that the direction chosen by a ministry is based on specific calculations, consideration of alternatives and that this direction is sustainable.**

Each ministry has to perform a thorough analysis and calculations to justify their chosen optimisation alternative.

The organisation of the ministry's ICT management and ICT Council that is the second attempt to fine-tune ICT infrastructure management

The MEPRD developed the concept of the Organisational Model for Governance of State Information and Communication Technologies in 2013, and one decided to introduce a partially centralised ICT management model in the country. It means that a central national ICT organisation is defined, but the ministries must establish ministerial ICT management organisations and ICT Councils.

When assessing the progress made by the ministries in improving the organisation of ICT management during the audit, auditors have concluded that the requirements of the statutory enactment on the ministerial ICT organisation and establishment of ICT Councils actually are not met (or executed formally) in the ministries audited (except the Ministry of Justice), because the activities of the ministerial ICT Council are formal (Ministry of Agriculture), or it is not established at all (Ministry of Culture and Ministry of Education and Science). It means that there is no prerequisite for the management of well-organised ICT infrastructure in those ministries, the ICT management organisation is not provided in line with the concept. Therefore, the optimal provision and use of ICT services and the optimal management of ICT infrastructure in the ministry are not provided.

Inadequate ICT organisation in the ministries hinders the implementation of good ICT management and optimisation-related decision-making process.

A single architecture of public administration information systems is the third attempt to arrange ICT infrastructure management

In order to solve the problems of ICT resource management, the architecture of public administration information systems (hereinafter referred to as National ICT Architecture) was developed in 2015, which defined the general approach for planning and managing ICT development activities during the new programming period of the European Union funds based on a single ICT architecture in public administration.

One intends to solve the problems with the fragmentation of ICT infrastructure by means of a logically unified data centre and a centralised national electronic communications service centre:

- The logically unified data centre (hereinafter referred to as LUDC) would be created from several ministerial data centres, into whose development or improvement investment has been made recently. The major benefit, which is not exactly quantifiable in financial terms, would constitute ensuring the appropriate level of security for placement of ICT infrastructure;
- The centralised national electronic communications service centre would provide various shared ICT services to institutions (for instance, storage of data backup copies, etc.). Although one plans to establish a centre, which would save financial resources of even 3 million euro in five years already since 2011, more intense activities for the establishment of the centre have started only in 2016 by envisaging the launching of the centre in 2019.

Laws and regulations do not stipulate the duty of institutions to use the infrastructure of the national electronic communications service centre, and the policy planning documents do not include an assessment how the establishment of the centre would affect the optimisation of ICT infrastructure already started in the ministries. Therefore, the risk exists that a situation can occur without the mandatory requirement for certain national information systems to use the services of a single data centre within certain deadlines and to the set extent and without the necessary funding where the data centre set up for several million euro will stay unused. A similar example was a negative experience with a national information system integrator when the institutions did not rush to use it and continued developing their own solutions while there was no clear regulatory requirement to use the integrator.

Safe placement of ICT infrastructure is the matter unresolved for years with a significant impact on the efficient management of ICT infrastructure

There are many institutions involved in ICT security in Latvia, but there is a lack of clarity as to who and how is providing identifying of ICT security situation in the country and common monitoring thereof, for example, the Regulations of the Ministry of Defence foresee a function to coordinate the development and implementation of information technology security policy, while the MEPRD is entrusted with elaborating a policy for ICT governance, organising and coordinating its implementation, including to promote the dissemination of good practices and the development of methodology for ICT governance issues, including ICT maintenance, development, **optimisation, and security**.

The regulatory framework for ICT infrastructure security is incomplete because no detailed security requirements for ICT infrastructure are set forth (for instance, there are requirements regarding different criteria of logical security, but there are no criteria for physical and environmental safety of the infrastructure, which also affects the availability of systems and data protection). Although public

policy planning documents point to the importance of ICT infrastructure security and the need to strengthen it, nobody has planned specific activities in this area at the national level. The Laws and the Cabinet Regulations envisage less about those ICT infrastructure security issues because the existing legal enactments in the country do not shape the requirements of ICT infrastructure security into a single logical system depending on the significance of information processed in the systems explicitly. The lack of clear, traceable and logical differentiation of security requirements to be met that would be interconnected in various regulatory enactments poses the risk that the same ICT infrastructure security requirements are not provided for the processing of information of equal importance and significance in the country as a whole.

There is also no monitoring system of the security management of ICT infrastructure introduced that would ensure the implementation of comprehensive and planned security measures. Security in the digital space is monitored by the state centrally, and the state responds to incidents taking place there, training is carried out, but execution of ICT security in the institutions is not monitored preventively by leaving it to the responsibility of each head of the institution, including the security risk analysis of the institution's systems and the requirements for the ICT infrastructure and the security measures implemented to mitigate the risk probability and their consequences. Although the overall responsibility for implementing ICT security in each institution lies with its manager, the understanding of the institutions on the significance of ICT security issues, the assessment of the importance of the information processed, and the resources available to the institutions to address ICT security issues vary widely. Hence, the actual ICT security in institutions is very different, but the situation in the country is not identified as a whole. A regular monitoring system of those processes would be needed, which would be able to evaluate entire public administration as a single system in total independently and under common criteria, to identify different approaches and prevent them by identifying common risks, and to plan preventive actions to mitigate the latter.

Deficiencies in the differentiation of security requirements and the lack of supervision over compliance with the requirements lead to costly protection where over-protection of insignificant information causes an excessive financial burden on the state budget. Without an adequate monitoring mechanism, the opposite situation is also possible when the protection of nationally important information is not ensured by compromising the access, confidentiality, and integrity of important information. According to the State Audit Office opinion, the ICT infrastructure and other ICT security requirements should be implemented based on nationally agreed and uniform requirements so that investment in ICT security to be sufficient and proportionate and not exaggerated.

In the country, one pays much attention to coordinated supervision of the digital space and prevention of related incidents, logical protection of the systems, but the protection of physical infrastructure has been neglected posing a risk that the institution will be able to identify and respond to attacks on the Internet, but it will not be able to ensure that an individual can exploit physical safety and environmental risks to damage, destroy, or steal essential technical resources.

There are no detailed requirements regarding ICT infrastructure security and a unified ICT security monitoring system in the country. Institutions have a very different understanding and actual approach to providing physical security.

In the opinion of the State Audit Office, the institutions that are unable to provide certain set security requirements should evaluate different opportunities of optimisation and centralisation of ICT resources more intensively.

The ministries can implement the secure hosting of ICT infrastructure through a single data centre principle and centralised management of specific ICT services. The use of a single data centre principle in the ministries would ensure that no one should invest in several server rooms of a ministry, as well as one would save the financial resources needed to maintain each individual server room.

Actual ICT management in the ministries: the lacking direction of ICT development, decentralisation of ICT services, and a single data centre principle that has not been implemented for years

Lack of clear ICT development plans in the ministries

There is no current ICT development and optimisation plan in the ministries audited (except the Ministry of Justice) as ICT optimisation plans elaborated in the ministries in 2010–2011 are the last planning documents designed to optimise specific ICT activities. The State Audit Office finds that one cannot consider those plans as currently appropriate action plans today because they are outdated given the rapid advancement of technology.

Since there is no single ICT development planning document in the ministries, which would define the directions, priorities, of the ICT development of the ministry, short-term and long-term planned tasks and activities for ensuring ICT management, including conditions for the optimal use of ICT infrastructure, the ministries do not facilitate a single ICT management organisation or achieving the overall goal of the ICT optimisation plan.

The ministries lack a clear plan for the development and optimisation of ICT. This does not contribute to the achievement of the overall national goals set forth.

ICT service management is decentralised in the ministries

Although centralised management of ICT services would allow optimising the human resources, financial resources, and ICT infrastructure in the long run, most of the core ICT services are decentralised in the ministries. The audit found that accounting system was centralised in the ministries as a result of ICT optimisation launched in 2010, centralised standard software procurement was provided in the two of the audited ministries (Ministry of Justice and Ministry of Culture) by centralising the record-keeping system partly and implementing unified hardware management partly. As the provision of ICT support in almost every ministry is provided by ICT maintenance responsible staff, units (ICT organisations) or outsourcing service providers, the ministry is responsible for the operation of its information systems and technical resources itself, including its own computer network management, e-mail system, document management system, and ministerial IS management and server room maintenance.

Mostly the provision of ICT services is decentralised in the ministries, with only accounting and record-keeping systems completely centralised, while other ICT services (e-mail provision, single user authentication and support, hardware management, etc.) are either partially centralised or completely decentralised.

Among the audited ministries, ICT management is centralised the most in the Ministry of Justice, whereas ICT management is decentralised more in the Ministry of Culture, the Ministry of Agriculture, and the Ministry of Education and Science. So far, the institutions have been addressing ICT management issues individually according to the competence and capacity of the institution's ICT staff. Thus, further development of ICT management requires a more active and targeted action by the superior institution (ministry) to address ICT governance issues in the ministry.

Better ICT development in the institutions requires more targeted action and involvement of responsible ministry.

ICT infrastructure placement: the non-implemented principle of single data centre

Already since 2010, the ministries attempt to solve the issue of single ICT infrastructure placement within the ministry or try to implement a single data centre within the ministry.

For identification of the problems related to ICT infrastructure placement, there were four ministries (Ministry of Culture, Ministry of Agriculture, Ministry of Justice, and Ministry of Education and Science) and their institutions visited during the audit, which maintained their own information systems in their server rooms totalling to 16 institutions visited. One concludes that 31 server rooms have been established and maintained in the institutions, and 7 server room services are also outsourced. The auditors assessed the security and workload of server rooms of the ministries.

The audit concludes that there are security threats in most server rooms. The auditors of the State Audit Office prepared two estimates of the cost of addressing those security threats. According to the estimate of the auditors:

- Investments of at least 247,000 euro are required to improve only those server rooms that contain information systems crucial to the ministry (increased security information systems or integrated national information systems);
- Investments of at least 765,000 euro are required to ensure that all identified security risks are eliminated and that all server rooms of the ministries are upgraded in all the ministries.

There are security threats in server rooms, and tackling them will require at least 247,000 to 765,000 euro.

The auditors made estimates[3] of how much state budget means could be saved by making better use of already existing high-level server rooms in the ministries. Considering that each of the three ministries (Ministry of Justice, Ministry of Agriculture, and Ministry of Culture) possesses unloaded high-level

server rooms where placing ICT infrastructure of the entire ministry is possible, then the introduction of the complete principle of single data centre in the ministries creates saving both from the fact that each institution no longer maintains its separate or several separate server rooms, nor does the ministry require investing in improving the security of each individual server room. The auditors prepared three estimates for moving towards a single data centre principle in the ministries:

- Transfer institutional server equipment only from the premises where the information systems crucial to the ministry are located (advanced security information systems or integrated national information systems) to the unloaded high-level server room of the ministry. In this case, one could save around 301,000 euro over five years in the three ministries or during the useful service life of the server hardware;
- Carry out full migration of ICT resources to a single data centre within the ministry. In this case, it would be possible to save as much as 791,000 euro over five years (during the useful service life of the server hardware).
- Decline from using the server rooms provided by an outsourcing provider and carry out the placement of the servers outsourced to the contractor in the unloaded high-level server room of the ministry. In this case, two ministries would manage to save another 516,000 euro over five years.

More efficient use of existing (requirement-compliant) data centres in the ministries and centralisation of ICT resources therein can ensure savings of up to 1.3 million euro in five years.

Therefore, total saving for ICT infrastructure placement could reach even 1.3 million euro over five years (or during the useful service life of server hardware) in the ministries.

Managing ICT services and ICT infrastructure beyond the ministries: doing everything oneself is cheaper than using an outsourced service provider

To assess how ICT management issues are organised beyond the ministries, three institutions were visited during the audit (National Electronic Mass Media Council, Social Integration Fund, and State Chancellery).

The audit concludes that the sharing of ICT in an institution is cheaper than using an outsourced service provider. In the institutions using shared resources with other public authorities, the cost of managing ICT resources (workstations, servers) is lower than in the institutions that outsource ICT maintenance and management to a service provider. For example, the cost of maintaining one user workstation (including consulting a user and maintaining the workstation's software) costs 14 euro per workstation if outsourced, while the institutions using shared resources with other public authorities pay 10 euro per workstation at an average.

Sharing ICT resources with other public authorities can contribute to cost savings.

Major Recommendations

Based on the audit conclusions, recommendations for improving the overall national ICT management and ICT security are provided:

- For organising unified ICT management:
  - In order to promote a centrally managed and hierarchically determined process of ICT optimisation, which would contribute to the reduced maintenance costs of ICT infrastructure, MEPRD shall develop a policy planning document for ICT resource optimisation according to the planning standards defined in the Law on Development Planning System and its subordinate regulatory enactments, and submit it to the Cabinet of Ministers for decision making;
  - To ensure a unified ICT management organisation in the ministries, MEPRD shall contribute to the establishment of a ministerial ICT council in line with the concept in the ministries and the appointment of the responsible ICT managers of the ministry;
  - In order to ensure the application of the ICT management principles set out in regulatory enactments and policy planning documents in the institutions, MEPRD shall develop methodology and train ICT managers of the institutions, integrating the issue inter alia on the fact how to identify the current situation in ICT provision and spending, identify opportunities for optimisation, and calculate financial impact against investments required for implementation of specific optimisation measures;
  - In order to promote a unified ICT development direction in the ministries and the direction of ICT development would comply with the principles and requirements stipulated in the national ICT policy planning documents, MEPRD shall promote the elaboration of an ICT optimisation plan for each ministry in cooperation with the ministries by defining the activities and tasks to be implemented in short term and long term.
- For improving ICT security:
  - In cooperation with other authorities involved in security supervision (Ministry of Defence and Constitution Protection Bureau), MEPRD shall establish technical requirements for the data centers of ICT central infrastructure resulting from various principles and objectives of classifying information and technical resources in order to facilitate the determination of a desired level of security by establishing specific minimum technical requirements for information and technical resources of low level classification at the same time;
  - To ensure single management of ICT infrastructure and to reduce the necessary expenses for maintenance of server rooms and improvement of their security, in cooperation with the ministries, MEPRD shall promote:
    - Reassessment of the application of the single data centre principle for the placement of ministerial ICT infrastructure;
    - Hosting of integrated national information systems according to the security requirements specified in the regulatory enactment.
  - The State Audit Office shall invite the Cabinet of Ministers to decide on further action in the implementation of such **proposal**:
    - In order to improve ICT security in the public administration, we do hereby invite the Cabinet of Ministers to instruct the Ministry of Defence, in cooperation with the institutions involved in ensuring IT security (Constitution Protection Bureau and

MEPRD), to develop a harmonized ICT infrastructure security monitoring mechanism coordinated with the assessment of the national cybersecurity risk identification capabilities to be developed.

[1] Informative Report "On Opportunities of Optimisation of Microsoft Infrastructure Software Usage and Information Technology Infrastructure in Ministries and Their Subordinate Institutions" (taken notice of at meeting No 17 of the Cabinet of Ministers on 6 April 2010 under 32§) and Informative Report "On Conceptual Architecture of Public Administration Information Systems" (taken notice of at meeting No 14 of the Cabinet of Ministers on 10 March 2015 under 22§).

[2] Concept "Organisational Model of National Information and Communication Technology Management" (supported by Cabinet Order No 57 of 19 Feb 2013).

[3] Estimates of server room migration are based on a server room that accommodates institutional support information systems (accounting, record keeping, etc.) whose operation does not require complex configuration or specific ICT equipment. The estimates do not include the potential additional costs that might occur in the case of developing a single network, the purchase of specific network communication equipment, or the insurance of equipment.