ONE WORLD
ONE SERVICE

Ministry of Foreign Affairs of Denmark

IT strategy 2013-2016

Contents

1. The Danish Ministry of Foreign Affairs' IT Strategy 2013-16

The Danish Ministry of Foreign Affairs' strategy for communication and information technology for the period 2013-2016 establishes the general outline for developing the organisation's IT systems over the next four years. The primary emphasis is on the challenges and strategic investments that are shared by the organisation as a whole: the shared network and the IT systems that everyone works with. Thus, the strategy does not directly concern itself with those dedicated applications that are used by the various departments in the Ministry and that are continually being developed in order to optimise the current workflows in the Ministry. The strategy replaces the existing strategy for 2008-12.

The MFA works determinedly to exploit the opportunities that digitisation offers. With more than 100 different addresses around the world, a culturally and linguistically heterogeneous staff composition and a relatively complex work portfolio, the MFA has benefited greatly from the rapid development that has occurred in field of information and communication technology. Digitisation has reduced the significance of geographic distances, and it has also made it possible to standardise and simplify a number of different workflows. The MFA's core business continues to be bound up with collecting, processing and disseminating information, but the tools we use to do this are changing all the time, which places great demands on the organisation and staff's ability to adapt and change. The MFA does not necessarily need to be in the vanguard in terms of digitisation, but on the other hand, neither can the Ministry afford to pass up the potential for achieving greater efficiency that is offered by smarter, more flexible and quicker ways to communicate and work. For the same reason, the MFA expends a relatively large amount of resources on supporting the digitisation of a growing number of work areas.

The MFA possesses a particularly well-functioning IT network that is characterised by a high degree of *operational stability* and a high level of security. The existing IT infrastructure and the organisation that has been developed to support and further develop the IT network have served the Ministry well. With the help of a proactive focus, long-term investments and the continual development of the IT staff's competences, the Ministry has succeeded in meeting the increasing demands for such things as mobility and flexibility without compromising the operational stability and the security of the network.

New challenges

Operational stability and security are under constant pressure. The MFA's IT enterprise architecture is strongly influenced by the extremely decentralised approach to IT development that the organisation has followed for the last 15-20 years. Business-driven IT development has set the agenda, while the IT Department's primary task has been to operate the shared organisational systems, the various dedicated systems and the underlying infrastructure. Today, the MFA operates with a large number of dedicated systems – some of which we have developed ourselves while others are standard systems – all with completely different requirements to the IT infrastructure. This is one of the factors that increase the complexity of the IT environment, which means greater operating costs (a need for more specialists) and an increased risk of service interruptions (when "foreign" systems must work together).

Simultaneously, demand has also been increasing for mobility and improved access via handheld devices such as smartphones and tablets. The PC is still necessary when large amounts of contiguous text and documents must be produced, but an increasing amount of the daily correspondence takes place today over mobile devices, which allow the user to quickly check emails and keep up to date. The mobility agenda presents a double challenge for security in the Ministry: firstly because the mobile devices are not nearly so well protected as the dedicated PCs and secondly because the staff can potentially use the mobile devices anytime and anywhere.

The challenges vis-à-vis operating the organisation's IT systems and meeting the increasing demand for mobile solutions coincides with a general increase in the interest for developing IT systems to support the existing workflows. Operational optimisation and the development of mobile clients for actual case processing/production must, therefore, be carried out concurrently with the launch of up to several major IT projects in the MFA, including an Electronic File and Document Management system (ESDH).

The stakeholders

With regard to the IT Strategy, the MFA has two groups of stakeholders: the staff and the external partners we work with at home and abroad. The external partners comprise public authorities and private actors in Denmark and abroad.

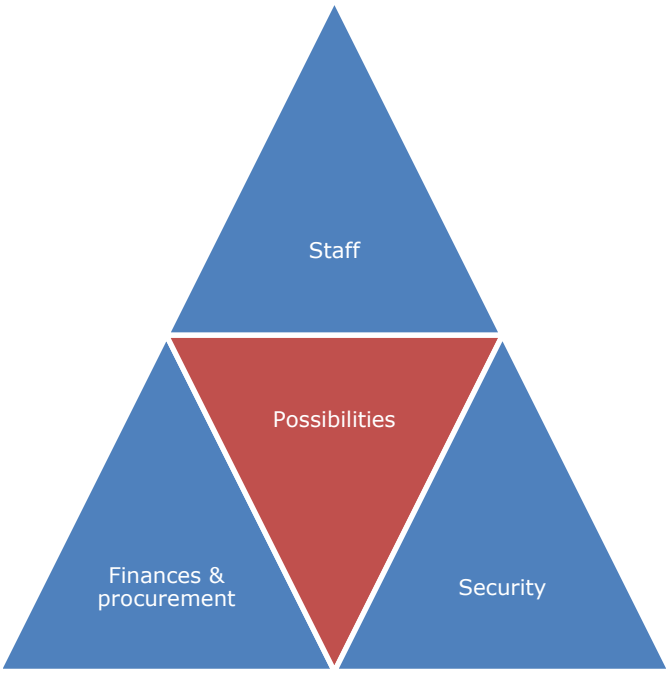
The MFA lives off of handling information, which is, on a daily basis, gathered together, processed and disseminated to our partners throughout the world. The MFA's timely access to relevant information depends, to a great extent, on the staff's credibility and ability to protect the information they are trusted with. In other words, the external stakeholders expect the MFA to be capable of adequately protecting the information. At the same time, the external customers demand that the MFA ensure openness and transparency with regard to a wide range of information of broad public interest (travel guidelines, country analyses, development assistance, etc.).

In return, the staff expects flexibility and a readiness to adapt and change. The Globalisation Analysis from 2006, as brought up to date by the Globalisation Agents in 2008, clearly emphasises the need for the IT support of Denmark's diplomatic presence in some of the most dangerous and least accessible hotspots in the world. The Danish Foreign Service must be able to operate everywhere in the world in a cost-effective and secure way. With regard to the framework for the analysis and its relation to the work on the IT strategy, the most significant change has been the economic recession that has struck the Western world and that has also had the effect of limiting the economic framework that is made available to the MFA.

The MFA's IT Strategy for 2013-16 is to fundamentally answer three principal questions:

1) How can we ensure maximum operational stability of the network within the economic framework which is available?
2) How can we ensure tighter control and prioritising of the Ministry's IT resources without at the same time weakening the various departments and the Missions' use of and benefits from the decentralised IT systems?
3) How do we meet the request for increased mobility without at the same time compromising information security?

These questions must be answered within the context of various overriding personnel policy, administrative and, not least, economic frameworks, which are not expected to change radically within the strategy period, cf. the below model:



The staff expect that the IT systems prioritise user friendliness, flexibility and mobility. The IT systems must make it easier to be employed at the MFA, not more difficult. Changes in the Ministry's network and connections to that network must, however, be planned in cooperation with the **national security authorities**. The MFA works in close cooperation with public authorities and private actors at home and abroad, which places great demands vis-à-vis the protection of the information that the Ministry is entrusted with. For the same reason, information security is not just an internal matter for the MFA's IT Department. Finally, the MFA's **financial** framework and the existing government rules on public procurement have brought finance and expenditure management into sharp focus. In general, the MFA must choose the most economical solutions, no matter how well they might otherwise match the Ministry's needs.

It is within this cross-pressure of considerations that IT development within the MFA takes place. To a large degree, the guiding principles or visions for the organisation's overall IT development are provided by the staff's expectations: It is primarily the users (i.e. the staff) who define the needs for IT support within the different areas of business. There are many administrative procedures that work perfectly well with protocol tags and fountain pens. They can undoubtedly be made marginally more efficient. But the primary task must be those areas of business where better IT support will *both* make the workflows more efficient *and* create added value. The MFA will never be a virtual workplace. The core business of the Ministry continues to be inextricably linked with a diplomatic practice that builds on a concrete presence, local knowledge and understanding, and establishing relationships based on trust.

The vision is thus of IT support that creates cohesion within the organisation across geographic distances and time differences; that creates open and flexible paths of communication without compromising information security; and that thereby provides the staff with the maximum possible freedom to act and manoeuvre. In other words, the vision is of the IT support of those areas of business that make it possible for the staff to display drive and professionalism (through timely access to exchange relevant knowledge), ensure openness and transparency in the administration (through electronic archives, media and search functions), and at the

same time creates the prerequisites for a good work environment where, through increased digital mobility, the staff have the opportunity to create a better balance between their work and free time.

The IT Department's ambition is to deliver relevant, stable and secure IT systems that comply with all the relevant standards and rules and that provide, within the financial framework that is available, the staff and the MFA's partners at home and abroad with simple and clear access to the relevant parts of the systems around the clock.

2. Objectives for the strategy period

The use of IT in the MFA is to support the implementation of the MFA's globalisation strategy and contribute to efficient and secure workflows and communication. Mobility and operative capacity, also in areas with poor infrastructure, along with openness and effective communication with both public and private partners at home and abroad thus continue to constitute key objectives. The ambition is to maintain the MFA's position as a trustworthy and professional organisation that is capable of managing large amounts of information and data in an efficient way and with a high level of security. Furthermore, developments within IT must take saving energy into consideration when choosing infrastructures, platforms and when putting new technology into operation.

In general, there will be a focus on IT support of the business through the optimisation of workflows and work routines, for example through the increased use of video conferences and digitalised workflows, the Intranet as well as through the establishment of new IT-based solutions and administrative systems. Finally, ongoing initiatives within "virtual diplomacy", transparency in administration and in the work of development assistance together with meeting the IT security requirements will be core tasks.

Within the individual subject areas, specific objectives have been defined for the strategy period. There will be continuous reporting on objective fulfilment, just as it will also be possible to identify and prioritise new objectives during the strategy period.

2.1. Digitisation, mobility and IP telephony

During the strategy period, mobility is to be given particularly high priority, for example through the continued distribution of laptop computers and handheld devices such as smartphones and tablets. Work is specifically being done to ensure that the staff have the quickest and most flexible access to the MFA's network within the framework of the existing requirements to IT security. As a global organisation, the Foreign Service must strengthen its shared Intranet as well as implement new services that take advantage of technology for direct communication and cooperation.

Programs or IT applications that support and streamline administrative procedures and the flow of information are essential for enabling the business to be run effectively as a modern work place. SharePoint is the MFA's main platform for supporting knowledge sharing on the Intranet.

Network telephony (digital IP telephony/*Unified Communication & Collaboration*) based on Microsoft's Lync 2013 is being introduced throughout the entire Foreign Service. In future, it will be possible to call colleagues at home or abroad or see when they are expected to be available again with a single click. In this way, Outlook, the calendar, the Intranet and the telephone system will be integrated throughout the entire Foreign Service. This also means that it will be significantly easier to keep contacts up to date and to find colleagues. Lync 2013 will thus, as is recommended in the Globalisation report, make it "possible to identify and take advantage of the competences of different staff members when a specific need arises, no matter where in the organisation they might be physically located".

2.2. Digital Diplomacy, communication on the Net

The MFA's communication and public diplomacy efforts vis-à-vis the outside world take place to an increasing degree exclusively on/via digital communication platforms on the Internet, i.e. both the Ministry's own websites and increasingly also on social media sites (Facebook, Twitter, YouTube, etc.). The MFA has approx. 100 websites in operation. These are

administered through a central Content Management System (CMS), which is hosted externally. The tool for editing and administering the content on the Ministry's websites as well as on the social media sites is the internet browsers on the Ministry's office PCs. The content on the Ministry's websites is maintained and edited at the local level, i.e. both at the Missions and in the units at Asiatisk Plads (in accordance with the Ministry's principle regarding decentralised responsibility for communication).

It is of strategic importance that the browsers on the Ministry's office PCs be configured at all times such that they meet the requirements demanded by the Ministry's Content Management System and, additionally, that they always match the current technologies on the Internet and the social media sites.

2.3. Green IT

The MFA will focus on the use of green IT and the reduction of energy consumption through, for example, energy-saving initiatives in relation to the hibernation functionality on IT equipment. Green IT is to be implemented, for example, by reducing the number of physical servers as well as through the increased use of virtualisation and mobility. The increased use of laptop PCs and smartphones provides a natural direction for the introduction of green IT because the technologies underpinning mobile devices pay a great deal of attention to energy consumption and, for example, battery capacity.

The MFA will constantly expand the opportunities for using video conferences globally on the encrypted network, which will reduce the need for official business travel and in that way also help to reduce CO^2 emissions.

2.4. Openness, security and finances

Confronted with falling operating budgets, the MFA must focus proactively on IT development and the efficiency benefits that such investments open up for. IT must be included in connection with efficiency initiatives within the Ministry, both with regard to the individual case areas but also across the organisation as a whole with a view to taking advantage of economies of scale.

As a part of the efficiency improvement programme for 2012-2013, it was decided that an IT Board should be established to ensure the managerial anchoring of all major IT projects as well as the improved management and prioritisation of dedicated IT systems in the Ministry. The board is, among other things, to ensure that new IT ventures work together with the existing IT systems and that the expected gains are realistic and the planned realisation of the gains is credible. Through its work, the Board will thus help to create a higher degree of openness and transparency in the MFA's administration of the overall IT portfolio.

3. Leadership, organisation and management of IT

IT is a resource on a par with the staff and with finances. The overall responsibility for IT in the MFA lies with the IT Department, which besides the strategic direction and guidance also provides operations support for both the organisation's shared IT systems and for the various dedicated applications. The Department is to ensure both that the MFA's IT systems and dedicated applications are protected against unauthorised traffic and run without service interruptions and also to ensure that users have access to effective and professional assistance in handling IT related problems. **Operations** and **security** is handled partly by our own specialists and partly by external providers, cf. section 7 on sourcing. **The support function** in the form of a 24/7 ServiceDesk is handled by our own staff IT experts with technical support from both the operations unit and, if necessary, from external providers. The Department's mission can basically be summed up by the motto: "*To serve and to protect*". The IT Department is to support the MFA's activities by delivering secure, stable and effective IT systems and lines of communication and be ready to quickly solve the technical problems that will inevitably and continually arise in a complex, international IT environment such as the MFA's.

The MFA's IT governance is anchored in the IT Board, which includes the participation of Senior Management, the Head of IT (chair) and the Head of Finances. The IT Board is to ensure that

- cohesion is created between the Ministry's business and IT
- an overview and effective management of the digitisation projects are created
- IT and digitisation provide improved service, increased quality and economic benefits

The task of the IT Board is the effective management of IT and digitisation throughout the entire organisation. All new IT projects must, therefore, be presented to the Board for approval, just as status reports on those activities currently underway must also be presented to the Board on a regular basis.

Decision-making structure for IT development

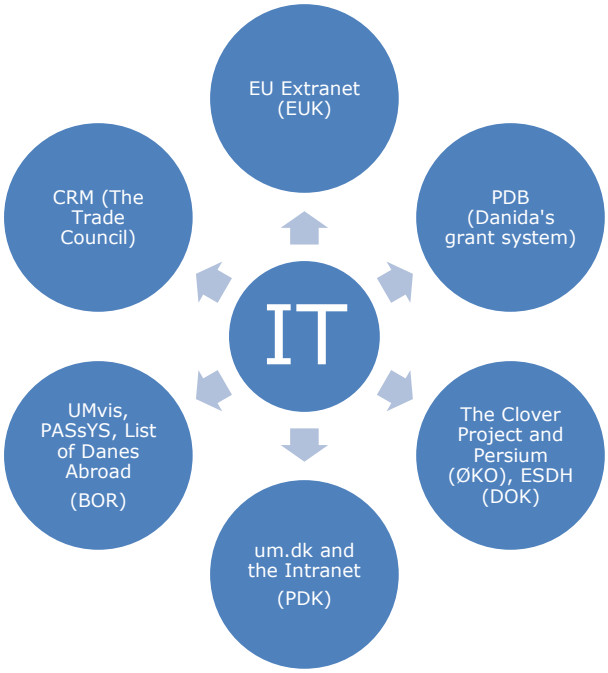
The IT Strategy approved by corporate management establishes the goals and the framework for prioritising and launching specific projects. The current IT Strategy is based on a comprehensive stakeholder analysis "The Borderless World – The Danish Ministry of Foreign Affairs and Globalisation" from 2006, the results of which were recently corroborated in connection with a broader internal investigative report in 2008.

The IT Strategy lays out the overriding framework for IT development and is supplemented by annual IT action plans that define the specific projects for 1-2 calendar years and set out time frames for their realisation. The annual action plans are an active element in the process of strategic prioritisation and resource management (SPR), which forms the basis for the performance contract between the IT Department and the Ministry's corporate management.

Each individual department is responsible for taking the initiative vis-à-vis establishing administrative systems (applications) in the units' specific fields. When relevant, these systems are to be established as shared services across the entire structure of the Foreign Service.

The individual units are themselves responsible for financing, establishing, further developing and operating the business-critical applications within the unit's task areas. This includes, for example, Consular Service's Visa and Passport systems, Danida's project database, the EU Extranet, PDK's web CMS as well as the Intranet, the Trade Council's CRM system the HR database and the financial systems. A unit (system owner) that wishes to establish a new IT-support prepares a business case to be presented to the IT Board and the IT Operations Forum

with the participation of all the major system owners. Major maintenance projects or the updating of existing systems must similarly be presented to the IT Board.



Apart from financial issues, the IT Board is also to consider the particular activity's compatibility with the existing shared service. In general, the MFA wishes to reduce the complexity and vulnerability of the existing IT system by relying on, to a greater extent, shared standard systems and off-the-shelf products. In this connection, the IT Board will also be able to consider the particular activity's expected strain on the GlobalWAN system. The capacity of GlobalWAN is a limited and expensive resource which must be distributed and used in a disciplined and cost-conscious way. Before the decision is made to launch any new application that needs GlobalWAN communication, it must be determined how much of the GlobalWAN resources it will use and what the consequences will be vis-à-vis the overall capacity. When these things have been determined, the result will then be included in the business case for the project.

The business case forms the basis for the IT Board's decision on whether to launch the project and, upon approval, is an important part of the basis of appropriation for the project. The project's overall timeframe and activity plan are included in the business case, together with a risk assessment and an evaluation of the project's organisational consequences and the possibilities for it to function as a shared service. IT projects costing over DKK 10 million must follow the regulations for the government's Project Model.

3.1 Managing and prioritising IT resources

Budgeting, managing and controlling the ordinary operation expenditures in the IT area are undertaken as a part of the Ministry's general budget cycle and are subject to the Ministry's primary guidelines, management principles and management tools. Major IT acquisitions are carried out as projects in which the project management is to be performed in a professional way and on the basis of best practice in the area. The system owner is responsible for organising and staffing the project, which includes the appointment of a competent (internal or

external) project leader. The IT Department normally participates in the project work, just as the IT Department has allocated resources to assist the units with IT business development.

The *IT Operations Forum* is the IT technical forum between the IT Department and the system owners. The IT Operations Forum has an overview of ongoing IT projects and will thus be a forum for the crosscutting coordination and integration of the systems. All relevant units are to contribute to this forum. The *Technology Committee* has been established as a committee under the Central Joint Coordinating Committee. All questions regarding IT, including specifically the possible impact that IT systems will have on the work environment, administrative procedures and forms of cooperation can be discussed in the Technology Committee.

During the strategy period, the IT Operations Forum is to regularly discuss the implementation of the IT Strategy and the work of further developing the MFA's dedicated IT systems with a view to promoting the horizontal dissemination of knowledge and not least of "best practice" in the IT area within the MFA.

Objective: *To have the IT Board direct focus on improved management and prioritisation across the organisation. The IT Department is to assume greater responsibility for technical sparring and support in relation to the IT projects in each department.*

The Joint Public Digitisation Strategy was adopted in August 2011 for the purpose of using digitisation to modernise Danes' welfare and streamlining the public sector. The digitisation strategy is a collaboration between the state, the municipalities and the regions, which are jointly working to implement the digitisation strategy's initiatives leading up to 2015.

The MFA abides by the state standards for mandatory open standards. At present, there are seven sets of mandatory open standards:

1. Standards for data exchange between public authorities (OIOXML)
2. Standards for electronic file and document handling (FESD)
3. Standards for electronic procurement in the public sector (OIOUBL)
4. Standards for digital signatures (OCES)
5. Standards for public sector websites/home pages and accessibility
6. Standards for IT security (ISO2001)
7. Standards for document exchange (ODF, OOXML and PDF).

4. Infrastructure

The MFA's infrastructure has not changed fundamentally in the last 15 years. A number of successful changes and adjustments have been made to the system (for example, domain consolidation, server virtualisation of the T-environment in the service at home and abroad, new services and infrastructure applications and improved support for mobility). However, the architecture is fundamentally the same now as was 15 years ago: a very large number of physical servers in the service at home set up in a domain structure with the servers at each location in the service abroad and with a number of client PCs connected in a so-called client-server-architecture at each Mission. Over the years, this model has proven to be particularly well suited to the Ministry's purposes. There is, however, a need to re-examine the basic architecture, at a time when three major themes have become pressing:

- Server virtualisation
- Cloud computing
- Centralisation/regionalisation

Fact box: *The MFA uses the PC platform Microsoft Windows 7 with IE9 and Office 2010 on all of its approx. 3,200 PC work stations, incl. devices, distributed among 2000 users a third of which are in the service at home and two-thirds are at the diplomatic missions. On the servers, the Ministry runs Windows Server 2008/2012. Microsoft SCCM and SCOM are used, for example, for system maintenance and monitoring, while SCSM is used for ServiceDesk and DPM is used for backup in Copenhagen.*

The MFA's technology choices are based on the Microsoft platform. The Communication and data lines are based on Cisco and the global WAN provider. The hardware for virtualisation and SAN comes from HP.

Server virtualisation

The MFA's IT Department has been ahead of the game in many areas vis-à-vis launching new and innovative solutions, driven primarily by sound business economics. In one of the greenest areas – server virtualisation – the MFA has, however, not managed to take advantage of new possibilities.

Server virtualisation is clearly one of the greatest technological innovations since the introduction of client-server computing. Server virtualisation can be described in many different ways, has gradually come to be used in many different areas and has a number of different advantages in these various areas. The IT Department focuses on server virtualisation that, in short, consists of being able to run multiple (software-based) servers on the same server hardware. There are many advantages associated with this, but improved utilisation of the server hardware, reduced use of space, reduced need for electricity and cooling and thereby far better overall economy are among the most important.

The two most significant drawbacks with server virtualisation are, on the other hand, a significantly greater complexity in the infrastructure and a higher degree of vulnerability. The greater complexity results partly from the introduction of a new layer of architecture between the hardware and the operating system, the so-called hypervisor, which is itself the layer that allows multiple operating system instances on the same physical hardware. However, due to the greater vulnerability that results from the multiple systems and the subsequent fact that many users are running on the same hardware, it is necessary to take special infrastructural

measures to avoid *single points of failure.* Such measures typically consist of setting up servers that run multiple server instances on the same hardware in so-called *clusters.* Set up, configuration, ongoing operation and maintenance of cluster environments are in themselves not minor technological challenges. And this applies to no lesser extent when each of the cluster nodes, i.e. the hardware servers, are host machines for a number of underlying virtualised servers.

At a time when resources are becoming increasingly scarce, the MFA needs to continue to work with virtualisation, even though it places great demands on our competences with regard to our operating organisation to build and operate an infrastructure environment that is server virtualised and clustered to a relatively large degree. Virtualisation takes place in many other IT areas: application virtualisation, desktop virtualisation, virtualisation of switch networks, etc. With terminal service, which can be seen as a special (and somewhat old-fashioned) type of desktop virtualisation as a possible exception, the IT Department does not expect to use any other virtualisation technology within the strategy period because there does not seem to be any business need and justification for it.

Objective: *To ensure that before the end of 2016, between 60 and 75% of the servers at Asiatisk Plads are run as virtual servers with high accessibility (clusters) on Microsoft's Hyper-V solution. 10% of the servers are to be converted before the end of 2013.*

Cloud computing

Unlike virtualisation, for which there are a large number of very specific technological implementations, 'cloud computing' is a more diffuse concept. If 'cloud computing' is the network-facilitated provision of IT services, then the MFA has had a private cloud at their disposal for the last 15 years. If 'cloud computing' is internet-based access to services in the public cloud, then the MFA has offered its users 'public cloud computing' just as long as the users have had access to the Internet.

The reason that the concept of cloud computing is being talked about more and more is primarily due to the fact that the number of services provided in the cloud is constantly growing. Today, a company can choose to equip employees with a simple PC and an Internet connection to the cloud, which in turn delivers everything from the Office suite to applications for data storage and backup. There is little doubt that the growth in this area is still only in its infancy. However, the MFA believes that, in terms of new major services, the market is currently still either commercially or technologically immature. Therefore, and because the MFA for security reasons generally keeps its own data within its own four walls, major investments in the public cloud area are not expected over the next 4 years.

Individual and actually very simple public cloud services have, however, been put to great use by both private and commercial enterprises. Dropbox is one example. Dropbox is a storage and file sharing application that allows users the opportunity to store and sync files online and between computers simply by storing them in a special file directory. Dropbox is particularly popular because it makes it possible to exchange large amounts of data quickly and effectively, without the limitations that result from the encrypted network (file size, firewalls, etc.). Dropbox clients are available for almost all desktop and mobile operating systems. From the MFA's point of view, Dropbox as a public cloud service is, however, very problematic because data is taken out of the encrypted (protected) network and placed on a public server, which is, for security reasons, unacceptable. Therefore, an internal Dropbox service is to be developed as a "private cloud"-service based on the SharePoint 2013 SkyDrive Pro-solution.

Objective: *To develop and launch UMDropbox on a private (protected) cloud before the end of 2013.*

Centralisation/regionalisation

The issues involving regionalisation and centralisation are about the type of connection and the manner in which the Missions in the service abroad are offered IT services. It is possible to distinguish between at least three connection types:

1. The decentralised (current)
2. The centralised
3. The regionalised

With the current decentralised type of connection, each Mission has a physical server on its premises. In brief, this server delivers all IT services (e.g. mail service, the login service, the file and print services and certain local applications) to the users, except for those services that are provided only in Copenhagen (e.g. the Intranet). The major advantage of this type of connection is the rapid delivery of the majority of services due to the fact that they are all locally available and independent of the GlobalWAN connection. The disadvantage is that this solution is costly both in construction and operation: There is an equal number of servers and associated server rooms and a similar need for cooling and subsequent system maintenance as there are Missions. In addition, web applications in Copenhagen and web applications accessed via the internet gateway in Copenhagen involve relatively long response times, so-called "latency". Based on experience, anything over 2 seconds in response time is seen as a major drawback in terms of daily work.

With the centralised solution, which is already available at some "server-less" Missions, there is no server located at the Mission. All IT services are delivered to the users and their PCs from a central group at Asiatisk Plads in Copenhagen. The solution is possible in two variants: one in which the server-less Missions run as they do today and which uses ordinary Internet connections. The great advantage of this type of connection is that it is inexpensive both to build and to operate because there is no server that needs to be transported, installed and maintained, and there is only a minor expense for the local Internet connection. However, with this solution nothing can be done without a strong and stable local Internet connection. This solution must, therefore, be regarded as wholly inadequate for even somewhat large Missions, where it is a necessity to have a GlobalWAN connection to the servers in Copenhagen. But even if there is a good connection via the Internet or GlobalWAN, if you are sitting on the other side of the world, long response times will sometimes still occur due to latency.

The regionalised solution can perhaps best be described as an extended centralised solution: A number of so-called NOCs (Network Operations Centers) are built, for example 5-7 of them around the world, presumably at the large Missions in each region. All diplomatic Missions in the region are then hooked up to this NOC, from which IT services are delivered to all users in the region. Depending on how it is implemented, there will be many benefits associated with this model: It would be relatively cheap to operate because there will be few points of maintenance and excellent opportunities for optimising the regional IT resources. With an appropriate distribution and placement of NOCs with regard to Missions, it will be possible to minimize response times (latency).

Objective: *To determine the way in which the Missions in the service abroad, individually and as a whole, are to be connected in the future before 1 July 2014.*

5. Communication

The MFA's Intranet is the central platform for communication and knowledge sharing in the service abroad and home service. The Intranet is to contribute to:

- Facilitating cross-organisational communication of news, e.g. from Senior Management
- Strengthening cross-organisational collaboration, e.g. through using team sites
- Making it easier to search for individuals, expertise, competencies and data
- Expanding self-services available through MySite, e.g. team placement and areas of responsibility

The IT Department has overall responsibility for the lines of communication at Asiatisk Plads, including landline and mobile telephony, communication with external partners (OSCE, EU and the Danish Armed Forces) as well as the video-conferencing facilities. In general, each Mission has its own switchboard desk and is responsible for the purchase of mobile phones and negotiation of subscriptions. Responsibility for the regular maintenance and testing of the MFA's satellite phones lies with the users, i.e. the relevant departments and Missions. After the phasing out of shortwave radio stations in 2012, the IT Department now offers the following IT communication lines:

- Landline telephony (The Central Administration's Common Telephone System)
- Telefax
- Mobile telephony
- Network communication (e.g. approx 140,000 e-mails are processed each month)
- Video-conferences

Added to this are satellite phones (as stated above) and a number of protected communication networks for exchanging classified information. The telefax is used very little today for outgoing traffic, but the MFA in Copenhagen and many Missions continue to receive a large number of telefaxes. In Copenhagen, the incoming faxes are converted into digital files, which are subsequently distributed via e-mail according to the same guidelines as incoming e-mails.

Landline telephony

As a result of the impending closure of the MFA's telephone exchange, the transition to PC-based telephony based on Microsoft's Lync is currently being planned. Initially, the plan is to convert the communications system of the entire home service in 2013 and in parallel initiate the conversion of the service abroad. The whole project is expected to be completed by the end of 2015.

Microsoft Lync is an application that integrates several communication services, including telephony, chat, online file-sharing and video-conferencing. In addition, Lync contains a presence indicator, which enables a person to see whether a colleague is available before phoning, thus minimising wasted time. Lync telephony utilises the IT-network that the MFA uses for other data traffic. The workstation (i.e. PC) is used instead of the traditional phone. As network telephony takes up very little network capacity (e.g. in relation to file transfers), the conversation virtually costs nothing in reality.

Objective: *To complete the conversion of the MFA to Lync by the end of 2015. To complete the conversion of the entire home service to Lync by the end of 1 July 2013.*

Once Lync telephony has been fully extended to the service abroad, phone conversations between all phone numbers at the Missions and the MFA in Copenhagen will be free of further

charge. Moreover, any international calls made outside the MFA's domain by staff with smartphones will also be extremely cheap when using the Lync client on the smartphone. In the long term, the MFA will have one single phone system that works in the same way regardless of where a person is posted. At the same time, the gradual rolling out of Lync in the service abroad will also solve a serious operational problem, in that the existing telephone systems of several Missions are obsolete and due for replacement.

Mobile telephony & mobility

In the MFA, as in the rest of the world, mobility is high on the agenda, and the expectations of staff put the IT Department under considerable pressure. The smartphone and other mobile units are a particular challenge, because the very nature of these units allows staff to use them whenever and thus wherever. Today, the IT Department offers e-mail, calendar and contact synchronisation on a limited number of mobile phones with operating systems that provide reasonable security. This service is offered to staff who are equipped with an MFA mobile phone as well as staff who wish to use their own mobile phone (BYOD – *Bring your own device)*. The IT Department is in the process of implementing Mobile Device Management that supports the popular mobile platforms:

Product shelf

				
	Managed PC	Windows Phone	iPhone	iPad
Price (guideline)	DKK 4,000	DKK 2,000	DKK 5,000	DKK 4,000
Shared calendar	Yes	No	No	No
Network drive (O-drive, etc.)	Yes	No	No	No
E-mail, contacts and calendar	Yes	Yes	Yes	Yes
Intranet	Yes	No	No	No
Lync	Yes	Yes	Yes	Yes
Skype		Yes	Yes	Yes
T-environment	Yes	No	No	No
Editing of documents	Yes	Yes (limited)	Yes (limited)	Yes (limited)
CRM	Yes	No	No	No
UM-Finans	Yes	No	No	No
UM-Ark	Yes	No	No	No
Editing of websites	Yes	No	No	No

The example services presented in the product shelf on the mobile units shows that they are not suitable for file-sharing and document management. In order to avoid staff using public cloud storage solutions, such as Dropbox, Skydrive, Google Drive etc., the IT Department wishes to be able to offer a private cloud solution equipped with a secure version of the Dropbox functionality.

In the future, the ambition is also to be able to offer this service to Google Android and Microsoft Windows phones. However, the scope of user support for these phone units will be limited to support for setting up mail synchronisation and will not encompass support for standard "daily use". This limitation has been introduced to minimise the support and administrative burden on the IT Department and ServiceDesk.

For staff, the optimal solution would be to have access to the MFA's network and applications through the handheld units. In principle, this could be done in one of two ways:

1) By developing apps that provide access to specific parts of the network, such as the Intranet or the archive system.

2) By offering a terminal server access, whereby a person in principle would be able to access the network from a mobile unit in the same way that can be done today through a Managed PC (MPC).

There are advantages and disadvantages to both solutions, which, among other things, are evident in e-banking solutions. Access via apps is likely to provide the best user experience, whilst terminal server access offers the best security and the broadest range of functions. Terminal server access for mobile units could also be used to offer remote access to the workplace from the home PC/private PC. On the other hand, the extra security means that the user in principle would need to follow the same steps that are necessary today in order to log onto the network via an MPC (bit-locker, code, connection).

Objective: *To install a Mobile Device Management system that supports several platforms in 2013. To enable access to at least parts of the networks and the Intranet through handheld units. To have the prototype solution ready by the end of 2013.*

The existing MPC platform has served the MFA well and been extended to increasingly more staff with an official MFA business need to access the network also from outside the office and outside normal working hours. However, this platform needs to be modernised, either as a 2nd generation MPC or as a dual-use machine, i.e. a unit PC that functions both as a laptop/tablet and, with the help of a docking station at the workplace, as a desktop PC. Lastly, it is worth highlighting that the upcoming LYNC 2013 implementation will make it possible to hold online meetings (including video-conferences) as well as conference and IP telephony using the most widely used mobile platforms.

Objective: *To develop an MPC version 2 by the end of 2014.*

Objective: *To examine the opportunities for making encrypted mail accessible to Danish Honorary Consulates by the end of 2013 by offering the UMGATE mail system.*

Classified Network Communication

With the expansion of e-mail over the years, the Communications Centre has acquired a different and more withdrawn function than earlier. Today, focus is primarily on communication with a number of external partners (OSCE, EU and the Danish Armed Forces), primarily on secure networks which, out of regard for security considerations, cannot be integrated in the MFA's standard network. Besides discharging its standard responsibilities within communication, the Communications Centre has assumed responsibility for, among other things, monitoring the MFA's e-mailbox and handling press releases, also outside office hours. Lastly, the Communications Centre is the MFA's hub in relation to the use and administration of REGNEM, both at home and abroad. The network is currently installed at more than 20 Missions and to a limited extent at Asiatisk Plads. However, it is highly likely that this network will be expanded during the strategy period, particularly in the home service but also in the service abroad in line with ongoing specific assessments.

The most recently introduced communication system is ACID: an offline encryption tool which is owned and administered by the Council Secretariat in Brussels. It is used within the EEAS for the communication of encrypted documents between the EEAS in Brussels and local EU Embassies in a given capital, so as to avoid sending non-encrypted mails over the open Internet. The various EU Member States have different networks, each of which is protected. However, the communication between Member States is not protected. For a long time, the paper documents carried by hand were thus the only way to exchange sensitive information. The ACID solution is far from being the most modern method and corresponds most probably to the level of security associated with distributing documents by courier service. There is a considerable amount of administration incurred in maintaining this type of offline solution, which rests solely with the respective Embassy.

Video-conferences

Since 2005, the video-conferencing system has been rapidly developing, and the MFA has positively embraced the media to an almost surprisingly positive level. The number of internal and external conferences has been steadily increasing since the new method of collaborative interaction was first introduced. In 2012, more than 7,000 video-conferences were held, representing an increase of approx. 65% in relation to 2009. In this regard, there is a steadily increasing demand for video-conferencing facilities.

The video-conferences inherently save the MFA a number of official business trips, which besides the financial saving also entails a saving on the CO_2 account. Although it makes little sense to translate the number of conferences to a number of hypothetical business trips, it is clear that the opportunities for working together around the virtual conference table have led to a number of changes in the ways things are done. A better preparation of the outgoing missions means that the number of travel days can be reduced significantly. At the same time, it has been possible to put together smaller outgoing missions, which in return can draw on colleagues in Copenhagen using the video-conferencing facilities.

The most striking advantages, however, are to found in the day-to-day collaboration across time and space. With more than 100 offices across the globe, the Danish Foreign Service is a "geographically challenged organisation". The video-conference contributes daily to ensuring that terms such as "*home service"* and "*service abroad*" today primarily relate to the geographical distance between Copenhagen and the world abroad.

The video-conferencing system has an underlying "infrastructure" that enables the MFA in a video-conferencing context to interact in all imaginable constellations. The individual

conference can be compiled by many different media, such as phone, video, recording, radio and TV, but there is naturally continued room for improvement and optimisation. The technology remains limited in relation to other communication platforms (Skype, Google Talk, etc.), but the work on facilitating "cross-organisational" communication is moving rapidly forward. This can be illustrated, for example, by the present measures to integrate the MFA's future communication (phone)system, Microsoft Lync, with the video-conferencing system, which will be so extensive that the two systems will virtually melt into each other. In this regard, the challenge will increasingly be to select the right instrument for the task. There is no reason to take up a conference room or video-conferencing facilities in order to hold a simple bilateral conversation. This can be handled significantly better on Lync. On the other hand, it makes no sense either to hold large conferences or multi-user conferences on the Lync platform when there exists a dedicated alternative that offers significantly better functionality.

A major reason for the success of the video-conferences is that the system has been set up according to the "keep it simple" principle. The video-conferencing equipment is relatively easy to operate and can be used by all and sundry. The way the system is set up also makes it possible to offer use of the platform to external guests and business partners. This possibility is already used by the Missions, which can book video-conferences with, for example, Danish companies, whose representatives turn up at the MFA's external conference rooms. In principle, however, the system could easily be used by a wider audience, such as Danish firms which, through the Trade Council's mediation, wish to engage in cooperation with foreign partners. The system is also used extremely actively in the communication with the Danish media and press, in which Danish diplomats are able to use the video-conferencing facilities to participate directly in interviews in Denmark. The sound and image quality is excellent for the purpose, although there are several places where it would be possible to improve the set-up of the systems (e.g. camera at eye-level, better positioning of the microphone, more aesthetic and camera-suitable background) without major effort.

Objective: *To continue the maintenance and modernisation of the video-conferencing facilities, including expanding the user group and upgrading "studio" facilities at more Missions.*

6. Global WAN and security

The MFA's global IT network is outsourced to an external provider. The current contract was signed in August 2010 and runs for five years with an option for renewals. Under the current contract, there is today connection between the MFA in Copenhagen and 107 Missions (98 terrestrial connections and 9 satellite connections[1]). At eight Missions, which recently switched over to terrestrial connections, the IT Department has preserved a relatively cheap back-up function by retaining the old satellite connections as an alternative. In the MFA and at eight of the major Missions[2], the IT Department also has additional terrestrial connections in place as back-up. Consequently, if the main line connection fails, the MFA would be able to restore communication quickly.

As a general rule, satellite connections are converted to terrestrial connections when it is technically prudent. However, the MFA does not anticipate any major changes to the above pattern during the period covered by the present IT Strategy, 2013-1016. The advantages of collecting the network under one provider are fairly considerable, which also explains why Norway, Sweden and Finland have adopted the same model. All network connections have a guaranteed bandwidth, intelligent prioritisation of traffic (more capacity is given to live video-conferences than other traffic) and guarantee of operational reliability, i.e. technical problems are resolved by the provider as soon as the problem is reported. In addition, the closed network, which is operated by a single provider, provides a far greater degree of security. The traffic is transmitted from the Mission directly to the MFA without first having to travel around the world through different open servers.

In principle, the MFA could consider a full or partial transition to commercial ADSL connections, which undoubtedly would reduce the cost-level. However, this would also impair the quality of the service offered. Experience shows that many ADSL operators sell more capacity than the cables can deliver, and any guarantees given by local ADSL operators in the nature of things cover only the connection from the Mission to the phone operator's nearest exchange.

Objective: *To conduct an analysis of the advantages and disadvantages of switching small Missions over to local ADSL connection in countries with good telecommunications infrastructure in, for example, Western Europe and North America by the end of 2015.*

The constrictive bandwidth

The biggest disadvantage or challenge regarding the GlobalWAN network is the limited bandwidth. In general, the Missions with satellite connection only have access to approx. 512 Kbps, whereas the average terrestrial connection provides approx. 2 Mbps, depending on the size and activity level of the Mission. For example, the Danish EU Representation in Brussels has 60 Mbps. This means that there are several applications originating from Copenhagen which feel unreasonably slow, including PDB, Clover applications, the archive system and the decentralised editing and maintenance of the MFA website. It is possible to create a set-up, in which the system "is fooled" into thinking that the application lies on the decentralised service, but this does not change the fundamental problem: The digital workflows that are designed to ease administration in the MFA are also eating into an increasingly large part of the IT network, which undermines the value of these workflows. It is absolutely vital that bandwidth is incorporated into the IT projects that the business prioritises. Otherwise there is a risk that more damage than good is done.

[1] Addis Ababa, Bamako, Beirut, Damascus, Harare, Niamey, Ouagadougou, Tehran and Thimphu
[2] Beijing, Berlin, Brussels (Danish EU Representation), London, Moscow, New York, Paris and Washington

6.1 Risk and vulnerability analysis

The IT Department's security section, IT Security, constantly monitors the risks that the MFA faces and the vulnerabilities of the network and the IT systems in general. A significant part of the analytical framework is determined by the national security authorities, which are focusing increasing attention on cyber-threats and vulnerabilities. Another important part of the analytical framework are the assessments from the commercial market.

Information security is defined broadly as the total measures taken to ensure confidentiality, accessibility and integrity. Measures include physical, technical and administrative controls, including policy, regulations, procedures and governing legislation.

Threats from outside

It is important that IT Security is constantly aware of existing threats to our systems. One of the tools for this is the cooperation with GovCert, which constantly monitors the Internet networks of central government authorities to identify potential cyber attacks and alert the relevant authorities. Spam filters and anti-virus programmes must constantly be kept updated. Every second year – or whenever necessary – a penetration test should be conducted against all MFA public IP addresses. The test is to be conducted by third party experts with security clearance. On the basis of the report received, IT Security assesses which measures, if any, are to be initiated to close any holes/raise security.

Threats from inside

The proverbial chain is only as strong as its weakest link, and the enforcement of the existing procedures and guidelines is unfortunately a constant challenge. Staff have great expectations to the capacity of the IT systems to support their discharge of tasks, and when the system falls short, staff in many cases find solutions that can circumvent the restrictions arising from the existing security regulations. The whole mobility movement thus poses a quite serious risk to information security in the MFA: staff exchange sensitive information on the mobile phone in the public space, they share files and other things with everyone who can manoeuvre in the bluetooth universe, and they use both public cloud facilities and commercial platforms to store and exchange sensitive information.

The MFA constantly scans all incoming and outgoing traffic to prevent classified material leaving the network. We can identify and hold back classified material, but there are also large amounts of sensitive information distributed widely across the network. This explains also why there is a great demand for services such as Dropbox, Evernote, etc. However, these storage facilities should be used with caution: material that is placed on such facilities cannot be immediately deleted or monitored. This caution also applies to social media, such as LinkedIn and Facebook.

Need to know

The MFA's activities in the field of information security are rooted in Security Circular CIR 204 of 7 December 2001 issued by the Prime Minister's Office and ISO 27001, which, among other things, stipulates that the number of staff with access to sensitive and/or classified information is to be kept to a minimum.

Objective: *To publish the new IT Security Manual in 2013, which is to be accompanied by an information and attitude campaign in 2013-2014.*

7. Sourcing and competence development

Utilisation of the IT systems is critical for efficient business. The efforts to enhance IT competence development must therefore be broad-based and targeted at all levels. On the basis of feedback from users and recommendations from departments, the MFA's HR Department in collaboration with the IT Department and the system owners will provide competence development to those members of staff who need support on how to use IT tools. Thus, the IT Department will deliver, among other things, competence development for those members of staff who need support on how to use IT tools in connection with, for example, postings abroad. The IT coordinators at the Missions are to receive basic instruction about systems, networks, administration, security and key applications.

The use of standard systems will facilitate the enhancement of staff's IT competencies. To a wide extent, standardised course offerings can be used, making the regular reshuffle and return/departure of staff less complicated.

The technical IT skills and knowledge of IT staff and the system owners must be strengthened and maintained in accordance with the MFA's general competence development, among other things through relevant certification-oriented courses. In parallel with this competence development, the IT Department maintains its own separate competence development policy, with the aim of adapting the competence profile to the ongoing professional demands, maintenance and further development of the IT systems.

7.1 Relationship between internal and external IT competencies

Due to physical and data-related security aspects, there are no alternatives to the MFA's own IT systems, which is also why support in the service abroad is provided by the Mission's own security cleared staff. Technological progress in the IT field is moving rapidly and has far-reaching implications for the MFA's administration and service delivery. It has become increasingly more difficult for the IT Department to keep up with developments by exclusively using in-house expertise.

The boundary between insourcing and outsourcing (of IT tasks) is constantly moving, for example in relation to specialised competencies. For the MFA, special conditions apply, partly because the tasks need to be supported globally and partly because the MFA has higher security requirements than many companies and public authorities. Tasks which previously could only be performed internally can be outsourced today (e.g. through the transition from own specific systems to off-the-shelf products). In contrast, there are more areas where it makes sense to assess regularly whether the preconditions for insourcing are present.

Importance is attached to the involvement of outside expertise in areas where the MFA does not have the required IT competence available in-house, for example concerning narrow technically specialised competencies, where it will always be necessary to contact outside experts for assistance.

Besides the actual purpose for using external consultants, they must be used to improve staff's knowledge and skills both in the particular field and in their role as internal consultants. Knowledge transfer is thus incorporated as an overriding idea in the use of external consultants with particular competencies. The transfer of knowledge and skills is promoted by extensively establishing teams composed of external consultants and internal IT staff, in which proper documentation is made of the work performed and the requirements to future maintenance.

As a number of IT tasks both in the IT Department and in units with system responsibility are outsourced and will be outsourced – e.g. tasks concerning the communication systems and programming tasks - supplier management and project management will also be a significant task for the IT Department.

As a shared resource for the units and in connection with EU procurement procedures, the IT Department enters into framework agreements regarding the purchase of consultancy services. In addition, the Procurement Division of the Ministry of Finance uses SKI (National Procurement Ltd.) framework agreements.

Fact box: Sitting in front of a laptop PC with a small screen for a long time is not good for the eyes and the working environment in general. You can contact the IT Department for working aids, such as separate keyboard, better screen or ergonomic mouse, which can be attached to an MPC or an IT workstation in general.

Besides the actual purpose for using external consultants, they must be used to improve staff's knowledge and skills both in the particular field and in their role as internal consultants. **Knowledge transfer** is thus incorporated as an overriding idea in the use of external consultants with particular competencies. The transfer of knowledge and skills is promoted by extensively establishing teams composed of external consultants and internal IT staff. As a number of IT tasks both in the IT Department and in units with system responsibility are outsourced and will be outsourced – e.g. tasks concerning the communication systems and programming tasks - supplier management will also be a significant task. All solutions must be documented. The documentation must be passed to the IT Operations Group.

Competence development of the IT Department's own staff

In order to deliver the required quality, IT staff are required to keep themselves professionally up-to-date. Keeping one's professional skills and knowledge up-to-date also allows the IT Department to recruit qualified colleagues for vacant jobs internally in the department. Besides the clear advantages for the department, competence development offers IT colleagues the opportunity for a career path, which, all things being equal, contributes to increased staff satisfaction.

Objective: *To develop material enabling new departmental colleagues to acquire basic knowledge about the IT Department's tasks and about who is responsible for what and who has the expertise for what.*

Peer-to-peer training

The server person on duty and any PC client person on duty cooperates in a structured way with ServiceDesk with the aim of ensuring knowledge transfer and reinforcement of 1st level response. Colleagues interested in other professional areas in the IT Department must, by agreement, be able to familiarise themselves with the particular area.

Knowledge transfer (from consultants)

External consultants assisting the IT Department participate to a greater or smaller degree in projects that directly or indirectly involve one or more teams. A colleague from the affected

team must acquire knowledge about the work that the consultant performs at least at the orientation level.

Central Government Training Portal - Campus

Colleagues must be allowed time, by agreement, to take courses on CAMPUS.

Self-study

Colleagues must be allowed adequate time to read IT-related articles that can generate ideas and/or technical know-how. Colleagues are to be encouraged to publicise references to, and knowledge about, articles and webinars to departmental colleagues.

External courses

Knowledge that cannot be acquired through peer-to-peer training, self-study, etc. should be acquired through courses. These courses must as far as possible be completed with an exam or a certification. Similarly, participation in relevant conferences, workshops, etc. also provides a good idea about new opportunities in the field. Courses must offer knowledge and insight that have immediate practical value, i.e. the work tasks must be planned so that both the department and the colleague are able to benefit immediately from the newly acquired knowledge.

Other training and education

Many IT colleagues are self-taught. Therefore HK and SAMDATA/HK are engaged in effort to provide opportunity for informal and non-formal learning, in which the individual colleague would be able to accumulate credit towards a computer scientist qualification. This cooperation is expected to result in a specific agreement with the Copenhagen School of Science and Technology (KEA) during spring 2013. The opportunity for informal and non-formal learning has already been ensured through legislation. If a person submits an application to enrol in a training programme, the institution is required to carry out an assessment of skills acquired through informal and non-formal learning. If the institution does not have a formal method for conducting this assessment, they must experiment their way forward. Assessment of informal and non-formal learning can therefore be offered to all colleagues.

Objective: *To set up an IT training committee tasked with formulating a comprehensive training strategy for the entire department supported by regular follow-up.*

8. IT service & support

Irrespective of how many resources the MFA sets aside for developing, commissioning, operating and maintaining the IT systems, there will be a need to provide ongoing service and support to the users who work with the systems. With the help of simple guidelines and "do-it-yourself" solutions, the users can learn to help themselves and each other. However, there will still be a need for professional help and trouble-shooting. This applies to all organisations using IT systems, and it applies in particular to the MFA, whose users are spread across 105 different offices around the world without a common framework of reference or understanding for how the IT systems function.

ServiceDesk 24/7

ServiceDesk (SD) is the focal point for IT enquiries in the MFA. SD is open 24 hours a day all year round and is fully staffed during daytime hours, which is when the vast majority of enquiries are made (Asiatisk Plads, Europe and Africa). The night and weekend shifts have today been reduced to a single person, who, in addition to handling the incoming calls, staffs the Communications Centre, which has responsibility for the MFA's classified communication tools.

The evening, night and morning shifts continue to be dominated by calls from North and South America as well as Asia and the Middle East. However, in step with the wider use of MPCs and handheld units with mail and calendar synchronisation, "local" enquiries are increasingly being made outside normal working hours. As the MFA operates 24 hours a day, user support must naturally keep up with these changing developments.

Over the last few years, the IT Department has sought to reduce the number of live enquiries to SD and thereby reduce the number of staff employed in the support function. The quality and number of guidelines being drawn up is increasing, and staff are also encouraged as far as possible to report problems via the Self-Service portal, enabling SD to deal with them according to their relative priority. However, due to the need for a duty roster and rotation system that prevents the nightshift staff being overstretched, it is not possible to further reduce the number of staff at SD. On the other hand, the IT Department has made a concerted effort to raise the competence level of SD staff, so as to enable them to handle both standard problems and more complex IT problems. In this way, increasingly more enquiries are already being handled at Level 1 (SD), i.e. currently around 75% of all incoming calls to the IT Department.

If the particular staff member is unable personally to solve the problem, it will be escalated to one of the IT Department's own IT operations staff (Level 2). More than 50% of the problems that SD is unable to solve are solved at Level 2. Any unsolved problems at Level 2 are escalated to Level 3, i.e. the external consultancy firms which have won contracts to perform tasks for the MFA following a competitive tendering procedure. There will always be faults and imperfections if the solution requires detailed knowledge that the MFA's own IT operations staff neither can nor should spend time on acquiring.

Through further developing the competence level of SD staff, the IT Department in return gains access to a pool of qualified staff who can engage in many different tasks in the department, including the rolling out of new focus areas, the training and education of users, as well as installation trips to the Missions.

ServiceDesk as Single Point of Contact?

In connection with the implementation of the Clover system in the finance sphere, it was decided to allow SD to function as Single Point of Contact (SPOC). SD registers therefore all incoming enquiries, whether they are submitted by phone, mail or online reporting via the Self-Service portal under the Service Manager system. The enquiries are subsequently distributed to the relevant desk officers in the Finance Department, other MFA departments and the Danish Agency for Governmental Administration (SAM), respectively. The advantages of this solution are two-fold: firstly, staff only need to relate to one (well-known) contact point; and secondly, all enquiries are registered, which makes it significantly easier to identify patterns in the problems experienced by staff. Lastly, there are inherent economies of scale to be gained by utilising an existing workflow instead of creating a separate workflow.

In principle, the same procedure could be used in relation to other IT systems in the MFA, such as the upcoming ESDH system. However, it is vital that there is a well-functioning support organisation just below SD. There are also no limits to the number of enquiries that SD can handle, but it only makes sense to the extent that there are competent staff able to resolve the problems as and when they are registered. Further extension of SPOC to other technical systems will therefore be subjected to a specific assessment.

Operation Level Agreement

As a natural consequence of the establishment of SD as a central SPOC for other units/applications, Operation Level Agreements (OLA) must be drawn up between the IT Department and the responsible unit that clearly describe the mutual expectations and the ongoing maintenance.

Objective: *To engage in further work on the ITIL-based integration of the processes concerning Problem Management, Change/Release Management, Service Level Management, etc. where relevant.*

Personnel resource

In step with the IT Department's involvement in more cases, an assessment should be undertaken of the working pressure versus working tasks. There needs to be more focus on ensuring that new tasks are integrated in already established workflows and automated as far as possible. Even though one new task (application) does not necessarily result in one new staff member, it must be regularly assessed whether the necessary workforce is present. This assessment could be anchored in the IT Board, so that the question of any staff implications is addressed when implementing new systems.

8.1 Printing/processing in the MFA

The IT Department has responsibility for all printing and final processing of documents in the MFA, whether it concerns ensuring the availability of network printers, handling the processing of documents itself or consulting with the customers on the outsourcing of photocopying tasks. Despite many initiatives in the direction of electronic workflows and the wider use of handheld units, it must be noted that the MFA is still a relatively paper-heavy organisation.

Local printers

It has been decided to phase out the use of local printers in the home service. The phasing-out process will be implemented by no longer purchasing toner cartridges for the local printers. At the same time, the IT Department will upgrade the capacity of the network printers located in the corridors. In connection with the phasing out of local printers, a set of guidelines has been drawn up regarding the printing of sensitive information on network printers. Similarly, a set of guidelines has been drawn up regarding how to print Referrals to the Minister. Labelprint is addressed through using designated label printers as well as a central label printer, which is installed next to the other shared machines in a separate printer room on the ground floor.

There will continue to be a need for individual local printers - e.g. for visa stickers and special tasks, as well as on closed networks where there is no network printing access. In order to reduce the administrative burden in connection with trouble-shooting and updating drivers, the IT Department will endeavour to reduce the number of approved local printers to a maximum of two models (b/w).

Local printers and drivers in the service abroad

The IT Department will not maintain drivers for local printers in the same way as earlier, but will attempt to phase out as many local printers as possible also in the service abroad.

Network printers

The network printers are primarily Xerox printers. A total of 60 units are set up at Asiatisk Plads and there is at least one unit per department corridor. In addition, there are approx. 25 HP printers of different types. It is doubtful whether the capacity will be sufficient once all table printers have disappeared. On certain corridors, there are extra network sockets and here the IT Department will be able to set up extra HP network printers (in stock). It will probably be necessary to draw cables to further network sockets.

When the present printers are due for replacement (depreciation over five years with expected replacement in 2013-2014), a solution offering "follow me" print as an integral component of the printer should be examined. This functionality will provide an extra element of security and at the same time make the equipment fleet significantly more flexible (as the user can print from any unit on the network). In addition, many newer printer models offer the facility to print from a USB stick (may possibly be used when printing T-documents).

Objective: *To install software that permits even better monitoring of network printers at home and abroad in connection with replacing the printer server (expected 2013 or 2014)*

The paperless society?

Large amounts of documents continue to be printed in the MFA, and the wider use of handheld units (in which the user so-to-speak can bring an electronic version of the documents to the meeting) has not had a noticeable effect on paper consumption in the MFA. Consequently, the IT Department will prioritise a behaviour campaign aimed at reducing the quantity of printing tasks in the MFA, including drawing up a "best practice" guide about the path to the paperless society.

Objective: *To plan and implement the staff campaign about the path to the paperless society during the strategy period.*

Glossary

App	Small program, application for download
CMS	Content Management System for editing the content and design of website in a user-friendly way
CRM	Customer Relations Management system
Domæne	.dk is, for example, the Danish domain on the Internet
EEAS	European External Action Service
ESDH:	Electronic File and Document Management
FESD	Obligatory Common Standards for Public Archiving and Document Management
GlobalWAN:	The MFA's system for global communication
ISO 27001	Standard for IT security
ITIL	IT Infrastructure Library. Method for supporting IT operations, support, infrastructure development, system management and security. Recommended by the National IT and Telecom Agency.
LAN, **WAN**	Local Area Network, Wide Area Network
Latency	Delay in response time due to distance to the communication satellite or the distance to the Missions on the other side of the world.
MPC	Managed PC – a computer administered centrally by the IT Department
PDF	Portable Document Format. PDF or PDF-A is typically used for websites for non-editable viewing. PDF is not suitable for document collaboration.
PDK	Name of MFA unit responsible for Public Diplomacy
ODF	Open Document Format, standard for document exchange
OCES	Standard for digital signature
OOXML:	Open Office XML. Obligatory standard for document exchange in the public sector
OIOXML:	Public Information Online XML. Obligatory standards for data exchange between public authorities in Denmark.
OIOUBL	Standards for Government eProcurement (OIOUBL)

Operational availability: The system's operational uptime

OWA:	Outlook Web Access is a web-based Outlook product from Microsoft.
SD	Name for ServiceDesk
Second-level support:	IT questions that cannot be dealt with by ServiceDesk (first-level level support) proceed to second-level support, e.g. IT Operations Department or the Danish Agency for the Modernisation of Public Administration.
Response time:	Response time to links on Intranet and Internet
VoIP:	Voice-over-IP. Telephony via network