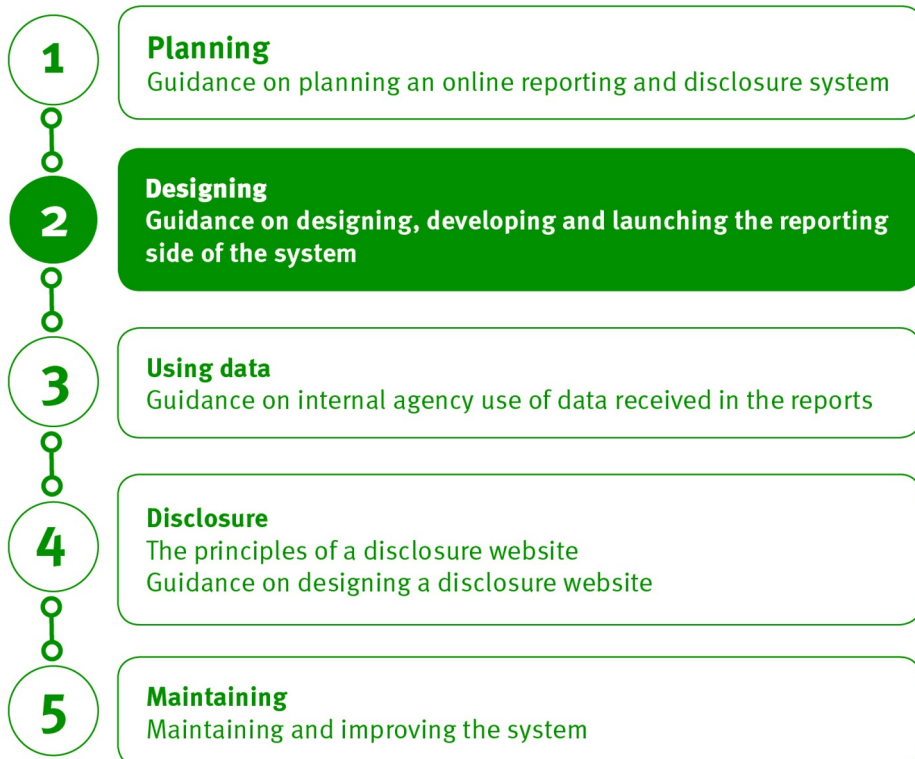


## 2. Designing and developing an online reporting platform



## 2.1. Introduction

Once the groundwork has been laid, with the aims and objectives clearly outlined, the feasibility of the project assessed and users' needs established, it is time to start developing the online reporting and disclosure system. This chapter focuses on developing the reporting side of the system; chapter 4 covers developing the public disclosure website.

This chapter draws extensively on the experiences of the countries listed in the Introduction to this Guide. It emphasizes the design phase of the reporting database and the user interface. It also focuses on elements of the design process, such as testing and launching the system. Oversight agencies are also urged to consider other salient issues, such as providing user assistance and whether the reporting system will be voluntary or mandatory.

## 2.2. Mapping the data

Before building the reporting system, you need to clarify exactly what you want to build. Mapping the data helps you achieve this. This means establishing all the information that will be entered into the system, how all these different items relate to each other and what the system does with this data. A thorough mapping of all data is recommended before any development starts. For example, before the Australian Electoral Commission (AEC) embarked on the development phase of its eReturns online reporting platform, it spent almost a year mapping out all the required data points and how they would relate to each other. Mapping all the system's possible outcomes and rules for these outcomes in advance (e.g., 'if X happens, Z will occur') meant that the Commission had a solid theoretical framework in place before any development work was undertaken.

## 2.3. Designing the reporting database

A database is a data structure that stores organized information (see Box 2.1). The reporting database is the foundation of any online reporting and disclosure system. This is the back end, where the data that parties or candidates submit are stored and classified. The reporting database gives the oversight agency a structure to view and work with the data internally. It also dictates what (and how) data will feed into the public disclosure website. The database is therefore the bridge that facilitates the disclosure of what is reported. The importance of getting this component right cannot be overstated; it is strongly recommended to invest sufficient time in database design. Any mistakes or omissions in the database structure will cost significantly more to fix later, when the applications have been built on top of them.

**Box 2.1. What is a database?**

A database is a data structure that stores organized information. Most databases contain multiple tables, which may each include several different fields. Each table records comparable items, such as political parties or electoral events. The columns in each table define the data format, such as text for the party name or date/time for the submission date of a return. The rules given to the database ensure the quality of the data set. For example, dates will always be recorded in the same way, so it will always be possible to sort a table of donations according to their submission date. As the relationships between tables are predefined, you will always be able to combine individual data sets in different tables (e.g. to filter donations by a political party).

**What to include in the database**

The exact nature of the tables that make up the database will vary from system to system depending on the country's specific reporting requirements. Annex E includes a sample list of database record types. In general, data categories include:

- actors who need to file reports (e.g. political parties, candidates);
- the type of information that needs to be reported;
- the reporting schedule;
- the sources and types of donations;
- the types of expense;
- the database user; and
- a history of recorded data and tables on the status of data.

In addition to the tables required to record the political finance data, the database will also need to include tables and views that:

- enable the user accounts to operate securely;
- enable the functions of the application; and
- provide a complete auditable history of all actions made via the applications.

### Database design considerations

#### *Achieving transparency*

Transparency of political finance data is achieved by providing detail. Data on party and campaign finance should therefore be built from the smallest units. For donations, for example, this means providing information on individual donations and their recipient, which would enable a user to search for donations made by an individual to any organization at any time. For expenses, this would mean detailing the amount, date and type of expense. Such detailed searches will only be possible in the disclosure site if the data are recorded in the database at the greatest level of detail possible.

#### *Compartmentalizing data*

Where there are data protection concerns, or where it is necessary to store and review the data before it is published, consider segregated servers. The first server sits behind a firewall and receives all data and stores it securely. The second server is read-only: it provides data to the disclosure website, and only includes information that can be made public. Moving data between the two can be managed according to a predetermined schedule.

#### *Auditable data*

To ensure that the system is auditable, build history log tables into the database design. These record every action carried out in the application and can be used to recreate who did what, and when. For example, where online authorization is employed, activity in the application may be the only legal record of a transaction. Security and audit logs could then demonstrate that data had not been tampered with.

#### *Data security*

Set up daily backups and undertake regular health checks on the servers. Ensure that firewalls and other security software is kept up-to-date to help prevent hacking. Consider running an off-site fail-over system, updated daily, that can be switched to in case of any issues with the primary system.

#### *Simplicity*

Keep the database as simple as possible to avoid confusion and errors. Where possible, avoid abbreviations, acronyms or codes in the tables' structure and use plain language to describe table names and columns.

### *Internal analysis*

Since agency staff will need to access the data for the purpose of internal analysis (see section 3.3), it is important to keep their needs in mind when setting up the database.

### *Hosting*

The choice to host the system's servers internally, externally or in the cloud will depend on several factors. It may be cheaper to buy external hosting, but at a cost of involving a third party. If you do decide to host all or some of the system internally, ensure that the agency retains infrastructure expertise.

### **Translating written reporting requirements into a database**

One of the main challenges associated with building an online platform for political finance reporting is translating the legal requirements into individual fields of data. The laws and regulations were most likely not formulated with an online system in mind. Arranging these requirements in a way that makes sense for a database is often far from straightforward, as legal text often does not lend itself to clearly defined yes/no options, which are often required for data fields. It is strongly recommended to align the legal reporting requirements with the database's data fields as much as possible. This was the approach taken in Estonia, where the law was rewritten with the online system in mind (see Box 2.5). This is the ideal scenario, where the two processes feed into each other. It also simplifies the design phase, as the law is reformed with the structure and content of data fields in mind. This approach is, however, not always a realistic option. As suggested in section 1.5, as part of the legal assessment of the feasibility study, other options for synchronizing the law and the database should also be explored, such as reforming regulations or by-laws that fall under the power of the oversight agency.

Where such a synchronized approach is not possible, it is likely that remaining grey areas will need to be resolved. For instance, marrying the legal requirements with the digital database has been a continual challenge for the FEC since its online reporting system was launched in 1995. To the extent possible, try to break down the regulations and all their reporting requirements into separately coded data points with all the possible variables that these may include. This prevents you from having to incorporate exceptions or add-ons to data points as you discover them along the way. Legal advice should be sought to ensure that the data fields accurately reflect the legal and regulatory reporting requirements.

### **Data migration**

Unless you are starting from scratch with no electronic records, you will need to migrate previously entered data into the new system. Thus you will need to

decide how many historical party and candidate disclosure financial records are to be transferred to the new system. Any new platform needs to be designed with this in mind in order to implement the data migration process as smoothly as possible. Particular attention should be paid to how best to migrate data from old data fields into newly coded ones without compromising its integrity or having to re-enter data manually. In other words, how can historic data best be ‘cleansed’ so that it is compatible with the new system and can be transferred over?

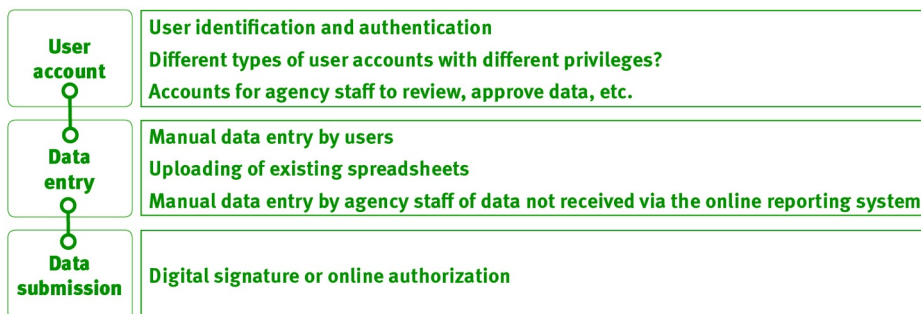
The ease with which data can be migrated will depend on its original format. If the data is already in an internal database it should be possible to convert it to the searchable online format required for the new system. In most cases this will probably be the only viable option to automatically convert old data. If the data is in spreadsheets or Word files it may be possible, but the conversion effort would be quite high and involve manual work. If the original data format is scanned paper documents it will be next to impossible to convert in good quality (even worse if the scans themselves are not good) and be a largely manual exercise. Remember to plan for the time it takes to migrate data to the new system, as this can be very time-consuming (see Box 2.2).

### Box 2.2. Data migration: lessons from the United Kingdom

The UK’s Electoral Commission brought together data from several older systems that used both databases and spreadsheets into the single database behind its PEF Online reporting system. The process took several months longer than expected due to unforeseen complexity in matching and cleansing similar data recorded differently in each source. Even after thorough regression testing to ensure the data’s accuracy following migration, several issues persisted. Most notably, system errors occurred where the application failed to handle null fields—gaps in the data that were possible in the historical records but not in the new system. On a few occasions, individuals with similar names had incorrectly been merged, which affected some user accounts.

## 2.4. The user interface

For web-based systems, an interface must be built that grants access to the system for users (to submit data) and agency staff (to review and analyse data). Agency staff will also use this interface to upload data not reported online. The reporting and analysis application is the most complex component of the system and the hardest to get right (see Figure 2.1). However, as this component controls the data input, and therefore data quality, it is essential for the success of the overall system.

**Figure 2.1. The main elements of the user interface and their functions**

The user interface should be user-friendly and intuitive to use. The design should therefore be kept as simple as possible and, as with the other phases, end users should be engaged in the design process to ensure it meets their needs. One way to do this is through user experience (UX) testing (see Box 2.3). It is recommended to avoid spending a lot of effort developing functionality for scenarios that will never, or rarely, be used.

### Box 2.3. User experience design

User experience (UX) design takes the system design and makes it work for real users. Customer- or developer-led system development often overlooks the needs of its end users in the design. With these approaches, the first time users see the system is when they test a nearly finished version, by which time it is too late to incorporate their comments. UX design is a specialist field that puts users first. A UX designer will take the outlined process and work through it with users before the system is built. They will then translate it into a scope for the developers, which should result in a system that is much more intuitive for users. The key requirement for the project team in working with UX designers is ensuring that the changes proposed by the UX designers do not compromise the statutory functions of the system.

### The user account


With a web-based reporting system, users will need to create user accounts. Access is typically granted through a user name and password. Managing user accounts can be difficult for users and resource-intensive for the oversight body staff. Making this process as simple to use and as robust as possible is always worth the extra effort. Constantly responding to requests to reset passwords can be time-

consuming for the oversight body staff, and can be avoided with an effective user account-management process.

Rather than giving a user a unique user name, consider using their email address. It is likely that this will be recorded in the database anyway, and it is already guaranteed to be unique. Users are much more likely to remember this than yet another user name. When setting up the account, request that users enter the email address twice to avoid any spelling errors.

Ensure that instructions for what to do if a user forgets their user name or password are clear. Make this process automatic as much as possible so that it does not require staff involvement. No matter how well the system is designed, users will occasionally have log-in issues that require additional help. Provide contact details and ensure that staff are equipped to handle these issues.

**Figure 2.2. The login page from the Australian eReturns site**



Source: Australian Electoral Commission, <<https://ereturns.aec.gov.au/Logon/?ReturnUrl=%2f>>.  
© Commonwealth of Australia.

Consider using existing tools as a site plugin to manage user accounts and the authorizations, rather than building a bespoke system. This can significantly reduce development costs, but may not be sufficiently flexible. State-run examples include RealMe in New Zealand or GOV.UK Verify in the UK.

The level of access of user accounts must also be considered, as well as whether different tiers of users will have different privileges. In the Australia, Mexico and the UK, for example, reporting systems allow a master administrator (who has full access and privileges) to assign subaccount holders certain, but not all, privileges. Subaccount holders cannot file reports, for example, but can enter data that then needs to be reviewed and approved.



## User identification and authentication

To ensure the integrity of an online political finance reporting system, only authorized individuals should have access. Authorized individuals must be identified before the online reporting process, for example through political party leadership or an official list of electoral candidates. To ensure that the process is secure and that the user is identifiable, use authentication that requires a unique identifier such as an email address, and thereafter allow the user to set their password.

For additional assurance where a statutory submission takes place online, consider using two-factor authentication. This requires a second piece of information in addition to a password. A common option is to send a unique, time-limited code to the user's mobile phone in a text message. Any potential imposter would need to have physical access to the user's phone as well as their password.

It is good practice to tie each declaration (stating that the information provided in the report is accurate and complete) to a particular individual who has the sole responsibility and permission to submit a declaration. This means that an electronic alternative must be found for signing a piece of paper (see the discussion on digital signatures below). Other examples of user authentication include the following:

### Electronic ID

- In Estonia, an electronic national identification (ID) card is utilized to authenticate the identity of those who file reports. A card reader is built into all new computers, but separate card readers are also readily available if required. The oversight agency was able to take advantage of this well-established national digital infrastructure when developing its system.
- In Sweden and Norway, the identity of the person submitting a report is authenticated through an electronic ID available to all persons with a bank account. In Sweden, the accountant of each political party is personally responsible for filing accurate reports. The oversight agency only publishes data from individuals who have written authorization from a political party to file reports.

### Physical receipt

- In Australia, political party agents are sent user credentials in the post, which must be signed for upon receipt. In this way, the AEC ensures that only the party agent has control of the user account, and he/she is responsible for all data submitted via eReturns. When the user first logs

on, they must create a login and password. A verification email is then sent to the user. Once the email address has been verified, the user can start to use eReturns.

### Password-protected submission of software

- In the USA, although anyone can download the reporting desktop software, only those with a password issued by the FEC can file a report. Only the current official treasurer and treasurer's assistant of a registered committee may obtain passwords. In theory, someone could pose as a valid user and receive a password. This would, however, constitute defrauding the US Government and have serious implications.

### Digital signatures

A digital signature or online authorization is used to replace the requirement to submit a paper copy with an ink signature. Before settling on this solution, though, its acceptance from a legal standpoint should be checked.

The UK Electoral Commission allows full online authorization. Party staff users may prepare a return online, but only the named party treasurer can submit it. They must log in to the system, navigate to the submission screen, where they are presented with a declaration and a two-factor authorization to identify themselves (including their email address). If the party treasurer elects not to sign electronically, the party staff still have the option to prepare the return online and print out the declaration to be signed and sent to the Commission by post. This printout includes a summary of the return details as well as the text of the declaration, but does not include the full line-by-line detail of the return. Only on receipt of this signed declaration can the return be accepted by the Commission.

In Montenegro, where legal advice upheld the requirement for an ink signature, a similar compromise solution has been adopted. The political party users prepare the return online and print out a PDF copy, including all of the details of the return and a unique barcode. This is signed by the authorized party official and submitted to the oversight body. Agency staff scan the printed PDF copy with the signature and the system presents this alongside the data submitted online. In this way oversight agency staff can visually check that the data submitted online exactly matches the document containing the signature.

These compromises may add some complexity to the system, but they ensure that the key benefits of submitting the data online are achieved even if there are legal obstacles to full online authorization.

**Figure 2.3. Online authorization for returns submitted via the Australian reporting system**

Source: Australian Electoral Commission, <[http://www.aec.gov.au/Parties\\_and\\_Representatives/financial\\_disclosure/qrg/political-parties/using.htm#menu](http://www.aec.gov.au/Parties_and_Representatives/financial_disclosure/qrg/political-parties/using.htm#menu)>. © Commonwealth of Australia.

**Figure 2.4. Online authorization via the UK's system**

Source: UK Electoral Commission, <[http://www.electoralcommission.org.uk/\\_\\_data/assets/pdf\\_file/0015/211740/EU-pefo-spending.pdf](http://www.electoralcommission.org.uk/__data/assets/pdf_file/0015/211740/EU-pefo-spending.pdf)>. Used with kind permission.

## Data entry

It is good practice with web-based systems to allow users to either enter data manually in the relevant boxes for the required data fields, or upload data from existing electronic records into the user interface. Entering data into the system manually is often a repetitive process and generally suitable only where the reporting entity has a small number of items to report. Where larger quantities of data need to be reported, it is very useful from a user's perspective to be able to upload data directly from their existing accounting systems or spreadsheets, as is the case in Australia, Colombia, Estonia, Georgia and the UK.



Incorporating existing data into the user interface also benefits the oversight body. The key requirement for entering data into the system is to ensure that it is as accurate as possible. The goal should therefore be to avoid the need for data re-entry wherever possible, while at the same time investing in finding the best technical solution to transfer data from one format to another to maintain the integrity of the data.

Allowing organizations to reconfigure their data into the standardized format required by the system helps avoid the need for data re-entry. It is also important to consider how data that is received in an incompatible format will be handled. Will the oversight body staff be required to undertake a complex and time-consuming data manipulation task, or will the person submitting the data be asked to manually enter data that could not be transferred automatically? Australia's system allows users to upload existing spreadsheets and then asks them to identify which columns of data in the spreadsheet relate to the fields the database requires. For data columns that do not match up, the system requests the user to enter the content manually. An example could be an original document which has addresses recorded all in one field, whereas the system requires them to be split into separate fields for street, postcode and state. It is recommended to allow the user to upload documents from all file types. This ability to upload data has been a big selling point of the eReturns system in Australia.

The UK provides offline templates for spreadsheets. Existing data records such as contributions and expenditure can be quickly copied across into these templates and then uploaded directly into the system. It should be noted, however, that accurately uploading large data sets from the political parties' records into the system is one of the hardest things to get right. If this process is not handled well, a great deal of time can be wasted troubleshooting or reworking the data. This is worth investing in, however, as it is a feature that is invariably appreciated by political parties. Where possible, allow existing records to be recalled by the system and make suggestions when the user is entering data, such as the details of donors. Both Brazil and Colombia have this function, which helps to ensure consistent data entry.

### **Data validation**

Introducing validation on each data entry field will help ensure the quality of the data being entered into the system. At a basic level this could mean that reports can only be submitted if all required data fields have been completed, or preventing text from being entered into a date field. It can also be used to ensure that the information entered makes sense in context. For example, the date a donation was received should be in the past but after the start of the relevant reporting period. Alternatively, validation can be dynamic, for example by preventing the date entered for a donation being accepted if it is earlier than the date entered for when the donation was received.

Validation can be a useful tool for helping to ensure compliance, but it is important that the system also allows for non-compliance. For example, a party will need to be able to report data after its deadline, or where they have exceeded a limit. In these instances, validation could be used to provide a warning message to the user instead of preventing them from entering the information. This helps prevent inaccuracies while maintaining the full functionality of the system.

## **Useful functions for the user interface**

### *Display report status to users*

The user should be able to see in one place which reports are due and the status of existing reports. This table could also show deadlines and links to edit the reports. Only relevant reports should appear, so if an entity is exempt from reporting for an event the system must filter this correctly.

### *Saving before submitting*

The user should be able to save their session and return to it later. In Australia, the eReturns online portal automatically saves what you are doing while you are working. If a system does not provide for automatic saving of data, it should at least allow the user to manually save their session.

### *Navigate between screens*

The user interface should allow the user to scroll back and forth between the stages of filing a report, so that they can review or amend what has already been entered or look ahead to what information will be required next.

### *Review screen*

A dedicated review screen at the end of the data-entry process gives the user the opportunity to see a summary of the information filled in before final submission.

### *Confirmation messages and option to print*

It is good practice that, upon submission of a report, the user receives a confirmation and the option to print out the filed financial return. Likewise, any changes made to account details should also trigger a confirmation message. In Colombia, the user receives a confirmation number, which allows them to track the progress of the review of the income and expenses report.

### *Language versions*

In some countries, providing the user interface in more than one language will be extremely beneficial for some users and will help ensure a system's success. Canada's reporting software, for example, can be used in either English or French, and Finland's web-based system is available in both Finnish and Swedish. If there



is a need, or a legal requirement, for a bilingual system, the additional cost for development and maintenance should be factored in.

### *Internal records*

A web-based reporting portal can be configured to allow the user to maintain comprehensive records of all their submitted data, both past and present. A political party could use this feature to track expenditure (as is done in Norway) or to maintain a database on donors, for example. The reporting system in Argentina has a function that allows donors' addresses to be geo-tagged on a map, providing a geographical breakdown of donors. Users of the Mexican reporting system can generate financial reports for their own internal use and select the timespan of the report by selecting start and end dates for the time period they wish to cover. Reports can then be downloaded in different file formats.

### **The user interface from the oversight body's perspective**

For many regular tasks, the oversight body staff can use the same screens as the regulated users, but with additional permissions. Staff will also need administrative and review functions as well as options for analysis or audit. A review function should allow staff to examine all of the data submitted in a return and then mark it as available for publication. The review function should also allow staff to easily see all areas of non-compliance.

Where it will not place an unnecessary burden on reporting entities, data entry fields should be separated into different categories to assist the oversight agency's review and analysis of submitted data. Uncategorized data is of limited value. It is good practice, for example, to divide expenditures into different types and request users to categorize all expenditures accordingly. Depending on their level of detail, the legal requirements for reporting may already dictate the categorization of data, as is the case with the Political Party Act of Norway.

Where the system allows for cross-agency sharing of data to assist with assessing compliance (see section 3.3), the user interface for the oversight agency should facilitate the visualization of this cross-checking.

## **2.5. Voluntary or mandatory online reporting?**

Whether online reporting will be voluntary or mandatory is a key consideration. Most countries with online reporting systems already in place still accept paper-based reporting as well. Estonia, Georgia and Lithuania, however, have mandatory online reporting on a nationwide basis, while the USA has compulsory electronic reporting for funds over a certain amount and in some states (Campaign Disclosure Project 2008). A number of considerations are presented below to help an oversight body decide whether or not online reporting should be mandatory.

### Legal basis

If an oversight agency is going to insist that regulated entities file reports online, then there needs to be a legal basis for this requirement.

### Inclusivity

All systems need to be inclusive. Use of an online reporting system should only be made compulsory if all those who are required to report have access to a computer and sufficient knowledge of how to use it. A country's Internet infrastructure also needs to be sufficiently widespread and reliable. Technology should not be an impediment to participating in democracy.

### An incremental approach

A voluntary approach has the advantage of allowing an incremental rolling out of an online reporting platform. A smaller scale allows more space to fix possible problems, and limits the damage if problems occur.

One option is to introduce the digital option in a limited geographical area and then roll it out nationally after some time has passed and any glitches have been ironed out and improvements made. Another possibility is to limit the area of activity for online reporting to one or two reporting requirements and then gradually expand to cover all areas of reporting. The Indian Election Commission is currently experimenting with online reporting, but is limiting it to candidate affidavits and candidate spending. Likewise, the new Georgian system covers party donations but not spending.

Another good option is to allow for a transition period, during which the new online system exists alongside the old offline system for a while and use is voluntary, until users have become accustomed to it. This also allows the old system to be used as a fallback option in case there are problems with the online system. Lithuania's Election Commission, for example, allowed for a two-year transition period before the online reporting system became mandatory.

### Mandatory above a certain threshold

In the USA, electronic reporting is mandatory if a campaign committee raises or spends more than USD 50,000 in a calendar year (although this does not apply to Senate candidates). Several US states also have thresholds for mandatory electronic reporting, which are normally quite low. In Tennessee and New York, for example, paper filing is permitted for those who raise or spend a total of less than USD 1,000 during the election campaign period.



### Incentives for filing electronically

If an online reporting system is voluntary, there need to be clear incentives to encourage people to use it. It should be easier than filing manually or emailing scanned documents. The system should have a number of selling points and should definitely not make the reporting process more difficult. In the UK, extended deadlines for reports filed online have been used as an incentive. In Australia, however, disincentives have been created for paper-based reporting by placing the relevant information in a less prominent place on the AEC website.

### Advantages of mandatory reporting

Mandatory reporting saves the oversight body time and effort that is otherwise spent having to encourage political parties to report online (see Box 2.4). Additionally, in a voluntary system, any data received offline must be entered manually into the database to obtain a complete picture that can then be made public on the agency website.

#### Box 2.4. The compulsory case of Estonia

Compulsory online reporting has been a success in Estonia. The country's Internet infrastructure and usage is one of the one most advanced in the world. Online services and solutions are embraced. All citizens have an electronic ID card that the political finance e-reporting system draws on. Estonia is a small country with a population of just 1.3 million people, and so introducing the system nationwide from the outset was manageable. The vast majority of citizens are used to using the Internet for official purposes. Although there is something of a generational divide in digital literacy, the oversight agency provides assistance for electronic filing to those who require it.

### Digital by default

If online reporting is to be voluntary, then consider a 'digital by default' approach. This means treating the online system as standard and promoting it accordingly, for example in guidance material on the website or in direct communication with regulated organizations. The offline option should only be considered a backup for users who are not able to use the online version.

## 2.6. In-house versus external development

An important consideration is the extent to which the development work is done in-house or outsourced to an external IT service provider. This is not always an



easy balance to strike. While a good system requires IT expertise, that may be best located outside the agency. There is, however, a danger that the oversight agency will lose control and sight of the development process and that an external service provider will produce a system that is not in line with what the agency originally envisaged. An oversight agency should not assume that an external IT supplier knows exactly what the system should look like. Even with well-developed terms of reference, the risk that an external developer will deviate from the oversight agency's vision cannot be overstated.

Norway avoided this risk by developing its online reporting platform entirely in-house, which allowed the agency to retain control throughout the process. For many agencies, however, this is not a realistic option, and the most suitable IT skills will be found externally. In this case, communication with consultants should be ongoing with regular feedback and progress reports. Adopting an Agile software development approach (see section 1.6) can be one way of achieving this, whereby there is a continuous dialogue between the oversight agency and consultants, and a flexibility to evolve and adapt the development process. One way of achieving this could be to have the external suppliers physically sit alongside the internal team at the agency, as was the case in the UK after communication issues arose. The AEC used this approach from the outset, with regular, sometimes daily, contact between the IT developers and the agency's project team. In Sweden, although the external consultants did not work at the agency, contact was also constant.

## 2.7. Building flexibility into the system

It is important to anticipate future needs and build these into the system from the outset. This includes possible regulatory changes as well as additional functions. This approach saves both time and money in the long run. While it may be tempting to think that you can always add functions later, it is not always that simple and it is highly recommended to include possible future needs in the original framework.

When Australia designed its online reporting platform, eReturns, there was an expectation that regulatory reforms would soon follow. The AEC therefore anticipated what these legal changes might be and designed eReturns to be able to incorporate them should the need arise. Although reforms have not yet come to pass, the Commission can easily adapt eReturns if required. The eReturns platform could, for example, deliver real-time reporting if regulations required it to do so.



## 2.8. Security

The security of any online system is of paramount importance. Both the reporting and disclosure sides need to be secure to protect the integrity of the data and the reputation of the oversight agency. Political finance is a sensitive topic, and all possible measures should be taken to ensure that the system is secure. This is particularly salient given the recent high-profile cyberattacks on the US Democratic Party and elsewhere, and NATO's warning in early 2017 that such attacks pose a threat to democracy itself (Vatu 2017). Security threats come in different forms, including:

- *Denial of service attacks.* These involve repeated hits on a website that prevent real users from accessing the system or data from the site.
- *Software threats.* These include viruses, which can potentially be delivered maliciously via the e-filing interface, especially where users are invited to upload documents into the system.
- *Hacking.* Apart from political finance data, the system is also likely to be vulnerable to hacking of users' personal information such as email addresses or phone numbers.

The following is a non-exhaustive list of tips to help increase security.

- *Invest in security.* As so much hinges on security, this is not something to scrim and save on. Money spent on digital security is well spent.
- *Stay up to date.* Online threats are constantly evolving, and the oversight agency needs to be aware of the latest threats and take preventative measures accordingly. Security measures need to be reviewed on a regular basis and updated.
- *Consult the experts.* In the fast-moving world of cybersecurity, it is a challenge for in-house staff to remain up-to-date on current developments. Agencies should therefore consider working in consultation with external cybersecurity consultants.
- *Schedule annual security reviews.*
- *Have a plan.* In the event that the reporting portal or public disclosure website is hacked, the oversight agency needs a contingency plan. This will help ensure that the appropriate steps are taken, that the damage is limited and that normal service can resume as quickly as possible.

## 2.9. Testing the reporting system

Testing of individual components, as well as of how they function as a whole, is a crucial part of the development process. As a rule, testing should be done multiple times so that the results can further inform and improve the reporting system before it is launched. Thorough testing during the development phase means that any issues can be addressed early on, saving both time and money that would be lost if left until later. Getting the system right at this stage also helps protect the reputation of the oversight agency. Testing should accordingly be seen as a long-term investment.

When considering testing, consider the following advice:

- *Test every single step of the filing process.* In Estonia, the Supervisory Committee on Party Financing ran three separate sites: an external site, a development site and a pre-live site. Each stage of the filing process was tested extensively as the system was being developed.
- *User experience testing.* Ensure that end users as well as the project team test the system. This is vital to create as authentic a testing environment as possible. A cross section of users, for example representing different age groups, should be asked to test the reporting process (see Box 2.5). Enlisting users to test the system also means that they feel invested in the final product and are often strong advocates of the final version.
- *Obtain expert advice.* Consider hiring a usability testing expert to translate the feedback received from users into new designs for the system based on the actual needs and preferences of users.
- *Use real data as soon as possible.* This does not need to be the complete historic data set, but it is very useful in highlighting unforeseen issues.
- *Perform stress testing.* Testing should, to the extent possible, replicate live conditions. One aspect of this is to see how the reporting system handles a high volume of traffic and data entry over a short time period, as might be the case around election time.
- *Test security.* While no digital system is ever entirely secure, repeated tests should be conducted to protect the system from hackers, and to secure the integrity of the user authentication and log-in process.
- *Consider piloting the reporting system.* This is commonly achieved by creating a beta version, although this is probably more suitable for

updating an existing system rather than a new one (see chapter 5 in this Guide).

- *Record everything in an issues log.* Prioritize issues and write up resolutions as user stories to be included in future releases. The issues log will become a core document for the life of the system.

### Box 2.5. User acceptance testing

User acceptance testing involves real users testing real scenarios. This is the only way to be sure that the system will achieve its aims, as opposed to the interpretation of these aims made by the project team and the developers. The project team should lead the testing and identify which scenarios the users need to test. These should be based on previously articulated user stories. Manage users' expectations by making it clear to them that the system is still under development and is therefore not complete, and share a list of any known issues with them. Record all user feedback. This should be consolidated by the project team and used to create new user stories. In cooperation with the developers, these will then be costed and prioritized. Resolved issues get tested in the next round of testing.

## 2.10. Launching an online reporting system

The launching of the system needs to be well planned and thought through. Elements to consider include:

- Formulating a communication plan for the launch, including details of who to reach out to (e.g. all external stakeholders and relevant internal colleagues) and what to communicate, as different groups may need to receive different information.
- The timing of the launch. It is recommended to launch the system at a time that is calm for users, so that any glitches can be ironed out with minimum adverse impact. Launching at moments when parties are filing returns, for example, should be avoided.
- Conducting user feedback sessions ahead of the launch (e.g. sharing beta software for feedback).
- Holding in-person training sessions for users. Also consider training of trainers, who can in turn train users on the new system in person. Online training alone is not sufficient.

- Planning an appropriate launch. Should the system be rolled out gradually, or would it be better with a big release? Its introduction could be divided into phases, in which the online reporting part is introduced before the public disclosure site.
- Conducting a risk assessment associated with the launch.
- Preparing for the first election, which is when the system will be properly tested.
- Showing a certain degree of leniency the first time reporting is done digitally, since punishing parties and candidates for filing incorrectly may not encourage them to do it better next time. Ask how the system can be improved to help prevent future errors.
- Conducting regular feedback sessions, technical checks and training, even after the launch of the website. The work does not stop when the website is launched.

## 2.11. Assisting parties and candidates with online reporting

Providing well-designed guidance that is tailored to users' needs is crucial to the success of any online reporting and disclosure platform. User guidance is an integral part of providing a public service and should not be considered an add-on.

While the goal should always be to make both the reporting and disclosure sites as intuitive as possible, there will always be room for additional guidance to maximize the successful and efficient use of the system. This is especially true for electronic reporting procedures, which will invariably require a greater level of user guidance than a public disclosure website. Where online reporting is optional, well-designed guidance and assistance will encourage parties and candidates to use it.

Guidance should always be clearly formulated, easily accessible to users, accurate and up-to-date. Out-of-date or inaccurate advice can undermine an oversight body's reputation and its ability to uphold compliance. If a regulated organization is non-compliant with the law, but has adhered to the oversight body's guidance, it will be nearly impossible to bring sanctions against it.

It is also good practice to solicit feedback from users and to incorporate this into guidance material. One way to do this is online, via the disclosure website.

### Types of user assistance

There is a range of different types of guidance material. The right combination will vary according to the context and users' needs.



*On-screen guidance*

Text explaining what is expected next to a data entry field can be very helpful for users, as it is quick and easy to find (see Figure 2.5). However, use on-screen help text sparingly, with caution, and only where the name of the field is ambiguous: using too many tips or making them too wordy can make the system harder to navigate as the screen becomes too cluttered, and it also makes the relevant help text harder to find. It also becomes more expensive to maintain the site.

**Figure 2.5. Example of on-screen advice from the UK’s PEF online reporting form**

Source: UK Electoral Commission, PEF Online reporting portal. Used with kind permission.

*Pop-ups*

To strike a balance between providing instant guidance and keeping the screen clear of unnecessary text, consider using pop-up boxes so that users can click on them if they need the extra help (see Figure 2.6). Where guidance is too complex to fit in a pop-up box, including a link to take the user to a dedicated page of guidance is a good option.

**Figure 2.6. Pop-up box from Norwegian reporting site**

The screenshot shows a table titled "Inntekter fra egen virksomhet" with five rows. Each row has a question mark icon in the right margin. A blue arrow points from a text box to the first question mark icon. The text box says: "Clicking on the ?-icon results in showing an explaining text".

Inntekter fra egen virksomhet	
6	Medlemskontingenter direkte innbetalt til partiledet
7	Inntekter fra lotterier, innsamlingsaksjoner og lignende
8	Kapitalinntekter (urealiserte inntekter tas ikke med)
9	Inntekter fra forretningsvirksomhet
10	Andre inntekter fra egen virksomhet

**Medlemskontingenter**

Regn bare med kontingenter som medlemmer har betalt direkte inn til partiledets egen bankkonto. Kontingenter som er samlet inn av annet partiled, for eksempel på sentralt nivå, og deretter utbetalt til partiledet, skal oppgis som interne overføringer i spørsmål 16.

-----

**Lovhenvisning:** pl § 19 (2) d

**Utdypende**

Medlemskontingenter som ble inntektsført året før rapporteringsperioden, og ikke ble betalt og ikke kunne inndrives i rapporteringsperioden, skal føres som kostnad (spørsmål 20 og 23) og ikke som inntektsreduksjon.

*Source:* Online questionnaire on sources of political party income, with a open pop-up box providing more information about financial contributions from members, RA-0604, of Statistics Norway, accessed 17 February 2017

### PDFs

Some users will prefer to print guidance. PDFs are commonly used and are very accessible. However, they can be inflexible and time consuming to update. There is also the risk that users may refer back to old, out-of-date guidance that they previously printed or saved to their computer.

### Video

Now common for many applications, video guidance should be considered. Users may find that a three-minute video is far easier to understand than pages of text on screen or on paper. Examples of video guidance include the US FEC's YouTube clips on how to use its FECFile software, and the Elections Canada website, which features short video tutorials on how to use its Electronic Financial Return software.

### Frequently asked questions (FAQs)

FAQs can be a good way of pointing users to the advice they need. The FAQs list should be actively maintained, drawing on feedback from users.

### Online guidance

Webpages of guidance are easy to create, link to and maintain (see Figure 2.7).

**Figure 2.7. Screenshot from the Australian Electoral Commission website**

## Lodge a financial disclosure return



Updated: 20 September 2012



### Who needs to lodge an annual return?

Registered political parties, associated entities, donors to political parties and third parties must lodge annual returns.

### How to lodge an annual return

Annual returns can be lodged through the [eReturns portal](#). To use eReturns you will need to obtain a username and password. Registered political parties and associated entities must [contact the AEC](#) to arrange a username and password. Donors and third parties that do not have an eReturns account may create their own.

- > [eReturns portal](#)
- > [Tips on how to lodge returns online](#)
- > [eReturns quick reference guides](#)

### Contact us

If you need additional information, assistance or to obtain a username and password, please contact the Funding and Disclosure (FAD) helpdesk via email at [fad@aec.gov.au](mailto:fad@aec.gov.au) or by calling 02 6271 4552. The FAD helpdesk is open from 9am to 5pm AEST, Monday to Friday.

Source: Australian Electoral Commission, <[http://www.aec.gov.au/parties\\_and\\_representatives/financial\\_disclosure/returns.htm](http://www.aec.gov.au/parties_and_representatives/financial_disclosure/returns.htm)>. © Commonwealth of Australia.

### *List of common mistakes*

This is a useful and simple way to preempt problems and help users in advance. The US FEC provides users with such a list.

### *Telephone helpline*

A telephone helpline is standard good practice and can be a very effective way to respond to users' queries, especially those not covered by other forms of guidance. It is especially useful when the system is new, or around a busy time such as an election. In the USA, every conversation that goes through the FEC's customer support is recorded to see if some issues keep occurring. If the operator is unsure of a solution, they can search in the call logs and view similar issues. Similarly, in



Estonia there is customer support to help with technical issues as well as an oversight agency consultant for substantive issues.

### *User manuals*

It is standard practice to produce a user manual for electronic reporting, either in PDF form or on the oversight agency's website. Links to examples are provided in the References section of this Guide. By providing clear, accessible, and comprehensive instructions and information on online reporting, an agency will minimize the number of queries from users that it has to deal with.

### *Test website*

Consider developing a test website that participants can familiarize themselves with during training sessions, or even privately. This can be invaluable when providing demonstrations in training sessions.

### *Dedicated team within the agency*

The US FEC has a dedicated information and outreach division, with 13 staff members. This division answers phone and email enquires about electronic filing, and all enquires can be made anonymously. The unit also organizes workshops and training to assist and update users on electronic filing, among other things. In addition, the Reports Analysis Division has about 35 people who do more detailed work on a one-on-one basis with users when they have filing issues. They are the frontline support for users of the e-filing software and they also review the reports once they are filed. Unlike the Information Division, the Reports Analyst Divisions' communications with filers are tracked and cannot be anonymous.

### *Training*

Consider providing a variety of different types of training for users, for example both in-person and online training. The US FEC organizes four regional conferences and four conferences in Washington, DC, during an electoral cycle to keep all stakeholders updated on the system. Online courses are also offered, focusing on specific issues. Norway provides workshops in different parts of the country that focus on exchanging users' experiences for the purpose of improving the reporting system, and to some extent include training. Colombia's National Electoral Council routinely organizes large training sessions on using its campaign finance reporting system, Cuentas Claras, ahead of elections.

It is standard practice to offer in-person training to political parties ahead of launching an online system and at subsequent later dates. Such training is extremely beneficial for users and well worth the investment for oversight agencies.



### *In-person demonstrations*

In Finland, the National Audit Office demonstrated the new system to political parties by inviting key persons to its office.

### *Issue reminders*

Reminders to file reports online can be emailed to users both before the reporting deadline and afterwards to those who do not submit reports on time.

### **Summary of key considerations for the design and development phase**

- **Simplicity:** keep the reporting user interface simple to use. It should be as intuitive and user friendly as possible. This is a fundamental part of getting people to use the system successfully.
- **User input:** as with the planning phase, continue to solicit the views and feedback of end users. This will help ensure that the design of the reporting system works for them.
- **Build the most important part first:** what is the core of the system? This should be the developmental departure point.
- **Review the development process at regular intervals.** This is especially important if external suppliers are being used to develop the system.
- **Database design is vital to the success of the system,** so invest resources in getting this right.
- **Decide whether online reporting will be voluntary or mandatory,** and consider the implications this has for the system's design.
- **Take possible future needs into consideration,** and where possible build them into the system.
- **Invest in security!**