**Exercise: Authorisation**

ACME Water has decided to implement a new database for Critical National Infrastructure (CNI) customers, such as hospitals, airports, and power stations. The database will store contact information for each organisation, general account information for invoicing and payments, current and previous incidents that affect their clean and waste water services, and a plan of any actions required to safeguard their supply. The database will be initially trialled in the Sturminster area in the hope that operations centre staff will be able to quickly access and update information about these organisations, and the services they receive.

You have been asked to devise a suitable role-based access control system for this database.

**Questions**

1.  Who are the stakeholders you need to engage when eliciting access control requirements for the database, and what requirements might they have?

*One of the difficulties in this question is that stakeholders don't directly interact with the database, but with the systems that use it. For example, accounts staff producing invoices, operations staff co-ordinating incidents, instrument technicians updating the system as part of a job, or more general information systems that managers may use in their offices. This means that stakeholders will frame their requirements based on the concrete artifacts they use in their day-to-day work, rather than abstract concepts such as types of data and forms of access.*

*The stakeholders themselves include, but are not excluded to, the following:*

* *Operations staff: They will be interested in reading contact information, information about incidents, and updating the database to assign technicians to incidents, and general information about incidents.*
* *Accounting staff: They will be interested in any information necessary to bill customers. They may require access to contact information, but information of relevance to them rather than incident management contacts in organisations.*
* *Instrument Technicians: They will need to update information about incidents while working on site*

*This is by no means an exhaustive list, and the more stakeholders you think of, the more subtle their requirements become. For example, CPNI staff or staff from emergency services may have the same requirements for reading incident data as operations staff, but we may not wish them to add data to the system. Similarly, we may wish to allow 'indirect' users like [authorised] incident managers in customer organisations to actually update information such as contact details.*

2. You would like operations manager to take responsibility for the creation and revision of access control policies.  To help them, you want to provide a tool to help them create and update access control policies; you would like the tool's user interface to build on ideas from Reeder's Expandable Grid.  Make a list of the considerations that need to be made when designing possible interfaces that build on both Expandable Grid and RBAC in general.  When answering this question, you may find it useful to make some assumptions that constrain the design space, and sketch possible interfaces.

*Here are some considerations you may wish to consider:*

* *Remember that Expandable Grid is based on a "Discretionary" rather than "Role-based" access control model. For this reason, you will need to think of at least 2 interfaces; one for assigning roles against objects, and another for users against roles. Similarly, read/write/execute permissions may be more appropriately replaced with create/read/update/delete actions.  It might also be useful to provide an interface that visualises what different users or roles might see based on existing policy settings.*
* *The design model should consider the user model for operations managers. For example, these managers may not understand how role-based access control works, so abstract terms like 'Subject' need to be replaced with [slightly] more familiar terms like 'My users’.*
* *Operations managers may not actually be the resource owner for all the data subject to access control, e.g. customer accounts contact data.  It may be worth thinking about how this sort of data should be dealt with in the roles/permissions interface.  Displaying the resource but greying it out/changing the colour may be one option, but will managers appreciate that a 'greyed out' resource means they aren't the owner, or will they take this to mean something else, e.g. the resources aren't in the database, or are allow-all by default, etc?  On the other hand, while not displaying it may reduce the number of objects on the grid, it may cause problems if a manager decides to try explicitly denying it; remember that they may not understand role-based access control, so might be working on the basis of an explicit allow/deny mental model.  Issues like these might be addressed with some fairly simple formative usability evaluation, such as low-fidelity prototyping.*
* *We may want to assume that an operations manager has teams of technicians working under him to cover certain ‘patches’, or work certain shifts. With this in mind, simply categorising staff as 'technicians' may be too coarse grained, especially when it comes to thinking about revocation.*
* *There may be a similar coarse- / fined- grained trade offs when dealing with customer or incident data as well because we may not want a team to access all records in the database but, similarly, depending on how busy operations staff are, it may not be sustainable to have an elaborate categorisation of customers depending on where on they are located, the type of infrastructure they support, how critical the infrastructure supported is, etc.*

3.  The Centre for the Protection of National Infrastructure (CPNI) have become aware of your work, and would like to trial the database in a water company serving Greater London.  How might the access control system need to be adapted, if at all?

*For this question, we need to think about how the contexts of use associated with a water company in Dorset differs from a water company in London, and what this might mean when thinking about access control usability.*

*Factors like different staff turnover rates, different modes of team working, and a need for faster access to data may mean that the access control system needs to be simplified while other mechanisms may be need to be bolstered depending on comparative risks faced by the London-based water company.*

*Operations staff and technicians working in London may work in a busier environment, making staff more likely to be non-compliant if factors like policy change lead-time get in the way of getting access to the data they need. As such, it makes sense to re-engage stakeholders from the London water company , not least because their insights may help when making decisions about how to adapt the access control system for them.*