Ohio Courts Network Requirements

Service Integration Work Group of the Infrastructure and Interoperability Subcommittee of the Supreme Court of Ohio Advisory Committee on Technology and the Courts

July 2006

Hon. John P. Bessey, Chair, Advisory Committee on Technology and the Courts

Thomas Zachman, Chair, Infrastructure and Interoperability Subcommittee

Celeste Hasselbach, Lead, Service Integration Work Group

Acknowledgements

This document is the result of years of hard work by many members of the court community and its justice partners. Countless others have assisted by visiting meetings, reviewing drafts, answering questions and providing a variety of other support.

Service Integration Work Group Members

Celeste Hasselbach, Lead
Lucas County Juvenile Court

Amanda Beck
Ohio State Legal Services Association

Anthony Berg
Cuyahoga County Juvenile Court

Michael Bracken
Rocky River Municipal Court

Brian Donato
Vorys, Sater, Seymour & Pease LLP

Daniel Dufala
Shaker Heights Municipal Court

Shawn Dunlavy
Montgomery County Clerk of Courts

Fred Engel
Ohio State Bar Association

Gretchen Faulstich
Ohio Department of Youth Services

Stan Kozlowski
Cuyahoga County Information Services Center

Matthew Krosse
Elyria Municipal Court

Carol Martin
Subject Matter Expert

Chris Moeller
Hamilton County Probate Court

Mark Schmidbauer
Ohio Bureau of Workers Compensation

Jeanne Shaw
Third District Court of Appeals

Bryce Tuohy
Office of the Ohio Attorney General

Jim Walsh
Geauga County Common Pleas Court

Chris Willkin
Ohio Office of Information Technology

Additional Past Members of the Critical Applications, Data Repository, and Portal Work Groups

Lawrence Adams
Hamilton County Court Administrator

Andrew Arana
Ohio Office of Criminal Justice Services

Charlie Arp
Ohio Historical Society

Martha Arter
Ohio Department of Job and Family Services

Darla Baker
Montgomery County Clerk of Courts, Area 2

Lee Baker
Lima Municipal Court

Sol Bermann
Mortiz College of Law

Barb Brunot
Supreme Court of Ohio

Ed Campbell
City of Lancaster

Omer Cunningham
Lorain County Clerk of Courts

Daryl Eshelman
Canton Municipal Court

Jeffrey Fortkamp
Ohio Legal Assistance Foundation

Phil Giavasis
Stark County Clerk of Courts

Randy Gonzalez
Canton Municipal Court

Jon Kaczor
Cuyahoga County Probate Court

Beth Kowalczyk
Ohio State Legal Services Association

David Lewis
Ohio Office of Criminal Justice Services

David Marburger
Baker & Hostetler LLP

John McKeown
Ohio Department of Administrative Services

Ed McNachtan
Montgomery County Clerk of Courts

Tod Mumpire
Columbiana County Clerk of Courts

Jennifer Noteman
Supreme Court of Ohio

Patty Olp
Cuyahoga County Information Services Center

Thomas O'Toole
Cuyahoga County Information Services Center

Burger Penrod
Ohio Department of Youth Services

Greg Scott
Montgomery County Juvenile Court

Mark Smith
Ohio Office of Information Technology

Wayne Smith
Chester Willcox & Saxbe LLP

Bill Ticknor
Ohio Department of Administrative Services

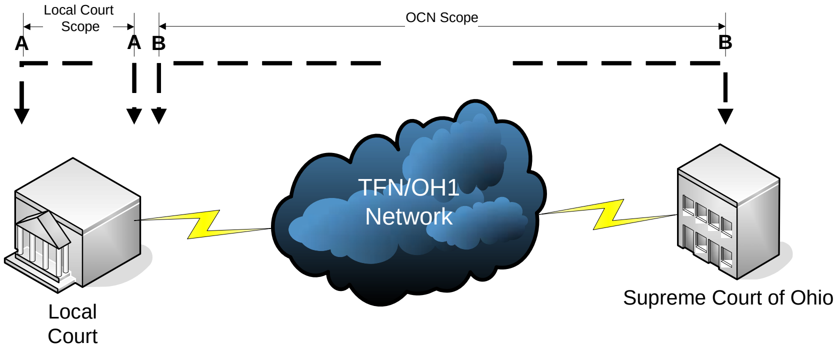
Don Worstell
Ohio Department of Youth Services

General Ohio Courts Network (OCN) Scope

The OCN responsibilities start at each local court's point of service (virtual and literal) and move back to the OCN's core. The OCN is responsible for the network's:

- Data Profiling (Extract, Transform, Load [*ETL*])
- Data Storage (Warehouse)
- Presentation of Data to Authorized Users
- Reporting of Data to Authorized Users
- Portfolio, Program and *Project Management*
- Governance and Policy
- Service Level Management (Operations, Administration)
- *Business Continuity*/ *Disaster Recovery*
- Security (Infrastructure, Transport & Applications)

Figure 1.0 OCN Scope Boundaries



Introduction

To meet the challenges of today's justice environment, judges, clerks, and court administrators, as well as law enforcement officers at all levels, must be able to make decisions quickly and intelligently, based on accurate and *timely* data. When different organizations need to share data today, they manually assemble the data and exchange it using both electronic and traditional paper methods. These approaches were sufficient when the data was not very complex and there were not many participants. However, today it is no longer possible to keep up with an ever-growing demand for justice system data sharing using inefficient and labor intensive methodologies. The Ohio Courts Network was conceived as an efficient and accessible method enabling all participants in integrated justice to access the right information at the right time. The *Data Repository* is the backbone of this network.

The Infrastructure & Interoperability Subcommittee of the Supreme Court of Ohio Advisory Committee on Technology and the Courts established the Data Repository Work Group, Critical Applications Work Group, and Portal Work Group in June of 2003. The work groups include representatives from Appeals, Municipal, Common Pleas, Probate, and Juvenile Courts; agency representatives from the Department of Youth Services, Bureau of Workers Compensation, Office of Criminal Justice Services, Department of Job and Family Services, Department of Health, Office of Information Technology and Office of the Attorney General; and practitioners representing the legal and integrated justice community. The technical background of group members ranges from very strong to moderate, and all members provide a robust sense of the business requirements from the perspectives they represent. The primary focus of the work groups was to identify the business needs or functional requirements of the Ohio Courts Network. Significant effort was made to include in the membership of each work group, non-technical stakeholders and staff who could best speak to the actual operational needs of the courts and community from the perspective of our predominantly non-technical user base.

Some assumptions have guided the process of the work groups. The work groups did not consider the cost of the overall project, but rather worked under the principal that "if you build it, funds will come." This allowed the groups to remove the limits of what could be considered and move beyond the experience of most members employed by the courts, who have previously worked with very limited funding. With this obstacle removed, the members could be proficient and revolutionary in the planning process.

The work groups took into consideration the need for local autonomy in counties, townships, cities, and villages as defined by law. Ohio is a "home rule" state, which means that each court may adopt procedures and systems of its own election to meet its particular needs. To ensure local autonomy the work groups were steadfast in identifying the *data repository* as a *data warehouse*, which will duplicate the information form the local court system. The *data repository* will not be a replacement for a case management system. The courts' participation in the *data repository* will be bound by minimum requirements that will be established under Ohio Rules of Superintendence. This left the group with the challenge to design functional business requirements for a system that could acquire data from multiple system types and convert it into clean, normalized useful information with little or no additional work for the local courts.

History of the Data Repository Work Group

The Data Repository Work Group was formed to oversee the design and construction of a statewide central *data repository* integrating content and ensuring the consistency and availability of the content from all 385 Ohio courts.
The work group established the following goals:

- Create the *data repository* design/architecture
- Build data operations and *data repository* application requirements and specifications
- Ensure that both current and future strategic reporting and information sharing needs are anticipated and included in the design considerations

From the outset the work group met on a monthly basis. The first task taken on by the work group was to define the data elements to be collected, taking into consideration all court types and all case management systems currently in use. The first list, compiled from case management system reports submitted by work group members, identified well over 7.000 data elements. The group quickly realized the necessity of a software tool or suite of tools to automate this process. The Data Repository Work Group made a recommendation to the Infrastructure & Interoperability Subcommittee, which in turn made a recommendation to the Advisory Committee on Technology and the Courts, to purchase such a tool. The Advisory Committee approved this recommendation on January 13, 2004, with purchase contingent upon the securing of funds.

The work group then moved on to the issue of reporting. The work group began by identifying a number of standard reports and forms used by each type of court, the recipient of the report and their associated level of government, as well as the frequency of report submission or generation. The reports were identified as required or courtesy reports, and as an aggregate, individual, detail, or summary level. There was an attempt to identify the current cost of generating these reports; however the work group was not able to come up with a solid standard to apply to all courts. The exercise of reviewing existing reports led to the requirement that courts be able to generate unattended reports as well as to review and approve reports before they are published or submitted. This also continued to fall in line with allowing local autonomy.

As year two began, the work group began to focus on defining the business requirements. The group identified the categories to be addressed as:

- Database
- *Data Cleansing*
- Data Validation and Integrity
- Quality Assurance
- Data Mapping
- Extensibility
- Reporting

- Data Acceptance
- Data Archiving
- Data Backup
- Ad Hoc Query
- *UDDI*
- *Disaster Recovery*

These topics were assigned to individual work group members to research and report back to the group for review and input. The information was then aggregated into the master business requirements for this project.

As the work group delved into the details of each of these topics some critical issues were identified which spurred some interim actions. The first critical issue was the need to identify and recommend an *XML* standard for the Ohio Courts Network. Based upon interaction with the Office of Criminal Justice Services, the Ohio Association of Chiefs of Police and the Office of the Attorney General, it was brought to the attention of the work group that partner entities were also in the process of standardizing and aggregating integrated justice information. Because each of these individual projects will benefit integrated justice as a whole and since the work group members agreed that it would be important to facilitate information sharing between these emerging systems, the work group recommended the adoption of the Global Justice XML Data Model (*GJXDM*) currently in use by the above-mentioned projects, as the standard for the OCN. This recommendation was approved by the I&I and Standards Subcommittees, and the standard has been adopted.

The next issues casing a great deal of discussion were expungements and sealings, which represent just one of the unique data handling issues to be addressed in the court setting. The complexity of the issue highlights how court autonomy truly impacts this project. Multi-vendor representation in case management systems will be the source of court data, and differences exist in the statutory requirements between the different types of courts for case handling. The issue of expungements and sealings has been referred to multiple work groups and engendered vigorous debates. Due to its impact on technology, the Standards Subcommittee has also recognized that this subject needs to be addressed.

The work group also explored the issues of how the *data repository* would be populated with data and how often that would happen. It was ultimately decided that the data would be pulled into the repository from courts' case management systems, rather than pushed or submitted to the repository by the court. This will allow for the implementation of a process that involves the least amount of operation or manual intervention. The frequency at which the data would be pulled from the courts will initially be once every 24 hours, with the expectation set that this frequency would increase in periodic updates that will eventually approach a near-real-time environment. Because the data is being pulled from a variety of sources the work group members felt that a real time or simultaneous update of the OCN with court data would be unrealistic, as it is necessary to allow for the local process of verifying the data is clean before posting. Although it will be quite a paradigm shift for local courts, it is possible to eventually achieve a near-real-time exchange of information. The work group also explored the possibility of intermediate "hosting" sites for courts wishing to push their data. The data would be pushed to this site by the court and then the OCN would pull from this site as though it were pulling from the local court. This would allow for autonomy on the part of the local courts while at the same time maintaining a standard operating procedure for the OCN.

History of the Critical Applications Work Group

The mission of the Critical Applications Work Group was to research, identify and recommend the critical back-end applications and application logic that will represent the architecture and support the business requirements for the Ohio Courts Network.

The work group identified the following goals:

- Design a system that will utilize the "leave and layer approach," leaving the legacy local court application systems in place and superimposing a newly designed layer of application logic, housed and managed centrally, that will enable *enterprise* wide information and process management.
- Build system requirements for data integration that utilize standardized interfaces, adapters and wrapper technologies (Web Services, SOAP, *UDDI*, WSDL) to connect legacy local applications to the newly created integration layer.
- Make design recommendations of application logic that include the transformation, routing, and process management logic necessary to accomplish data consistency, multi-step process and composite application relationships for integration.

Since its inception the work group met on a monthly basis. The group spent 2003 getting oriented and hearing presentations regarding emerging *enterprise* application integration technologies, and then spent the first few meetings of 2004 discussing possible applications needed in the OCN and categorizing applications into logical groups.

The work group developed a critical application matrix and requirements template to be used to further categorize and assign applications to group members for more detailed analysis and to standardize the information collected by each group member and ensure consistency in the requirements document.

The group identified these categories of applications:

- Administration
- *Business Continuity*
- Collaboration
- Data Management
- Operations
- Reporting
- Security
- Service Management Requirements
- Support

Once the list was finalized, these application areas were assigned to individual group members, who researched and prepared a detailed analysis of the application-specific technology. Each analysis focused primarily on functionality of the application as opposed to technical specifications, but where appropriate, technical specifications were included in the analysis. Each group member then presented the application area requirements report to the work group for review and feedback. Once a set of application area requirements was deemed complete by the work group it was placed into this master document.

History of the Portal Work Group

The Portal Work Group was formed to develop requirements for a statewide judicial information portal. The work group identified these application areas for the portal:

- Dashboard
- Local Core Business Information
- Search and Find
- Customization
- Electronic Filing
- Central Financial Transactions
- Authentication
- Interaction/Communication
- Help

The requirements define the content for an *enterprise* portal application. The requirements specify the functions such a portal must and should be able to perform, without defining how it is to perform them. The requirements are structured so they may be used as an outline to develop design specifications or for the issuance of a Request for Proposal (RFP). The OCN and vendors may choose a multitude of methods to implement the requirements.

In the fall of 2005 the three work groups joined together to form the Service Integration Work Group. The requirements documents prepared by each of the work groups were merged together and then underwent a review process by the group. Each work group member took a section or category that someone else had written and reviewed it for clarity, consistency, common requirements, assumptions, and terms to be defined. As a result of this process, the document reflects the wide range of perspectives and experiences represented in the work group.

General Assumptions

- The acquisition process will result in a suite of products – contractors will provide an entire *solution*.
- If an application group is outsourced, OCN will not implement the *solution*, but will manage the Service Level Agreement (*SLA*) with the chosen vendor.
- The vendor must monitor and meet *SLA* agreements and contracts.
- The application must support interoperability with heterogeneous platforms such as Windows/Unix/Linux/Novell.
- The application must provide support of *application layer protocols* and must meet open standards for application interfaces.
- The application must meet industry standards where applicable.
- The application must be *scalable* (supports different monitoring architectures and numbers of users).
- The application user interface must be simple and flexible.
- The applications must provide *timely* problem identification and resolution (automated where possible).
- The applications must manage hardware and software (only OCN owned and operated hardware, software, and infrastructure – not locally owned systems).
- All OCN applications will need to be operational with the Network Operating System/Operating System (*NOS/OS*); this will effectively qualify product options.
- All local court users of the OCN have an active e-mail account.
- The OCN recommends *solutions* that do not require application installation and support at local court sites.
- The system anticipates annual data growth rates of 40% or more.
- A help desk will be available.

Implementation Assumptions

- The application must be flexible/programmable/customizable/scriptable.
- The applications should allow for *distributed administration*, enabling project deployment to many different employees at different locations.
- The applications must provide stable operations (keeps *enterprise* in control, limits abuse/hacking/unauthorized access/processing or server takeover, as in virus propagation).
- All applications and interfaces must be Input/Output (*I/O)* tested and certified prior to implementation.

General Requirements

- The *solution* must be available, agile, *scalable* and ensure core functionality 24/7/365
- The *solution* must provide backups & archiving
- The *solution* must provide *disaster recovery*
- The *solution* must provide log analysis
- The *solution* must not compromise the security of *enterprise* resource and data
- The *solution* must support a variety of roles in a diverse *enterprise* environment
- The *solution* must monitor capacity, activity, availability, response time, and utilization
- The *solution* must include *capacity planning*
- Alerts must be available, utilizing email, paging and/or event messaging and escalated based upon the level of severity to the environment
- The *solution* must provide ease of operations
- All stakeholders, and particularly court personnel, require a network that is not prone to downtime and provides a secure source of critical data.
- The OCN requires an easy-to-use, locally manageable and secure method for users to access the services provided by the system.

Technology Requirements

- The *solution* must be reporting capable for all levels of management
- The *solution* must provide "what if" capabilities for modeling and design
- The *solution* must allow data exchange (the ability to import & export various file types)
- The *solution* must be *Platform-neutral*
- The system must be application-neutral
- The system must be *script capable*
- The *solution* must provide alert paging and email event messaging, alert processing (notification), logging and reporting
- The *solution* must provide standard reports
- The system must provide comprehensive asset management.
- The *solution* must provide adapter certification and verification
- The *solution* must provide *policy-based automation* to minimize data protection administration
- The *solution* must provide the ability to encrypt data.
- The *solution* must support the OCN's broader objectives of the "leave and layer" approach to data heterogeneity
- The *solution* must include strong technical support and industry-wide acceptance
- The *solution* must be supported by a large pool of qualified consultants and experts
- The *solution* must have user friendly and comprehensive administrative tools
- Data must be processed in non-proprietary formats

- The *solution* must support emerging technologies such as object oriented databases
- The *solution* must be web based and accessible
- The *solution* must support single sign-on security

Success Measures

- Revisions, *patches*, etc. are demonstrated to be up-to-date and functional through an applications/equipment audit.
- Configuration/*Release Management* is practiced
- Compliance auditing capability is available
- Third party services are scheduled in advance (proactive rather than reactive)
- Budgets parameters are met
- Seamless user functionality is in place.
- There is less use of the help desk for login functions
- Users authenticate to servers and applications without trouble or delay.
- *Intrusion detection* benchmark is met
- Speedy and thorough recovery from attacks with *minimal* loss of services
- The roots of attacks and malfunctions are identified
- Issues are located, tracked, and resolved
- Stakeholders and other users access the system with a minimum of effort.
- Reduce customer service demands on local courts.
- Meet user needs for self-service.

Definition
In the OCN environment, a user profile is a record of user-specific data that define the user's working environment. The record can include display settings, application settings, and network connections. What the user sees on his or her computer screen, as well as what files, applications and directories they have access to, is determined by how the network administrator has set up the user's profile. (*Whatis.com*)

Definition
Enterprise System Monitoring is the proactive watching over the critical resources to ensure availability, responsiveness and performance quality. This application will monitor, alert and/or recover critical applications, servers, network and related infrastructure equipment. [*Intrusion detection* not covered here]

“*Operations monitoring* will quickly become an important part of our company's Service Delivery Platform,” said John Rowell, Vice President of Operations and Engineering at OpSource. “By providing a consolidated view of individual activities across diverse and complex infrastructures, *Operations Monitoring* allows more precise assessments of operational effectiveness and ensures that business objectives and agreed upon service levels are met.”

Definition

Planning and Managing applications cover a variety of areas including those that relate to *Project Management*, Budgeting, Financial Planning, *Issue Tracking* and more. Their purpose is to present a structure from which the administrator(s) can keep track of the present *enterprise* facilities as well as plan for ongoing upgrades, updates and renewals.

Definition

Securing applications ensure sound network management practices through auditing of the *enterprise*'s infrastructure, servers and policies.

"The activities of *Information Security System Managers (ISSM)* can be broken down into the following five categories: functional security; coordination; documentation; *configuration management* and certification and accreditation; and *risk management*. Accomplishing all of the tasks associated with these five areas ensures an *ISSM* is limiting his/her organization's liability, and is accomplishing due diligence in support of the organization as well as any customers associated with the organization." (Shelley Bard, CISSP senior security network engineer, Federal Network Systems. Bard is an info security professor and has briefed the Whitehouse, Department of Defense, interest groups, industry and academia.)[1]

Definition

Administrative applications are those used to manage a wide variety of equipment and application contracts, *SLAs* and other third party support contracts. (Not including: Planning & Management; Human Resources)

Process

- Applications must determine user levels (from "Inquire Only" through "Administrative")
- Users must be defined as internal *or* external users
- User access requirements such as security certificates, authorizations, time-of-day, etc. must be included
- Applications should incorporate user *human factors* – some *profile managers* can incorporate Americans with Disabilities Act (*ADA*) characteristics such as handicapped, color-blind, keyboard restricted
- Applications must support the hierarchy of resources
- Application must support critical monitoring triggers
- *Monitoring applications* must be implemented
- Applications must fine tune to focus on pivotal failure points (*fragile artifacts*) in an ongoing, iterative process
- Applications must be configured
- Application needs to be capable of recurring audit cycles

[1] http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci948651,00.html

- A *Data Recovery Assessment* analyzing the pertinent data types and availability needs for each type of data must be completed.
- Applications must have importable system configuration data (account information, resource information, directories, security profiles, network configuration information [Domain Name Servers {*DNS*}, Dynamic Host Configuration Protocol {DHCP} tables], database tables [the data itself] including validation tables, procedures, *disaster recovery* plan, network *schemas* [Visio diagrams, Transmission Control Protocol/Internet Protocol {TCP/IP} layout], e-mail, *firewall* configuration information)
- OCN data must be normalized
- Application configuration data must be included
- Questions relating to acceptable downtime for each data source must be answered to arrive at a *Recovery Time Objective (RTO)*.

Relationships

- Applications interface with other selected applications, features, and services.
- Applications could interface with third party support.
- Applications need to cover a large number of resources including facilities, equipment, infrastructure, other applications and people.
- Applications are dependent on managing and maintaining a wide range of hardware (servers, routers, switches, hubs and *firewalls*), as well as the software and *firmware* while keeping all up to the latest known functional revision. Including service release updates and *patches*.
- Applications must interface with the security scheme
- Application access must be defined in user profiles
- The *portal-dashboard* application should support user profiles

Data Management

Data Management Executive Summary

Data Management is defined as controlling, protecting, and facilitating access to data in order to provide information consumers with *timely* access to the data they need. These functions are provided by a database management system. Data management has been separated into three sections: *ETL*, Filtering and Integration.

Definitions

Extract, Transform and Load (*ETL*)

Extract, Transform and Load software extracts records/fields from one data source, converts the data to new formats and provides the ability to load the data to other target destinations. This data handling and processing precedes final storage in the *data repository*.

To meet the challenges of the justice environment, judges, clerks, court administrators, managers and other high-level technology users have recognized that decisions must be made quickly and intelligently and must be based on accurate and *timely* data. In the past, when different organizations needed to share data they would use hand-coded bespoke applications, submit paper documents to be re-entered, or communicate via phone calls or emails. This was sufficient when the data was not very complex and there were not many participants in the process. However, hand-coded bespoke applications are not capable of handling today's complex data and the large numbers of people involved in sharing it. *ETL* tools make it possible to meet these challenges. *ETL* is considered a component of a complete *business intelligence solution*. *ETL* can be thought of as the interpreter between systems, either system to system, system to central warehouse, data file to system, data file to central warehouse, etc. Using only one interpreter allows system administrators to concentrate on learning and leveraging the *ETL* tool rather than hundreds of different systems.

Filtering

Filtering is the limiting of data based on the security level of a user.

Integration

Integration is defined as pulling together and reconciling dispersed data for analytic purposes that organizations have maintained in multiple, heterogeneous systems. Data needs to be accessed and extracted, moved and loaded, validated and cleaned, and standardized and transformed.

Data Management Security Requirements

- Authentication of incoming data.
- Secure user areas will be created for data staging:
  - All data prior to the extract function
  - All data prior to cleansing and normalization

- The database product must support field-level *encryption* and ensure that data sent across the Ohio Courts Network transport infrastructure is encrypted.

Application: Data Acquisition, Translation, and Importation to Warehouse

Definitions

Extract
The extract component has to work with whatever data sources are appropriate to the business need. Most courts will have a wide variety of potential data sources dating over many years and many different generations of technology. There may be few (or no) staff remaining who are skilled in a particular storage technology which must be used. The product should not require technical knowledge of the source environment in order to be of use.

Source systems will often be supporting a critical business process, and will therefore be sensitive to any extraction process which has a noticeable impact on performance or availability. The product should accommodate existing workloads by sharing available resources and not requiring exclusive access to the data. It will normally be required to extract information from source systems selectively rather than to simply grab the entire contents. This means that the product should be intelligent enough to determine the most effective way of selecting just the information needed depending on the storage technology in use by the source system. The product should have the ability to extract from multiple sources simultaneously and independently. It should also provide support for rules based (i.e. pull every Friday), event based (i.e. pull when new case entered) and bulk data extraction.

Transform
Transformation implies any number of changes which need to be made to the source data before it is suitable for loading into target system. Where there are multiple source systems it will normally be necessary to merge the various input streams and to reconcile any differences between them. This is unlikely to be a simple process.

Typical problems that occur are:

- Different source systems have different update schedules so that each represents a different version of the same facts
- Simple spelling errors or alternative ways of writing a name may make it difficult to recognize that information from different systems relates to the same person or organization
- Required data may be missing
- Date or other data formats may be incompatible
- Multiple records from multiple sources may need to be combined to create one complete record.

Rectifying these types of problems is known as "*data cleansing*". A number of organizations specialize in particular aspects of *data cleansing* – such as name and address "de-duping". Some types of errors simply cannot be fixed in any automated way but require human intervention. The product should provide as much automation as possible but still permit individual errors to be corrected manually. Once the data is clean any merging of inputs can be performed. After that further transformations may be required.

For example, a judge may want to access information on a specific murder case or the judge may want to see aggregate counts of murders by county. Extending this example a bit further, when we want to share this information with homeland security and other criminal justice agencies the same data may need to be formatted in several different ways.

Instead of simply reading information in, processing it and writing it out again, it is often necessary to provide temporary storage for data while all of these intermediate activities take place. Depending on requirements, this staging place may represent a considerable database in its own right.

Specialized tools automate different portions of transformations, one of which is identity matching. Data transformation should work in conjunction with user security when an agency or entity is requesting information from a data source for a data extract.

Load

The choice of target system will normally be made independently of the choice of product – this process is often treated as an afterthought, or "not strategic". Therefore, products must be extremely flexible in the format of the out put data streams they support. For a single database product there are typically a number of ways of presenting data depending on whether information is to be updated in-flight, appended as a batch task or replacing the existing contents entirely, so many different databases need to be supported.

Where the target system is an application package such as a court’s case management system, some products do not allow direct update of the underlying database but require that the supplied programming interface be used. This adds yet another level of complexity to the requirements of products.

Because of the performance implications of loading very large amounts of data, the product must be aware of any features of the target system which support parallel load (the processing of several input streams at one time to utilize multiple processors) or other performance options. It should not be necessary for staff to have deep technical knowledge of these features in order to use them successfully.

Product features can be categorized as follows:

- General Architecture
- Platform Support
- Data Extraction
- Data Integration
- *Data Cleansing* and Transformation
- Development and Administration

- Concurrency and security
- Error Handing
- Meta Data Management
- Performance
- Scheduling

Redaction

Redaction is the process of sealing or expunging case information from public consumption. The process of redaction usually entails some type of information changing on the case record that could be used to trigger an event to extract redaction information. When case information that was originally public and saved to the central warehouse needs to be redacted, a process would need to be in place to update that information based on a redacted extract file. This would either delete or secure the original public data into redacted data.

Process

- An event will trigger an extraction.
- The extraction will be transformed.
- The cleansed data will be loaded.
- The systems administrator will have audit and metadata information at every step in the process.

Data Cleansing

Also referred to as data scrubbing, the acts of detecting and removing and/or correcting a database's dirty data (i.e., data that is incorrect, out-of-date, redundant, incomplete, or formatted incorrectly). The goal of *data cleansing* is not just to clean up the data in a database but also to bring consistency to different sets of data that have been merged from separate databases. Sophisticated software applications are available to clean a database's data using algorithms, rules and look-up tables, a task that was once done manually and therefore still subject to human error. Source – Webopedia.com: http://www.webopedia.com/TERM/D/data_cleansing.html

Business Drivers

To be successful the OCN infrastructure must be available to get the right information, to the right people, all of the time.

There is a need to provide a central database of all court data which will enable standardized automated reporting and centralized analysis of data.

External access must be read-only to preserve the integrity of the official record.

Implications

Needs

Efficient, reliable, accurate and *scalable* means to access data from disparate courts, apply business rules to the data, load the data to a central warehouse, match the data from the disparate systems and return the data in meaningful ways.

Risks
Extract Risks

- Overhead on source system.
- Require exclusive access to data
- Technical knowledge of source system
- Time required
- Transform risks
- Required data missing
- Incompatible data formats
- Difficult rules for parsing/matching
- Different version of same facts (determine which is most recent and accurate)

Load Risks

- Performance implications
- Data lineage (the ability to find out when and where the data came from)

Performance Risks

- Frequency of data load must be balanced with responsiveness to queries

Relationships

- Interpreter among and between courts system and central warehouse
- Interaction with messaging function to guarantee delivery of message

Dependencies

- Identification of source data
- Identification of the sequence of mappings and transformations
- Network connectivity will need to be in place. Central repository (test repository) will need to be in place for load
- *Lightweight Directory Access Protocol (LDAP)* or similar authentication mechanism might be desirable to be in place
- Acquisition of an automated data mapping and *heuristics* tool

When/How often does it occur?

Ideally the extraction, transformation and loading would happen in real time. The closer the implementation is to real-time, the higher the benefit to stakeholders is. Some factors to consider are source system performance, source system availability, source data format, cost, *data cleansing*, and data entry mistakes. The frequency must be adjustable to allow for progression from a frequency of a number of days down to a number of minutes or near real time.

Priority Scale

1=Must have.

Success Measures

Audit and operational reports for each phase

Technology Requirements

- General Architecture
    - The *solution* must have a modular structure with standard and optional modules
    - The *solution* must include parallel use and distribution of modules
    - The *solution* must include high-availability functions
    - The *solution* must include report writers and online help
- Platform Support
    - The *solution* must include native support of source platforms
    - The *solution* must include Open DataBase Connectivity/*Java* DataBase Connectivity (ODBC/JDBC)
    - The *solution* must include targeted DataBase Management System (*DBMS*) and support for native bulk loaders
- Data Mapping
- Data Extraction
    - Data must be moved from multiple source environments
    - The *solution* must include event-based change data capture
    - The *solution* must allow bulk data movement
    - The *solution* must include components that can be used to work around the file size limitations on platforms that have such limitations
    - The *solution* must support concurrent processing of multiple source data streams without writing procedural code
- *Data Cleansing*
    - The system will import and clean data from 385 courts across Ohio. Municipal, Appellate, and Common Pleas Courts, Probation Departments, Mayor's Courts and Juvenile Courts must be considered as appendages in commonality of data for the Supreme Court.
    - A cleansing percentage of not less than 80% must be attainable and ongoing within 7 days of receiving a new database format. Defined mandatory reporting requirements.
    - Exception process for items that cannot be resolved with the automated cleansing process
    - A 100% placement rating of data should and will be attained within 14 days with the understanding that interventions are written for the remaining fields. This is under the assumption that no changes are being made to outlying data items/elements being translated. Any addition of changes to the standardized data element set would need to go through the

Governance Work Group or an equivalent policy process/group. (Note: Using known statistics of an estimated 7,000 data elements to be imported, this would mean interventions would be needed for 1400 items. After the data mapping products are used, we may result in as few as 2300 data element. This is around one-third of the original 7,000 data elements. Approximately 462 items would need intervention.)

- Data elements of multiple types must be translated with item-by-item evaluation as to the location and storage of those items that are considered other than raw data. (Note: These items may include video, audio, links, scanned images, and various standards of file format consistent with each court's individual case needs.)
- Mapped data must be cleansed before posting to the OCN to ensure consistency, conformity, accuracy, and completeness using data type validation, range checking, validation tables, and procedure-based business rules or other proven technologies.
- Provide an automated administrative review tool with the ability to cleanse data through use of a single user interface, which sends updated, purified data to both the sending and receiving files.
- Internal validation audits will communicate with all levels, including vendors and court personnel, where needed. Any problematic situations discovered will be labeled as procedural, programming or communicative and tracked for resolution through the Quality Assurance Tracking System
- The cleansing process must allow for field by field identification of whether missing or dirty data will be cause for entire record rejection.

- Data Validation and Integrity
    - The system will adopt procedures of tracking and audit methods to qualify data. Standards of item definition by individual court application must be defined and be dynamic to the resources available in computerization.
    - *Heuristic* methods are required as to minimize the amount of hours needed to manually validate the data for integrity error. *Heuristics* are definable and able to be aligned/combined. (Note: A definition of *heuristics*: involving or serving as an aid to learning, discovery, or problem-solving by experimental and especially trial-and-error methods [*heuristic* techniques, a *heuristic* assumption]; also: of or relating to exploratory problem-solving techniques that utilize self-educating techniques [as the evaluation of feedback] to improve performance [a *heuristic* computer program])
    - The methods must be controlled as to placement of data and ensure data is not revised from original state (calculations of numeric data or money fields).
    - The system must allow for redundant enforcement of business rules using data type validation, range checking, use of validation tables, procedure based business rules, or other proven technologies.
    - The system must provide business analyst tools for building or modifying business rules dynamically. Provide for creation of reusable business rules that can be applied to individual data sources.

  - The system must provide quality testing utility for purposes of verifying the correctness of every field in every record.
  - The system must provide a data integrity tool that tests for *referential integrity*.
  - The system must allow for rules that define process points that will allow acceptance of incomplete data while identifying the incomplete status.
  - Timeliness of data will be demonstrated with identification of update date/time.
- Data Integration
  - The *solution* must support various data formats, including American Standard Code for Information Interchange (ASCII), Extended Binary Coded Decimal Interchange Code (EBCDIC), and eXtensible Markup Language (*XML*)
  - The *solution* should have some level of integration with various third-party applications, including *Enterprise* Resource Planning (ERP) back-office systems, and must use open *API*s.
  - The *solution* must join information together from dissimilar types of data sources such as .txt files and Relational DataBase Management System (*RDBMS*) tables.
  - The *solution* must include Universal Description, Discovery, and Integration (*UDDI*) capabilities
  - The *solution* must include *data cleansing* and transformation functionality
  - The *solution* must allow for the creation of business rules
  - The *solution* must allow for conditional and mathematic data transformations
  - The *solution* must have the ability to parse concatenated field(s) to individual records/fields
  - The *solution* must include query parsing support
  - Support for slowly changing dimensions is very important for mature data warehousing *solutions*
  - The *solution* must offer visible data output at each stage of transformation
  - The *solution* must include incremental aggregation and computation of aggregates in one pass of the source data
  - The *solution* must have the ability to specify complex transformations using only built-in transformation objects. The goal is to specify transformations without writing any procedural code
  - The *solution* must not need to land data on disk during transform
  - The *solution* must have the ability to create a *data warehouse* on any database.
  - The *solution* must include user-defined *Structured Query Language* (SQL) statement execution subject to security roles
  - The *solution* must generate the model of transformations designed
- Development and Administration
  - The *solution* must include a centralized administration console or component
  - The *solution* must allow parallel running of components

  - The *solution* must have graphical user environments
  - The *solution* must include audit functions
  - The *solution* must include the ability to view and tune/edit the *SQL* the tool is generating against the database
  - The *solution* must support debugging and testing during development
  - The *solution* must support the analysis of transformations that failed to be accepted by the process
  - The *solution* must offer extensive reporting of the results of a session, including automatic notification of significant failures of the process
  - Making changes to developed jobs or routines should be easy
  - The *solution* must produce audit and operational reports for each data load
  - The *solution* should support unicode and multi-byte character sets localized for Japanese and other languages
  - The *solution* must include strong *data warehouse* administration functions
  - The *solution* must have the ability to back up and restore the backup of transformational model. (Version Control)
  - The *solution* must include performance tuning
  - The *solution* must include concurrency and security:
  - The *solution* must allow for a varying number of possible concurrent users and developers
  - The *solution* must have the ability to limit access for one user or a group.
  - The *solution* must have the ability to leverage *LDAP* or other in-place security mechanisms for authentication purposes.
  - How are *change management* functions or "versioning" handled within the tool? What happens if two developers attempt to make changes to the same routine or transformation object at the same time? Can older incarnations of various routines be retained for reference?
  - Does it allow you to deploy object level /operation level security? (Granularity)
  - The *solution* must have the ability to assign specific security roles as defined by the Security Work Group.
- Error Handling
  - The *solution* must allow for error recovery: If anything goes wrong, can the tool roll back the systems to a known consistent state? (Checkpoints)
  - The *solution* must allow for error handling. It can be done in various ways on a component-by-component basis. The developer can specify that no error will be tolerated, then the component will halt at the error. Error handling can be addressed within the transformation process or error-causing records can be routed elsewhere for further processing either within the application or outside. How and where is data landing in that case?
  - Database connectivity components used for extraction and load must deliver the error-handling capabilities of the database to which they are connected.

  - How flexible is the tool when executing dependent job streams? Can the tool recover from a failed job without manual intervention? How flexible is the error-condition testing? How are errors logged?
  - How well does the product respond to spurious failures such as network problems, server crashes or running out of disk space?
  - The tool should include an exception handling policy at each step of the *ETL* to direct operator to resolving error. This should be rule based, extensible and wizard driven.
- Metadata Management
  - The *solution* must include an extensible metadata repository
  - The *solution* must create *Data Definition Language* (DDL) for tables, views
  - The *solution* must allow metadata sharing with third-party applications
  - The *solution* must include metadata bridges to *Business Intelligence*/OnLine Analytical Processing (BI/OLAP) environments
  - The *solution* must include metadata capture/exchange. Does it support drawing of metadata information from the data sources? To what extent?
  - The *solution* must allow for central management of distributed engines and meta data using a central console and a global metadata repository
  - The *solution* must allow the creation of new metadata through *Genetic Data Environment* (GDE).
  - The *solution* must treat metadata as data, i.e., it can be processed and transformed
  - The *solution* must allow import of complete data models from external data modeling tools
  - The *solution* must automatically generate centralized metadata.
- Performance
  - The *solution* must allow for data partitioning and distributed processing in order to achieve best possible performance
  - Any processing component can be assigned to any server in the environment
  - Extensive logging information that indicates how resource utilization is distributed over time by processor. This allows fine-tuning of the application.
- Scheduling
  - The *solution* must have the ability to schedule sessions on time or the occurrence of a specified event, including support for command-line scheduling using external scheduling programs
  - The *solution* must have the ability to schedule File Transfer Protocol (*FTP*) sessions/web services on time or by event

Application: Filtering

Definition
The filtering application filters *data repository* data based on the role of the user.

Process

- Each data element is classified into a category.
- Each user is assigned a role based on their job responsibilities
- Each request is reviewed.

Business Drivers
The need to provide information to stakeholders while protecting both the confidentiality and integrity of the data.

Implications

- Roles must be defined and assigned to users
- Data elements must be categorized for purposes of filtering by role.
- Categories of data will be made available based on the role of the user

Relationships
Filtering is the front-end for all data requests

Dependencies

- The security structure must be defined and in place
- Security must be defined to the field level or at least to the field type (i.e. demographic, financial, etc.) level

Technology Requirements

Access to multiple data elements will have to be defined for individual users and achieved through the use of data classification, categories, and roles.

When/How often does it occur?

As needed

Priority Scale
1 = must have

Success Measures
Stakeholders receive the information they require to do their jobs and the confidentiality of the data is protected.

Application: Integration (Brokers)

Definition

An integration broker, built primarily on messaging middleware, provides an end-to-end integration platform addressing the critical business components required to completely automate business processes across the extended *enterprise*. It provides wide-ranging, pre-built application adapters, and bi-directional connectivity to multiple applications, including packaged and mainframe applications.

An integration broker does not replace traditional middleware as Message-Oriented Middleware (MOM), Remote Procedure Calling (RPC), or distributed Transaction Processing (TP) monitors. It is rather built on top of existing middleware technology, most often on messaging middleware.

Process

An integration broker extracts data from the source node at the right time, transforms the data, converts the *schema*, and routes the data to the target node. Here, the node can be an application, a program, or a person **-** as defined in the business process workflow. Communication between applications and an integration broker occurs mostly in the form of messages. An integration broker also provides a repository for archiving, searching, and retrieving these messages.

Business Drivers

To be successful the OCN infrastructure must be available to get the right information to the right people all of the time.

Implications

Risks

- Proprietary Issues: software, technology
- Compatibility with other products
- Longevity of vendor
- Extensibility

Relationships

The integration broker is the core piece to the success of the OCN project. At a minimum, it needs to integrate the disparate systems of the courts with the central repository. It should also integrate with the other OCN critical applications.

Dependencies

The network infrastructure and the central repository need to be in place. Depending on the integration broker chosen, *ETL* tools and messaging middleware may also need to be in place. System administrators and vendors will also play a vital role at this point.

When/How often does it occur?

The closer to real-time, the better (and more expensive)

Priority Scale

1=Must have.

Success Measures

Validation of complete, accurate and *timely* records

Technology Requirements

- Transformation - *syntactic*, *semantic*, *ontology*
- The *solution* must be easy to use, extensible with custom-coded rules, *xml* capable, and have built-in functions
- The *solution* must have legacy, middleware, hub to hub, spoke to hub, and object request broker connectivity
- The *solution* must have content-based, push, pull, publish-subscribe, and rule controlled flow intelligent routing
- The *solution* must include micro flow (also called dialogue management or application level protocols) support for the execution of business logic, in which some state is maintained for the duration of a short term process (such as a public process in a RosettaNet Partner Interface Process [PIP]).
- The *solution* must include business process management/workflow: long-running, multi-step processes spanning multiple applications that require their state to be managed for days or weeks. Includes support for human work activities and may include basic business process modeling.
- Adapters
    - Adapters are programs that connect the integration broker to resources. Package application adapters can vary significantly in their capabilities. The following five kinds of adapters should be considered:
        - Packaged-application adapters: programs that connect packaged applications to the integration broker
        - Technical adapters: programs that connect to heterogeneous software environments, such as:
            - Application servers
            - TP monitors
            - Component Object Model (COM)/COM+
            - ORBs (Object Request Brokers)

  - Database gateways
  - Gateways to third-party MOM
  - Mobile/wireless
- Industry standard protocol support: Support for industry standard messaging interfaces, such as:
  - Health Level Seven (HL7)/Health Insurance Portability and Accountability Act (HIPAA)
  - Electronic data interchange (transformation, gateways)
  - Financial information exchange
  - Society for Worldwide Interbank Financial
  - Telecommunication (Society for Worldwide Interbank Financial Telecommunication [SWIFT]) format
  - RosettaNet
- Adapter Development Kit (ADK) — ease and power: This is essentially the integrated *development environment* provided for adapters. Components include adapter templates, development tools (for example, introspection) and development methodologies.
- Packaged integrating processes: frameworks that define a set of activities that are used to integrate applications using the capabilities of the integration broker suite, including adapters, canonical messages and process flow

- Portability
  - Business rules owned by the OCN must be systemically portable to other *enterprise* applications critical to functionality
  - The vendor should be selectable independently of need for vendor's other suite products
- Overall Ease of Use and Power
  - The *solution* must demonstrate integration and consistency of the integration broker's functionality, such as those used for transformation, business process management or intelligent routing
  - The *solution* must support partitioning of labor (for example, business analysts for process definition, system architect for message design, software developers for adapter development)
  - The *solution* must support the programming language or languages that have been chosen as the *enterprise* standard
- Message Warehouse
  - A message warehouse provides persistent storage for messages that transits the integration broker. It is similar to a database log or journal and is used for:
    - Message tracking
    - Auditing
    - Compensating transactions
    - *Business intelligence* (such as feeding a *data warehouse*)
    - Business activity monitoring
- Administration/Management

  - The *solution* must include administration and management functionality that provides:
    - Pre-installation sizing and testing guidelines
    - Central administration
    - Configuration and distribution functions
    - The ability to expose availability and performance data
    - The ability to integrate with external management tools using protocols like simple network management protocol or *Java*
- Management Extensions
  - The *solution* must provide security functionality such as authentication and authorization, and to integrate with external security tools
  - The *solution* must use and integrate with platform management features of other technologies, such as application servers
- Business-to-Business (B2B) Capabilities
  - The *solution* must include B2B functionality that supports the transaction of business electronically.
  - Consider the following four areas:
    - Trading-partner management: the *solution* supports the management of business partner relationships through trading-partner profiles, including:
      - Protocols to be used
      - Trading-partner entitlements
      - Rules for transactions
      - Policies for nonrepudiation and provisioning that allow trading partners to set up a profile easily
    - Security
      - The *solution* supports standards that address *encryption*, authentication, authorization and nonrepudiation needs
      - The *solution* records each document of a B2B transaction in a database (this may be implemented by the message warehouse)
      - The *solution* conforms to established security standards, such as World Wide Web Consortium (W3C) Digital Certificates,
      - The *solution* conforms to W3C *encryption* or Organization for the Advancement of Structured Information Standards (OASIS) security
    - The *solution* must support Assertions Markup Language
    - The *solution* must support network connectivity: safe, reliable and interoperable connectivity for public and private networks that works through *firewalls*, including predefined logic for enveloping, validating and demonstrating interoperability with other middleware products in the exchange of business data
    - The *solution* must support end-to-end tracking and management: the ability to track a business document from its origin to its

destination, inquire on the status of that document and address exceptions

- Business Activity Monitoring
    - Event management and alerting
    - *Portal-dashboard*
    - Mobile and other notification mechanisms
    - *Business intelligence* analytics
- Web Services Support
    - The *solution* must provide support as a web services provider
        - The *solution* must have the ability to expose a defined business process as a web service
        - The *solution* must have the ability to expose an adapter as a web service
    - The *solution* must provide support as a web services consumer platform:
        - The *solution* must have the ability to assemble web services into a system
        - The *solution* must have the ability to introspect *UDDI*
    - The *solution* must support the management of web services
- Metadata Management
    - The system must record detailed metadata from all forms of integration touch points. This may be developed by the vendor or supplied through vendor partnerships.

Data Storage

Data Storage Security Requirements

- Sensitive court data will need to be highly secured. In addition to multi-user access/*profile management*, security at the role, field, row, and column levels is required.
- Sensitive court data will need to be encrypted:
  - When stored in the database
  - When transmitted through IP
  - When stored in a backup of the database
  - When the data is downloaded to laptops, PDAs, etc. In addition, these devices will need to be password protected.
- The expectation is that the database product's security will be rated and the ratings made available. The security ratings must meet U.S. Department of Justice standards.
- Complete audit capabilities of the OCN database product must include the tracking and capture of who, when and what was changed or viewed on the database. This will be referred to as the "audit log."
- Replicate database capabilities to protect the production database.

Application: Database Management System

The database and *DBMS* are the storage foundation for the *data repository*. A properly designed and tuned database will highlight the work of the network and applications as well as be available on demand for the customers it supports.

Definition

(Paraphrased from *whatis.com*) A *DBMS*, sometimes just called a database manager, is a program that lets one or more computer users create and access data in a database. The *DBMS* manages multiple users and multiple program requests so that who is using the database and what applications are accessing the database is transparent. The *DBMS* ensures the integrity and security of the data. Integrity is making sure it continues to be accessible and is consistently organized as intended, and security is making sure only those with access privileges can access the data.

In simplistic terms, a database is a collection of data that is stored in a method that promotes ease and speed of search. A database also provides isolation of the data from an application – meaning many applications can use data that is stored. It also provides ease of management of large amounts of data and better data integrity.

A *DBMS* can be thought of as a file manager that manages data in databases rather than files in file systems and is an inherent part of a database product.

Types of Databases used in Data Warehouses

The most typical *DBMS* is a *RDBMS*. In relational data stores, data which is repeated is removed and stored in one table but is referenced by other tables. The tables are related by keys that are pointers. Using the relational model assists in saving space and assures the integrity of the data. A newer kind of *DBMS* is the object-oriented database management system (ODBMS).

In ROLAP (relational) and MOLAP (multidimensional) data stores, the detailed data and the cubes of aggregate data are stored in the native stores. In HOLAP (hybrid), the detailed data is stored in a relational store, while the aggregates are stored in a multidimensional store. This provides the capacity of relational stores for large detailed-transaction databases without duplication in a multidimensional data store, along with the high performance of a multidimensional data store.

MOLAP storage provides excellent performance and data compression. It provides the potential for the most rapid query response times appropriate for cubes of aggregated data with frequent use and the necessity for rapid query response.

ROLAP query response is generally slower than that available with MOLAP or HOLAP but is a preferred *solution* for large data sets – typically detailed sales transactions or the like that are infrequently queried or are less recent historical data. ROLAP storage enables *enterprises* to take advantage of their investment in relational technology and *enterprise* data management tools.

HOLAP storage offers the benefits of MOLAP for aggregations without necessitating duplication of the underlying detail data.

HOLAP is ideal when the predominant type of queries will be against aggregates of large databases and rapid query response is required and where there is also a requirement to occasionally drill down into the source data. Cubes stored as HOLAP are smaller than the equivalent MOLAP cubes and provide faster queries than ROLAP cubes.

MultiDimensional DataBases (MDDBs) are databases constructed specifically to support the analysis of quantitative data, along multiple dimensions. These databases hold this “multidimensional” data in a “pure” multidimensional form, so that data can be analyzed over time to uncover trends. Other dimensions might involve geography, organizational unit, customer, product and others. MDDBs are optimized for fast and interactive analysis and come with analytic functionality and provide good performance, but typically require a lot of time to load and also expand the size of the source database many-fold. Because MDDBs typically contain largely aggregated data, they come with a “reach through” capability that enables access to the detailed data in the *RDBMS* that contains the cube’s source data. (A “cube” is a term usually used for a multidimensional structure, even though the structure can have more than three dimensions.)

Business Drivers

The OCN infrastructure requires a database management platform that is sophisticated, robust and available 24/7. The *DBMS* will need to store and process in a *timely* manner the extraordinary amount of data emanating from approximately 385 connected client agencies and systems.

Implications

Needs

The *DBMS* environment will be managed and administered by OCN personnel and will store aggregated, normalized, and processed information from client agencies for access by OCN web applications.

A solid, mature database product will ensure the success of the OCN. Product references must include at least 10 web-based large-scale *data repository* *enterprise* projects implemented in a *production environment* for at least 4 years. References must include those of VLDB (Very Large DataBase) implementations of more than 1 TB in size.

Product references will also include performance statistics showing the impact of 200 users running concurrent queries against the same database table.

Risks

- There are few options in the marketplace, each with their own strengths and shortfalls.
- Initial and ongoing *DBMS* licensing, support, and storage costs
- Performance problems if not sized/tuned properly
- Need staff with experience in *data warehouse* and database modeling and database administration including tuning and sizing
- Need near-immediate technical support from vendor for urgent problems

Dependencies

- The successful implementation of connectivity for all Ohio courts.
- The OCN system is first established by installing the NOS and *OS*
- The OCN security framework is in place (accounts directory, etc.)
- The OCN backup and recovery infrastructure is in place
- All *Enterprise* Application Integration (EAI) applications have been determined so that compatibility and support issues can be considered in depth.

Technology Requirements

(all Priority 1)

- The *solution* supports all common data interchanges (i.e. ODBC, JDBC, Object Linking and Embedding [OLE], Dynamic Data Exchange [DDE])
- The *solution* supports standards such as *Structured Query Language* for relational *DBMS* and such as Object Data Management Group (ODMG) for object oriented *DBMS*
- The *solution* supports a wide array of *API*s, programming languages, scripting platforms and tools
- The *solution* supports broad array of open-source integration brokers, service oriented architectures and application logic
- The *solution* supports database mirroring and partitioning
- The *solution* features extensive querying, sorting, analysis, and reporting features
- The *solution* supports bulk loading (static data and streaming data) from a variety of sources – text files, mainframes, *XML*-based repositories, other systems; extensive *ETL* features, both built in and via open 3rd party toolsets
- The *solution* supports data mining and data warehousing
- The *solution* includes customizable error handling for stored procedures and scripts, with alerting, process control and notification features
- The *solution* offers transaction and concurrency control
- The *solution* supports server *clustering*: multi-node, active-active, active-passive, online *failover* testing
- The *solution* has strong backup and recovery features for full and incremental backup, including support for common third party database backup agents, and online restore capability. Backups will need to be coordinated and tracked with software upgrades so that version control is thoroughly utilized.

- The *solution* provides strong *XML* support – native *XML* programming capabilities, efficient storage and retrieval of *XML* data, native *XML* document storage, and *XML* querying
- The *solution* provides strong security features including access logging; granular permission control (row, column, field level), *schema* access controls, strong password policies, execution-level permissions on modules and procedures, data *encryption* within the database, granular administrative roles, tools to determine the actual severity rights of any user, outbreak mechanisms to prevent colossal attack
- The *solution* is platform independent and must provide for multi-application data sharing
- The *solution* provides automatic *load balancing*
- The *solution* provides maximum scalability
- The *solution* provides tools to measure and track database and application performance
- The *solution* provides query results in under 9 seconds on large database and code which has been performance tuned
- The *solution* provides for the loading and retrieval of relational, MDDB, ROLAP, HOLAP and MOLAP data stores
- The *solution* provides for data integrity that can be verified
- The *solution* provides exceptionally high database availability

Priority Scale

1=Must Have

Success Measures

- The *solution* provides extensive auditing/logging features
- *Minimal* cost of ownership
- Customers who are getting the information they need when they need it.

Presentation of Data to Authorized Users

Application: Portal-dashboard

Definition

A *Portal-dashboard* is a user interface, similar to an automobile's dashboard, which organizes and presents information in a way that is easy to read. It provides the front-end interface between the user and the system for all applications, features, and services provided. *Portal-dashboards* can leverage *enterprise* data resources to present users with clear, actionable information.

Process

- User logs into the OCN.
- A *portal-dashboard* is displayed containing features and capabilities based on the user's security level.

Business Drivers

- *Portal-dashboard* should leverage OCN data resources to present users with clear, actionable information. *Portal-dashboards* should make it easy for the user to investigate and explore further, and to ensure *timely* business decisions.
- The *solution* must provide *agility* for the *portal-dashboard* to be controlled locally but capability also being managed centrally.
- There is a statewide need for faster service in answering basic questions regarding court phone numbers, addresses, etc.

Implications

- If the basic information is not easy to find or navigate, there will be no time savings for the customer, the help desk, or staff at all Ohio courts.
- Without providing basic information, the *portal-dashboard* will fall short of its mission to deliver a single source of basic information about all Ohio courts.
- While the *portal-dashboard* provides information about courts and cases, it is not intended to provide detailed legal research.

Risks include

- Poor design stemming from not understanding the organization's true business needs
- Data quality suffers because data is inaccurate or not properly cleansed.
- Software packages from several vendors will likely be needed to provide all of the required functionality. Getting this software to work together seamlessly will increase the complexity the *portal-dashboard* implementation.

Relationships

The *portal-dashboard* interfaces with every application, feature, and service provided.

Some of this standardized general information will provide a front-end navigation point into various local court websites.

Local courts are responsible for maintaining this information, including their list of local services.

Dependencies

- *Data Repository*
- User Profile
- Key Performance Indicators (*KPI*) need to be identified by individual users and by groups of users (i.e.: judges, clerks of court, etc.) and communicated to the designers.
- *DBMS*
- Security Infrastructure (Directory)

Technology Requirements

- The *Portal-dashboard* needs to be able to view all data resources via a show/hide methodology.
- The *portal-dashboard* should provide drill-down functionality that lets the user get to detail, if necessary.
- *Portal-dashboard* implementations should be flexible so that as user needs change the dashboard can be modified to support those changes.
- The *solution* must have a *Graphic User Interface*/*Portal-dashboard*
- *Portal-dashboard* software should handle centrally distributed applications
- *Portal-dashboard* software should be easy to administer and maintain.
- Users must be able to set preferences for *portal-dashboard* layout, screen sizing, etc.

Technologies used for *portal-dashboards* include

- *OLAP*, a query generator that provides users with the ability to explore and analyze summary and detailed information.
- Data mining tools: using statistical or modeling techniques, data mining tools make it possible to discover hidden trends.
- Data visualization tools: provide visual drill-down capacity to help users examine data graphically.
- Global Justice *XML* Data Model (*GJXDM*)
- Should support *HyperText Markup Language* (HTML), *Portable Document Format* (PDF), and other formats
- *Java* 2 Platform *Enterprise* Edition (J2EE) *Java* Compliant

Requirements

- The *solution* must refer to the most current data when opened
- The *solution* can display data in graphical and tabular forms
- The *solution* provides drill-down reporting for further detail
- The *solution* provides exception reporting to highlight trouble spots or unusual trends (alerts). The vendor must provide the means, such as a content management tool, for local courts to maintain a basic set of information and update it in a *timely* manner. This is discussed in more detail in the local core business information section found below in this document.

Priority Scale

1=Must have.

Success Measures

- The number of users continues to increase over time. If the number decreases or levels out at a point less than the maximum number of potential users, it is an indication that people are not using OCN for some reason.
- "All *business intelligence* is about getting the right information in front of the right user at the right time"[2]. If the proper general information is successfully provided, click through data should indicate increased visits to the various other areas of the website and not as many abandoned visits to the main pages. The *portal-dashboard* could also offer feedback surveys in order to determine satisfaction with the site. Participants in the surveys would be given the opportunity to share suggested improvements. Portions of customer feedback are also included in the help function.

[2] http://www.hyperion.com/downloads/uk/HyperionNews.pdf

Application: Formatting/Rendering

Definition

Rendering processes data into a format the user can view. Report rendering is separate from the initial processing of the report data in that the same report can be delivered in different formats (such as HTML, PDF, etc) for different users. Data visualization applications render large quantities of data in the form of basic charts, graphical indicators, *scorecards*, *portal-dashboards*, advanced visualizations, and animations.

Process

- The report or data request is selected
- The report is formatted and rendered based on the user's profile or output as requested by the user.

Business Drivers

Stakeholders need flexibility in viewing information from the OCN.

Implications

Since different types of users will want to view data from the OCN in different ways, data will need to be formatted and rendered based on user type. As an example, judges may wish to view information via a *portal-dashboard* or *scorecard* reports while a department manager would want to view data via conventional reports, spreadsheets, or charts.

Relationships

The *solution* must work with both the ad hoc and production reporting tools

Dependencies

- User Profile
- *Data Repository*

Technology Requirements

- The *solution* should support HTML, comma delimited, PDF, Tagged Image File Format (*TIFF*) (image), *XML*, and American National Standards Institute (*ANSI*) formats
- The *solution* should support ad hoc, scheduled production, and *OLAP* generated reporting
- The *solution* must provide a wide range of visual formats including charts, graphs, maps, and animation.

- The *solution* should provide the ability to cut and paste into other software
- The *solution* should provide mouse over capability to support drilldown requirements

When/How often does it occur?

As needed

Priority Scale

1 =must have

Success Measures

- Feedback from users
- Ratio of active users to support calls

Application: Local Core Business Information

Local courts must be able to update their core business information as needed, but reminders will be sent on a scheduled basis to validate the information. Updates will be near-real-time, but may be scheduled in advance. For example, if a fee schedule is changing on October 1, the court may input the new information in September and select the option to have the new schedule displayed beginning October 1. The effective date will be displayed on the court's boilerplate page, as will the date that all other information was last updated. Prior to the effective date of the fee schedule change, both fee schedules will be displayed with their associated dates. For other, non-financial, data fields, courts will have the option to display both the old and the new information or just the current information. The type of information to be included on the boilerplate page is listed below.

Court Name/Type
Physical Address:
  Street
  County
  City
  Zip Code

Driving Directions

Phone
Fax
E-Mail (for general inquiry)
Operating Hours

Presiding/Administrative Judge
Other Judges
Jurisdiction of Court/Serving: (list municipalities/counties)
Clerk of Court's Name

Payment Address:
  Attn:
  Street
  City
  Zip

Online Services List:
  Local Website (if available)
  Link to or text of Local Rules (if available)
  E-Filing Available (yes/no)
  Online Payments (yes/no)
  Online Records Search (yes/no)

Payment Methods:

Cash
Personal Checks
Money Orders
Cashiers Checks
Electronic Check/Automated Clearing House (*ACH*)
Wire Transfer
Credit/Debit Cards (specify)

Fee/Cost/Fine Schedule (changes to fee rules in financial engine should result in update to this list, not vice versa)

Application: Search And Find

The search and find function of the *portal-dashboard* shall be designed to function in two fashions. The first function shall be to search court records and cases by the use of predefined search parameters. These parameters are listed below. The second function shall use a "search wizard" to allow the end user the ability to define a search by different data elements. In the "search wizard" function, once the search parameter has been defined by the end user it may be saved in order for the end user to use the same search again without redefining the search.

A "docket" is a record of all the proceedings of the case. It will list all service (paperwork mailed out), paperwork filed, and other important information that must be cataloged by the clerk of court(s) for each case. Whichever method is used to retrieve case information from the above listed methods, the end user shall also have the opportunity to search the docket text with a full text search.

The site search shall search text throughout the site for the requested information. The search criteria shall then be highlighted throughout the results. In addition, the user shall also have the opportunity to select a next or previous button. This will give the end user the ability to go to each occurrence in which the search criteria is found.

On all search functions, any input field that has no data entered shall act as a wild card for that field. For text stream handling, the default functionality shall be "starts with." Additional functionalities shall include "contains," "ends with," and "exact." All search results will also include the capability to search within results. Search function will provide "did you mean" functionality.

	TABLE 1: FUNCTION AND SUB-FUNCTION	Mandatory	Optional
1.1	System shall provide case type search in conjunction with a date range and court id / name, such as DR (domestic relations), CV (civil), JL (judgment lien), etc.	X	
1.2	System shall provide search by case number and the court id or code.	X	
1.3	System shall provide search by last name and the first initial of the first name.	X	
1.4	System shall provide search by organization name.	X	
1.5	System shall provide search by Date of Birth (DOB)	X	
1.6	System shall provide search by Social Security Number (SSN)	X	
1.7	System shall provide search by Drivers License Number (DL)	X	
1.8	System shall provide search by ticket and /or citation number	X	
1.9	System shall search court locations by zip code, county, city,	X	

	and/or appellate district.		
1.10	System shall provide ability to search for a date range within one or more of the following: a. Attorney registration number and./or b. Last name and first name of the attorney.	X	
1.11	System shall provide ability to search for a selected attorney's case assignment by date range with one or more of the following: a. Attorney registration number and/or b. Last name and first name of the attorney	X	
1.12	System shall provide ability to search for a selected court's calendar by: a. Judge's last name, b. Court name or court id, or c. Date range.	X	
1.13	Search Wizard	X	
1.14	Ad Hoc Reporting		X

Sub function 1.1 The term "case type" refers to the type of action, cause, suit, or controversy, at law or equity filed with the court. Abbreviations may differ between courts. In order for this feature to work properly, a date range shall be required in conjunction with the case type and court name. The case type and court name shall be in a format that will allow the user to select them from a list.

Sub function 1.2 Each action that is filed with a court is assigned a unique case number. The system shall provide a search by case number and optionally by court name or "all" by default to be used in conjunction for this search.

Sub function 1.3 This system shall have the capability of searching by last name for parties who are individuals. The end user may also enter the first name or first initial of the first name.

Sub function 1.4 On certain occasions, lawsuits or actions are filed against organizations. The system shall have the capability to search by organization name. This would be no different from subfunction 1.3.

Sub function 1.5 The system shall have the ability to search by DOB and require that not less than the full last name be used in conjunction with the search. The DOB shall be the only identifier visible to the end user. "Starts with" functionality should not be available for this search.

Sub function 1.6 The system shall have the ability to search by SSN and require that not less than the full last name be used in conjunction for the search. The search results shall not display the SSN in any form. "Starts with" functionality should not be available for this search.

Sub function 1.7 The system shall have the ability to search by DL and require that not less than the full last name be used in conjunction with the search. "Starts with" functionality should not be available for this search.

Sub function 1.8 The system shall provide the ability to search by ticket or citation number. Each ticket or citation that is issued by law enforcement has a unique number pre-printed on the ticket or citation.

Sub function 1.9 In order for the public to gain knowledge of where a specific court is located, it is necessary that the system provide a means to present this information through different options. Any one field may be used to perform the search. Once the end user has entered any of the fields for search, all the courts matching that search will be displayed and the end user will be given an opportunity to select any of the courts listed. The system will then route the user to the appropriate court web site or, if none is available, direct them to the court's boilerplate page on the OCN site.

Sub function 1.10 The system shall be capable of performing a search for the cases the attorney is scheduled for by use of the last name and first name of an attorney or the attorney registration number in conjunction with a date range or all future schedules.

Sub function 1.11 The system shall also be capable of performing a search for actions that a particular attorney has filed. This search shall be done with the last name and first name or the attorney registration number of the attorney and case status. The option should include open, closed or all actions. In addition, a date range may be used in conjunction with all previously mentioned criteria.

Sub function 1.12 The system shall be capable of performing a search for the court's schedule for a certain date range. The search shall use the judge's last name or last name and first name or the court name (the participating courts shall be in a list for the end user to select from) and a date range.

Sub function 1.13 The "search wizard" shall be incorporated into the search and find function to enable the end user a broader search capability. This addition will in turn allow the end user the ability to design his/her own search within the parameters set. The system shall provide capability to specify "null" in any field. The parameters that will be available for the end user to select from shall be the following:

- Party Names
- Case Number
- Case Type
- Court
- County
- Calendars
- Schedules
- Judgments
- Date Range

- Actions
- Attorneys
- Judges
- Disposition

The wizard will then walk the end user through steps which will clearly define the search criteria selected. Once the end user has completed the process, the system will give the end user the ability to save the search criteria with a unique name identified by the end user.

Sub function 1.14 Ad Hoc Reporting is based on parameters, but is not limited to a small subset of parameters. The user chooses from among a large set and constructs a unique query, often for a single use. Such searches are very flexible, but require the user to know something about the nature of the data structure in order to obtain meaningful results. Ad hoc reporting will not be available to the public.

Application: Customization

Definition

The objective of the customization function is to provide frequent users of the OCN *portal-dashboard* with the ability to create a customized profile. The profile can then be used to easily access and individually customize specific services of the *portal-dashboard*.

Business Drivers

Customization will promote efficiency for frequent users of the OCN *portal-dashboard* and encourage more frequent use of the *portal-dashboard* by practitioners and others. It will be easier for users with a customized profile to get the specific information that they want from the *portal-dashboard*.

Implications

Customization will permit quick and easy access to specific and customized services offered by the *portal-dashboard*. A risk is that users of customization may infrequently access other areas of the *portal-dashboard* that could be of interest or relevance to them.

The customization feature should allow opt-in placement on the login screen of "*cookies*" on users system to expedite repeat users' login process.

If a user opts-in to customization, they create a username, password, and password hint. They can choose to give their e-mail address if they wish to have password recovery/reset capability. If the password is lost, the ability to recover customized account information is contingent upon the user knowing the password hint or supplying a valid e-mail address during account creation.

Customization must be designed so that the user's behavior can remain anonymous, and there will not be any tracking of activity.

Relationships

Users who opt-in may use services such as Authentication/Authorization, Central Financial Transactions, and stored searches.

Note – Attorneys, Pro Se Litigants, and Internal Court Personnel will have expanded customization features and authentication requirements beyond the public. See sections on attorney services, e-filing, and authentication.

Priority Scale (1=Must Have; 2=Should Have; 3=Would Like to Have)
1

Success Measures

A good measure of success could be the number of customization accounts that are created, and the average amount of activity that occurs for each account over a specific period.

TABLE 2: FUNCTION AND SUB-FUNCTION		Mandatory	Optional
2.1	Account Creation	X	
2.1.1	Required Fields	X	
2.1.1.1	User-ID	X	
2.1.1.2	Password	X	
2.1.1.3	Password Hint	X	
2.1.2	Optional Fields		X
2.1.2.1	Name		X
2.1.2.2	Email Address		
2.1.2.3	Postal Code		
2.2	Customization Options (Choices)	X	
2.2.1	Local Courts of Interest	X	
2.2.1.1	Pick from a list of all courts participating in OCN	X	
2.2.1.2	Order list by proximity to postal code		X
2.2.2	List Services		X
2.2.2.1	Opt in or out		X
2.2.2.2	Specify court and case to track		X
2.2.2.3	Specify name to track		X
2.2.2.4	Specify SSN to track		X
2.2.2.5	Include docket entry text in email sent to subscribers		
2.2.2.6	Remove item(s) from list tracking		X
2.2.3	Alerts/News/Bulletins	X	
2.2.3.1	Subscribe to alerts/new/bulletins from OCN and specified local courts	X	
2.2.4	Case Tracking	X	
2.2.4.1	Select cases to track	X	
2.2.4.2	Specify order/grouping of selected cases	X	
2.2.4.3	Link to dockets, documents, calendars, party and case information for each selected case	X	
2.2.4.4	Remove cases from tracking	X	

Application: Electronic Filing

Definition

This function seeks to provide practitioners the ability to file and over the internet, via the OCN *portal-dashboard*. It seeks to provide the individual courts an easy way to access these documents via electronic interface.

Business Drivers

This function will enable the courts and practitioners to reduce the cost and improve efficiency related to paper documents and provide practitioners a single user interface for filing with any Ohio court.

Implications

The e-filing function of the *portal-dashboard* is highly dependent upon drafting and ubiquitous adoption of policies and procedures to govern how individual courts interact with the e-filing system. Answers to questions such as those below could profoundly impact the specification:

Possible Assumptions Regarding E-filing Statewide

- There will be a single interface of e-filing across the state through the OCN *portal-dashboard*.

- Local courts’ filing and payment processes will inform changes in the interface. For instance, the e-filing interface will change its cost field based on what venue/court is selected for filing.

- Centralized e-filing through the OCN will act as a post office to route filings to local courts (both whole documents and discrete data fields) and also will act to transform the filings into *XML*/eXtensible Stylesheet Language Transformations (*XSLT*) to be accepted into local Case Management Systems (CMS). The transformation and acceptance of the data into local CMS will need to be specified through 1.) CMS Standards, 2.) E-Filing Standards, 3.) *XML* Standard, among other things.

- Pro Se filing will be provided for. The issue of authentication must be addressed, since there must be a way of getting in touch with the filer later. A registration process at the time of filing will be necessary. There must be a mechanism for regular pro se filers to store profile information in the system. This will not include storage of financial information.

- There will need to be a consistent definition of "success of filing" across the state through a superintendence rule or standard. There will need to be a procedural agreement (rule of superintendence) between local courts and the OCN commission governing the process of acceptance of e-filings. This process will need to be clearly communicated to practitioners. Courts must additionally agree to honor the time of filing from the OCN.

- While attorneys and pro se litigants may file electronically to a court, it does not guarantee that that court makes electronic copies of all documents available through some type of web service (be it local or through the OCN). For example, Hamilton County may provide the attorney, through its local website, with images of the electronic documents an attorney filed online, but the same attorney may file in Logan County and only be able to retrieve basic docket info (field screen) and not full electronic documents.

- E-filing will not be required of a filer at this time. The paper process will stay in place as a parallel process for some time to come.

- It is required that all courts must recognize e-filings as valid when the service is available through the OCN *portal-dashboard*.

Relationships

This function could be dependent on the method of authentication and authorization utilized by the *portal-dashboard*. Additionally, there are the following dependencies:

- A central financial payment engine will need to be in place prior to or concurrently with e-filing implementation. This central payments engine will route the costs/fees/fines to the local courts financial systems in the same way that the e-filing application will route the filed documents to the local CMS.

- Filing processes and their adjacent fees vary from court to court. Business process rules must be generated for every court for the e-filing system to understand what are required documents and costs, by court and by case type, by judge, etc. The process of writing these rules will be intensive (somewhat like site assessment) and will require one-on-one discussion/documentation between the OCN e-filing vendor and the local court. The analysis to identify these items is part of the business requirements.

- The Supreme Court Attorney Registration Section will work with various Infrastructure and Interoperability (I&I) work groups as well as the OCN commission to develop a secure means of authenticating attorneys through the centralized e-filing system (ex., digital certificates, smartcards, etc.). There will be a single way to authenticate attorneys through this system. There will be an electronic process for creating an attorney account.

- Courts must accept electronic credentials such as “digital signatures” and “e-notarization” standards, in their most general form, (i.e. authenticated user ID and password) as determined by the Standards Subcommittee under Sup.R. 27.

Priority Scale (1=Must Have; 2=Should Have; 3=Would Like to Have)

1 – This is a key feature for the OCN from a practitioner’s perspective, and represents a key opportunity for the court system to reduce costs.

Success Measures

The system must successfully allow users to file documents electronically. Additionally, there should be a measurable increase in the efficiency of courts receiving these filings and importing the information into their case management systems.

TABLE 3: FUNCTION AND SUBFUNCTION		Mandatory	Optional
3.0	**E-filing**		
3.1	Filed documents for a new case		
3.1.1	Gather required information to open a new case		
3.1.1.1	Collect party information		
3.1.1.1.1	First, middle, last name, mail address, e-mail address, and other information as identified by analysis of local court filing requirements.		
3.1.1.2	Collect other relevant information as identified by analysis of local court filing requirements.		
3.1.1.3	Collect Bar ID and password via single sign-on as identified by security workgroup.		
3.1.2	Upload documents and exhibits		
3.1.2.1	Allow filer to assign document type (i.e. pleading, brief, draft order) information as identified by analysis of local court filing requirements.		
3.1.2.2	Allow upload in PDF format only.		
3.1.2.3	Calculate and store *FIPS 180-2* secure hash algorithm or similar for verification that document has not been modified.		
3.1.3	Provide ability to resume upload if interrupted.		

3.1.4	Confirm Status of filing		
3.1.4.1	Perform automated transfer of filing package using the *XML* Data Model specified by the Standards Subcommittee under Sup.R. 27 for EDI (Includes hash(s) which will be used to verify documents at receiving end).		
3.1.4.2	If filing is successfully received, record date and time of filing in audit log		
3.1.4.2.1	Send email to filer reporting time of filing, status pending verification, list of what was filed, and court filed with, and confirmation number. (Include link to document and, disclaimer language explaining that court must still validate filing)		
3.1.5	Generate fees and communicate to billing subsystem		
3.2	File documents for an existing case		
3.2.1	Collect relevant information as identified by analysis of local court filing requirements.		
3.2.2	Upload documents and exhibits		
3.2.2.1	Allow filer to assign document type (i.e. pleading, brief, draft order) information as identified by analysis of local court filing requirements.		
3.2.2.2	Allow upload in PDF format only.		
3.2.2.3	Calculate and store *FIPS 180-2*, secure hash algorithm for verification that document has not been modified		
3.2.3	Provide ability to resume upload if interrupted		
3.2.4	Confirm filing is complete.		
3.2.4.1	Perform automated transfer of filing package using the *XML* Data Model specified by the Standards Subcommittee under Sup.R. 27 for EDI (Includes hash(s) which will be used to verify documents at receiving end).		
3.2.4.2	If filing is successfully received, record date and time of filing in audit log		
3.2.4.3	Send email to filer reporting time of filing, status pending verification, list of what was filed, and court filed with, and confirmation number. (Include disclaimer language explaining that court must still validate filing)		
3.2.5	Generate fees and communicate to billing subsystem		
3.3	Local rules update		
3.3.1	Provide a means to allow local courts to update local filing requirements.		

Comment [Bjd1]: Can existing case management systems support this?

Comment [Bjd2]: Can existing case management systems support this?

Application: Central Financial Transactions

Assumption: Convenience Fees will be absorbed at the OCN level rather than being passed on to either the court or the public.

Public Records Requests

Definition

To allow for the electronic payment of fees associated with public records requests.

Business Drivers

- Courts and clerks are required to satisfy all requests for public information in a *timely* fashion
- Requests for public records which are not accessible through the OCN or the local court internet could be made electronically through the OCN
- Courts and clerks are allowed to charge a fee which offsets the cost of filling these requests
- The means by which these requests are filled can be any means available to the court and acceptable to the requester

Use Case

Depending on the type and scope of information available to the users of the OCN and the local court websites, there will likely be some public information or documents which are not readily available on demand to the public via the internet. If there were an electronic means to make and potentially fill the records requests built into the system and an electronic means for calculating and paying the fees associated with these requests, this would satisfy the business need.

Implications

Possible Efficiencies: Allowing payment of costs associated with records requests online would reduce the time it takes to fill public records requests and allow courts to provide improved customer service
Possible Risks: There is no statewide standard for fees relating to public records requests.

Dependencies

This functionality is dependent on:

- An electronic means of making and filling the public records request
- A financial relationship with a credit card processing provider with competitively negotiated rates

- A well-formed privacy policy and statement that provides the requester with assurance that their privacy is protected during and after the transaction
- A secure, encrypted means of processing the transaction
- An efficient and accurate means of transferring the electronic payment information into the local case management system
- A system which handles the money being properly *ACH*d to the appropriate local bank account
- A system to provide checks and balances to ensure that all transactions are accounted for and have passed through the *portal-dashboard* and to the appropriate local court
- Local courts must keep the *portal-dashboard*'s record of their local fees and costs table up to date. The *portal-dashboard* application must provide a method for local court personnel to make the updates themselves. Updates to financial information will automatically be reflected in the display on the court's boilerplate page.

Success Measures

If the system provides a means to make and fill these requests electronically, this service is utilized by those in need of the public information, and the system properly fills the requests and appropriately transfers the money collected, then it can be considered a success.

Priority Scale (1=Must Have; 2=Should Have; 3=Would Like to Have)
3 – Would Like to Have

Pro Se

Definition

To allow for the electronic payment of fees associated with Pro Se litigants.

Business Drivers

- Pro Se litigants file necessary paperwork and if these filings were allowed to be done electronically, then electronic payment of these filing costs would need to be available
- Courts and clerks are required to collect and disburse those payments
- Payment by electronic means provides an added measure of convenience and efficiency to the process

Use Case

Pro Se litigants are a reality in the court system. Clerks of Court have a requirement to receive these filings and to collect and disburse funds associated with these filings. Electronic filing and payments will only address this business need if there is a method available to import electronic transactions directly into the local court case management system.

Implications

Possible Efficiencies: Allowing pro se litigants to pay their costs online would reduce clerks' data entry time and allow courts to provide improved customer service
Possible Risks:

- Security of financial transactions
- Proper integration with local case management systems
- Proper business rules checking to ensure filings meet rules and standards

Dependencies

This functionality is dependent on:

- The OCN offering electronic filing
- A financial relationship with a credit card processing provider with competitively negotiated rates
- A well-formed privacy policy and statement that provides the filer with assurance that their privacy is protected during and after the transaction
- A secure, encrypted means of processing the transaction
- An efficient and accurate means of transferring the electronic filing and payment information into the local case management system
- A system which handles the money being properly *ACH*d to the appropriate local bank account
- A system to provide checks and balances to ensure that all transactions and filings are accounted for and have passed through the *portal-dashboard* and to the appropriate local court

Success Measures

If the *portal-dashboard* is able to successfully offer the agreed upon transactions for electronic filing, the service is utilized by Pro Se litigants with some measure of frequency that would be determined to be successful usage, and the system successfully transfers the transaction information and money to the local court, then it is successful.

Priority Scale (1=Must Have; 2=Should Have; 3=Would Like to Have)
2 – Should Have

Attorney-Related

Definition

To allow for the electronic payment of attorney-related transactions.

Business Drivers

- Attorneys file paperwork on behalf of the plaintiff/defendant. If these filings were allowed to be done electronically, then electronic payment of these filing costs would need to be available
- Courts and clerks are required to collect and disburse those payments
- Payment by electronic means provides an added measure of convenience and efficiency to the process

Use Case

Attorneys have requested the ability to file documents electronically. Clerks of Court have a requirement to collect and disburse these payments. Electronic payments will only address this business need if there is a method available to import electronic transactions directly into the local court case management system.

Implications

Possible Efficiencies:

- Reduce clerk's data entry time, improved customer service

Possible Risks:

- Security of financial transaction
- Proper integration with local case management system
- Proper business rules checking to ensure filings meet rules and standards

Dependencies

This functionality is dependent on:

- The OCN offering electronic filing
- The local court allowing electronic filing
- A financial relationship with a credit card processing provider with competitively negotiated rates
- A well-formed privacy policy and statement that provides the attorney with assurance that their privacy is protected during and after the transaction
- A secure, encrypted means of processing the transaction
- An efficient and accurate means of transferring the electronic filing and payment information into the local case management system
- A system which handles the money being properly *ACH*d to the appropriate local bank account
- A system to provide checks and balances to ensure that all transactions and filings are accounted for and have passed through the *portal-dashboard* and to the appropriate local court

Success Measures

If the *portal-dashboard* is able to successfully offer the agreed upon transactions for electronic filing, the service is utilized by attorneys with some measure of frequency, and the system successfully transfers the filing information and money to the local court, it can be considered successful.

Priority Scale (1=Must Have; 2=Should Have; 3=Would Like to Have)
1 - Must Have

Inter-Agency Disbursements

Definition

To allow for the electronic transferring of inter-agency disbursements

Business Drivers

- Courts and clerks are required to file reports and disburse money collected to a variety of local, county and state entities
- Reporting and payment by electronic means provides an added measure of efficiency to the process

Use Case

Clerks' offices have a requirement to file reports and disburse money collected. Electronic agency disbursements will only address this business need if there is seamless integration between the systems of the local court and the participating agency.

Implications

Possible Efficiencies:

- Reduce clerk's data entry time
- Shorten the length of time it takes agencies to receive these reports and disbursements

Possible Risks:

- Security of financial transactions
- Proper integration with local and agency case management systems
- Rules in place at the local, county, and state level that would allow for this type of transfer of funds

Dependencies

This functionality is dependent on:

- Local, county and state agency support
- Local, county and state agencies having rules and policies in place to allow for receiving electronic reporting and disbursements
- Any reporting which accompanies disbursements would need to be transmitted electronically as well

- A financial relationship with a credit card processing provider with competitively negotiated rates
- A secure, encrypted means of processing the transaction
- An efficient and accurate means of processing the electronic disbursement information through the local, county and state case management systems
- A system which handles the money being properly *ACH*d to the appropriate local bank account
- A system to provide checks and balances to ensure that all transactions and reporting are accounted for and have passed through the *portal-dashboard* and to the appropriate local court

Success Measures

If the *portal-dashboard* is able to successfully identify agencies willing to accept electronic reporting and disbursements and establish a procedure for doing so, the service is utilized by those courts and agencies, and the system successfully transfers the reports and money from the local court to the agencies who agree to participate, then it is successful.

Priority Scale (1=Must Have; 2=Should Have; 3=Would Like to Have)
3 – Would Like to Have

Costs and Fines (Party Related)

Definition

To allow for the electronic payment of party-related transactions

Business Drivers

- Parties are required to pay fines, court costs and fees
- Courts and clerks are required to collect and disburse those payments
- Payment by electronic means provides an added measure of convenience and efficiency to the process

Use Case

Parties have a requirement to make these payments. By allowing them to make these payments electronically, we improve the prospect of compliance by making compliance less painful for the defendant.

Clerks' offices have a requirement to collect and disburse these payments. Electronic payments will only address this business need if there is a method available to import electronic transactions directly into the local court case management system.

Implications

Possible Efficiencies:

- Reduced data entry time
- Increased collection rate
- Improved customer service

Possible Risks:

- Security of financial transactions
- Proper integration with local case management system is necessary to avoid inappropriate action being taken for perceived non-payment
- Business rules must be built into the payment system so that only a certain sub-set of offenses are payable online.

Dependencies

This functionality is dependent on:

- A financial relationship with a credit card processing provider with competitively negotiated rates
- Well-defined business rules which allow for only certain types of cases to paid electronically
- A well-formed privacy policy and statement that provides the defendant with assurance that their privacy is protected during and after the transaction
- A secure, encrypted means of processing the transaction
- An efficient and accurate means of transferring the electronic payment information into the local case management system
- A system which handles the money being properly *ACH*d to the appropriate local bank account
- A system to provide checks and balances to ensure that all transactions are accounted for and have passed through the *portal-dashboard* and to the appropriate local court
- During site assessment, local courts must provide a costs and fines schedule (see General Information)

Disclaimer/Assumption: Any monies collected by OCN are based on the most current version of local court fee schedule. This could be established by rule.

Success Measures

If the *portal-dashboard* is able to successfully offer the agreed upon transactions for payment to the defendant, the service is utilized by the defendant with some measure of frequency, and the system successfully transfers the transaction information and money to the local court, then it is successful.

Priority Scale (1=Must Have; 2=Should Have; 3=Would Like to Have)
1 - Must Have

Application: Authentication

Definition

Authenticate citizens, practitioners, court personnel, and other authorized entities for future access to the OCN.

Business Drivers

To offer appropriate services, each user group will require some means of authentication.

Public Users:

- No authentication will be required for basic use.
- Customization of public content is optional.
- With customization, user ID, password, and password reminder are required
- Providing e-mail for password reset is optional

Practitioners: Authentication required

- User ID and password will be required
- Password reminder function will be required
- Heightened authentication may be required for attorney-specific functions
- Confirmation letter will be sent to the home address of the applicant when account is created or changed.

Court Personnel: Authentication required

- User ID and password will be required
- Password reminder function will be required
- Passwords will have expiration dates and users will be prompted by the system to change them at a regular interval, such as quarterly.

Implications

- Risk of unauthorized use by "hackers" or disgruntled employees.
- Users wishing to use the customization features must allow *cookies* on their computers.

Relationships

Authorized users will be allowed access to additional types of information. They will also be able to set up a "My OCN," and have access to various reporting functions.

Functional Requirements

Allowing opt-in placement on login screen of "*cookies*" on users system will expedite repeat users' logging process.

If a user opts-in to customization, then they create a username, password, and password hint. They can choose to give their e-mail address if they wish to have password recovery/reset. If the password is lost, the ability to recover customized account information is contingent on the user knowing the password hint or supplying a valid e-mail address during account creation.

There will be a greater likelihood that a customization user's behavior can remain anonymous, and there will not be any tracking of activity.

Priority Scale (1=Must Have; 2=Should Have; 3=Would Like to Have)
1=Must Have

Success Measures

- System will authenticate the user within the OCN, and track their login date and time.
- Low incidence of users resetting passwords.
- Low incidence of unauthorized access.

Application: Interaction/Communication

Definition

Provide a way to allow the *portal-dashboard* to more adequately meet the individual needs of the stakeholders and reach the user in various informative and unique ways.

Business Drivers

Stakeholders have a need to be kept informed of various data that the *portal-dashboard* tracks. It is not always practical for the user to navigate and/or visit the *portal-dashboard* for updates. If the *portal-dashboard* can provide updates and notifications then it becomes a much more valuable tool to the users. All notifications will be opt-in.

Implications

This type of functionality increases the complexity of the *portal-dashboard*. Interaction and customization will allow the *portal-dashboard* to be more useful and better meet the needs of the individual user. However, what communications devices and methods of notification will be supported must be determined.

Functional Requirements

Necessary notifications:

- Press releases
- Usage statistics
- Training opportunities
- System outages/upgrades/messages
- Court calendar (docket changes)
- Court cancellations or emergencies
- Text of docket entry (case tracking)
- Continuing Legal Education (CLE) notifications/opportunities/transcripts
- Bar registration deadlines/expiration

Download calendar and special alerts:

- To Outlook and/or Palm *OS*
- Email attached appointments to subscribers; link automatically adds appointment to calendar.

Message medium:

- *RSS Feed*
- Mobile communication (cellular phone, handheld device, pager, etc.)

Priority Scale (1=Must Have; 2=Should Have; 3=Would Like to Have)
2 = Should have

Success Measures

These types of interactive tools will require registration to use. A review of the number of registrations and the various tools that have been set up should provide a gauge as to how successful this has been.

Application: Geographic Mapping

Definition

- Geographic mapping provides the ability to localize data into a familiar format.
- The *solution* displays information in a geographic format so stakeholders can use it for analysis.

Process

- The user requests the information to be reported and the coordinates required (i.e. street addresses, zip codes, etc.)
- Based on the user's profile and security level, data is reformatted (presented) in the requesting court's format (i.e. map, graph, chart, etc.)
- Results can be displayed on the *portal-dashboard* or in a report format

Business Drivers

Geographic mapping is a tool to aid stakeholders in accessing the "big picture" and making informed decisions about funding, services, trends, and needs. When combined with *OLAP*, geographic mapping helps provide "*business intelligence*" to the stakeholders and other state or local agencies. For example, the OCN could track Domestic Violence (DV) cases through the courts by county, zip code or census tract. This information could be used by law enforcement agencies as will as social service agencies to identify areas in the state that need the most funding to deal with this issue.

Implications

Geographic mapping is dependant on address data accuracy and the *data cleansing* process. Incorrect zip codes, misspelled street and town names, missing or inaccurate address numbers will cause inaccuracies in the maps.

Relationships

- Data Dictionary
- OCN's *OLAP* cube.
- Interfaces with *portal-dashboard*

Dependencies

- *Data Warehouse*
- *OLAP* tool
- Querying Tool
- *Portal-dashboard*
- User Profile

Technology Requirements

Solution should be:

- Easy to learn and easy to use
- Able to display results in a format that best meets the users' needs.
- Able to provide access to outside data sources like census data.
- Able to display charts within a map.
- Web compatible

When/How often does it occur?

As needed

Priority Scale

3=would like to have

Success Measures

Success can be measured by how much the tool is used. If it is easy to use and provides the output in formats the users want, it will be used more frequently.

Application: Help

The Ohio Courts Network is designed to link the Ohio courts to the portal through a web browser connected to the internet. The public also requires an easy way to navigate through the amassed amount of court information. Many volunteers have worked to give court information users a centralized site to interact with Ohio courts twenty-four hours a day, seven days a week from home or place of business. These users, for whom the portal is designed, can utilize the feedback function to provide the OCN with their comments. The OCN will constantly strive to provide the best service to the public. One way for OCN users to learn more about the opportunities the portal has to offer will be to select a link on the home page for a tour and quick guide to the portal.

The help functions included in the portal design are expected to provide the public with the means to select and receive portal assistance in a *timely* manner.

The proposed help selections available are:

- Self help, including tutorials and guides, which would be designed to facilitate citizen interaction with the courts for specific functions.
- Portal help, such as a tour of the features of the portal
- OCN help, such as linking to the appropriate court web page
- Help for related content, linking to the selected content for the desired information
- Help finding case information
- Frequently Asked Questions (FAQs)
- Feedback
- Technical help
- Profile help

The help function may be accessed by computer, telephone, cellular phone, mobile device, and fax machine. The public can select which method of help they desire by selecting from a predefined menu.

The following requirements identify the process, business drivers, implications, technology requirements, relationships to other parts of the application, and success measures for each of the major components of the reporting process.

Definition

The help functions submitted in the portal design are expected to provide the public and other user groups with the means to select and receive content and technical assistance in a *timely* manner.

Business Drivers

There will be a need for content-based, technical and navigational assistance to the users of the OCN portal. OCN users would be able to select the method of help they desire by using a predefined menu found on the portal interface.

Implications

Any website that expects a large number of users and to make complex data and software tools available to those users must provide for a considerable help desk system to guide customers through the site. For instance, the public could become intimidated and frustrated if the information they are seeking is not readily available or easy to locate, or if the site continually goes down.

Functional Requirements

- The help function must have the capacity for an unlimited number of hyperlinked help pages
- The help function must include the ability to submit questions to and receive answers from ("chat" with) live help-desk operators
- The help function must provide users with the ability to submit feedback
- The help function must provide users with the ability to access FAQs
- The help function must provide users with the ability to receive live support over the phone by calling a help-desk operator (not necessarily 24/7)

Relationships

While the portal will provide an interface to the help desk, Critical Applications, Network, and Security will inform the more technical and system-related aspects of the help function while Governance and Privacy will provide policy guidance on the limits of the help desk as well as what information and tools are available to each user group.

Priority Scale (1=Must Have; 2=Should Have; 3=Would Like to Have)
1 – Must Have

Success Measures

- Widespread adoption and use of the portal by public and governmental user groups.
- Fewer help related email and calls to the OCN customer service staff.

Self Help

Definition

The purpose of the self help subfunction is to enable the OCN user to locate their information by entering keywords. A feature of self help would allow the user to select an item from a drop down menu to access the help tutorial, guides, help for case types, glossary and terms and create a help wizard for self-assistance.

Business Drivers

Many questions may need to be addressed from users of the OCN portal. Self help should be designed to reduce the frustration of users who seek assistance for access to court related information. The assistance should provide quick and accurate responses.

Implications

Self help should reduce the volume of email and calls to the customer support staff. However, providing limited or no assistance would risk non-use of the OCN and/or increased calls to the staff.

Success Measures

- Fewer help related email and calls to the OCN customer service staff.
- Self help should provide the user with opportunity to rate the effectiveness of the answer.

FAQs

Definition

The purpose of FAQs is to enable the OCN user to access Frequently Asked Questions about the OCN and court related information by selecting a hyperlink. This is necessarily a sub-part of the self help section.

Business Drivers

Many questions will need to be addressed from users of the OCN portal. FAQs should be designed to reduce the frustration by users who seek assistance accessing court related information. The assistance should provide quick and accurate responses.

Implications

A successful FAQ should reduce the volume of email and calls to the customer support staff. Limited or no FAQs would risk non-use of the OCN and increase calls to the staff.

Success Measures

- Fewer help related email and calls to the OCN customer service staff.
- FAQs should provide the user with opportunity to rate the effectiveness of the answer.

Feedback

Definition

The purpose of this subfunction is to provide the OCN user with a means to communicate their feedback to the customer support staff. The OCN staff may receive e-mail or phone calls from OCN users about what is working well and some of the issues the support staff should be addressing. Problem tracking and follow up with the users are important tasks for measuring the success of the network.

Business Drivers

It is important for the OCN staff to be responsive to feedback in a *timely* manner. New ideas for improvement may be gleaned from the users' feedback.

Implications

The OCN portal is being developed for the public convenience. It is important to receive input and feedback from those who will be using the network.

Priority Scale (1=Must Have; 2=Should Have; 3=Would Like to Have)
2 – Should Have

Success Measures

Monitoring customer response to the OCN through the use of feedback may reduce the number of e-mails and calls to the OCN customer support staff. The feedback could be compiled by the OCN staff and categorized by issues, improvements and other related information.

Technical Help

Definition

The purpose of the technical help subfunction is to provide the OCN user with a means to request and receive assistance for OCN technically related issues from the customer support staff. The assistance would need to be logged, monitored and facilitated through several automated applications as well as human support staff.

Business Drivers

The OCN users may encounter a slow network connection or response, browser navigation problems or experience other technical issues.

Implications

The customer support staff could provide assistance via e-mail, telephone or other digital means of communication such as Personal Digital Assistants (PDAs).

Success Measures

Many users are not technically proficient and may require assistance. Initially, there may be a flurry of technical requests for assistance. The portal should include in the design hyperlinks to technical FAQs and tools such as browser upgrades and shareware to help the users through technical issues.

Profile Help

Definition

The purpose of the profile help subfunction is to provide the OCN user with a means to request and receive automated assistance for OCN login issues through the OCN portal. The assistance would need to be logged, monitored and facilitated through several automated applications as well as human support staff.

Business Drivers

The OCN users may forget their login IDs or passwords and require e-mail or telephone assistance from the customer support staff if an automated process designed in the OCN portal does not resolve the problem.

Implications

The customer support staff could provide assistance via e-mail, telephone or other digital means of communication such as PDAs.

Success Measures

Initially, users may require login ID or password assistance. The *portal-dashboard* should include a process for the users to request a new password based on their security profile/access. If a user forgets their ID, they will need to create a new one. There should be considerations in the design to perform periodic profile maintenance based on inactivity (i.e. user was not logged in for 365 days).

Reporting of Data to Authorized Users

Reporting Executive Summary

Judges, clerks, court administrators, and other justice personnel need accurate and *timely* data to be able to make decisions quickly and intelligently. The OCN *data repository* will provide a vast amount of data about court proceedings and activities collected from the various courts throughout the state. Now information will be able to be shared across the boundaries of organizations and jurisdictions while ensuring that the privacy and security of sensitive data is upheld. In order to facilitate this information sharing; justice personnel will need tools to assist them in accessing, analyzing and manipulating this data.

The reporting function of the OCN will provide the methods to extract, analyze, and report on the data stored in the *data repository*. State, county, local, and federal reports can be produced in a standard format thus lowering the reporting costs for local courts and improving the overall timeliness and accuracy of these reports. Sophisticated data analysis tools will be available for data analysis. Data will be filtered and extracted based on user-specified criteria providing results tailored to individual needs. The ability to respond more effectively to media requests about the judicial branch as a whole will be greatly enhanced. Court personnel will be able to organize and view data over time so trends can be established. These views will not be limited to just paper reports or screen displays. Data visualization technologies will render large quantities of data in the form of basic charts, graphical indicators, *scorecards*, *portal-dashboards*, and animations giving judicial personnel many ways to visualize and analyze information.

There are essentially three means for reporting:

1. Standardized Reports (covered later in this section – “Application: Standardized Reporting”).
    a. Predefined and preformatted.
    b. Statutory or Agency required.
    c. Pre-run and available in most cases without need to wait for processing.
2. Queries (also covered later in this section – “Application: Querying”).
    a. Formatted within a predefined superset of available formats.
    b. User selected data elements as well as constraints and criteria.
    c. For use at the local or agency level.
    d. Usually run at request time.
    e. Some queries will evolve into a menu of “standardized queries” – reports that are not required statutorily nor by agencies but that have broad general appeal and frequency of request.
3. Ad Hoc Reports (covered in the “Presentation of Data to Authorized Users” section – “Application: Search And Find”).
    a. Larger/more complex and/or highly specialized.
    b. Developed with the assistance of OCN technical staff.
    c. May develop into standardized queries if the interest is believed to be broad enough.

Application: Business Intelligence

This section covers development tools for each of the reporting means.

Process

- Report format will be modified based on user profile to fit local requirements.
- Government reports will match current government guidelines for content and format.

Business Drivers

- All reports produced will adhere to federal, state (Supreme Court) and local standards for format and content according to all statutes and rules.
- The *solution* must support users requiring ad hoc database query, reporting and basic *OLAP* analysis. Priority = 1
- The *solution* must provide report design functionality. Priority = 1
- The *solution* must support "information democracy," or the spread of BI tools to all types of potential users in an *enterprise* (*Enterprise* *Business Intelligence* Systems (*EBIS*s) support all levels of user skills). Priority = 3

EBIS Portal-Dashboard

The *solution* must include a portal-like front end to the *EBIS* (a.k.a. portal) because the web-enabled versions of the *EBIS* provide a web entry point into court data. BI portals also should provide support for linkages to unstructured information. Priority = 1

Collaborative BI

The *solution* must allow adding annotations to reports and sharing analyses with other users as well as work-flow capabilities. Priority = 2

Improved thin-client capabilities

The *solution* must include report design capabilities to thin-client web tools; as well as support for robust *OLAP* functionality. Priority = 2

Web Services

EBIS may deliver its technology as web services.

Linking BI and information from text documents

The *solution* may include text-mining technology that primarily enables the correlation of textual information with quantitative data. Priority = 3

Technology Requirements

- BI Platforms Priority = 3

- Characteristics of a BI platform must include a modular distributed architecture, supporting relevant standards like *XML* and OLE DB for *OLAP* and providing total web deployment.
- It must be open and extensible so that third parties are encouraged to and can easily add functionality.
- The vendor must provide a strong third-party support program.
- Of course, the product must have comprehensive BI functionality.

- Modern Platform Architecture
  - The BI platform must provide support for modularity (for example, components) and an accepted distributed computing model.
- Third-Party Extensibility
  - The BI platform must provide the capability to add significant new functionality without fundamentally altering the core BI platform with a useful and well-documented set of *API*s.
- Vendor Support Programs
  - The BI platform vendor must support the creation, promotion and advocacy of third-party extensions and product offerings, when possible.
- BI Features
  - The BI platform must provide BI-specific functionality, such as database access capabilities (like *SQL*), multidimensional (*OLAP*) data manipulation, modeling functions (such as what-if analysis), statistical analysis and graphical presentation of results (such as charting). Priority = 2
- The *solution* must include parameter-driven reports or, at the highest level, by ad hoc queries and *OLAP*. Standard reporting requirements call for pre-defined reports run against the most recent available data. End users will have the ability (provided by the report developers) to provide parameters at runtime to tailor the information in their reports. Capabilities include web-client report design. Priority = 2
- Controlled Reporting Environment Priority = 1
  - Allows end users to graphically access create and distribute reports.
  - Gives users the ability to run standard reports, parameter-driven reports, ad hoc reports and *OLAP*-enabled reports from any web browser.
- BI *portal-dashboard* is HTML-based and allows users to create a customized user interface for access to the reporting and BI tools.
- The application set leverages data resources from repositories, including relational databases).
- The development toolset is platform independent and integrated with *OLAP* services for dynamically generating information using cube data; pivot tables; and many documents in a variety of formats, including *XML*, HTML, *Common Gateway Interface* (*CGI*), and PDF for display in web browsers or for use with desktop applications. Priority = 3
- The *solution* must include cube data compression, partial data aggregation with on-the-fly aggregation and partitioning. Priority = 3

- The *solution* supports parallel processing and load distribution through cube partitioning, parallel querying against partitioned cubes, as well as wizards to help determine how to trade off storage considerations for performance. Priority = 3
- The *solution* offers automated procedures that handle data manipulation, information storage and retrieval, descriptive analysis and report writing. Priority = 1
- The *solution* includes query and reporting. Priority = 1
- The *solution* includes *OLAP*, *enterprise* information systems development, data mining, data analysis, data visualization and application development interfaces. Priority = 3
- Users can employ analytical tools and view the results over the web. Priority = 2
- The *solution* provides an integrated query, reporting and analysis environment that provides access to analytic functionality and other capabilities without programming. Priority = 3
- Reports for the OCN should be standardized.

Application: Querying

Definition

Querying allows users to develop data extractions from the *data repository* for analysis and reporting.

Process

- Data elements are displayed to the user based on the security level in the user profile
- The user selects data elements (based on constraints/criteria) to appear on the report, sequence of data, level of detail, etc.
- The report is produced as a hard copy or on screen
- If the user desires, the report can be converted to a regularly scheduled report (production basis)
- All reporting templates will be modifiable and downloadable at the local level into *XML* or comma delimited
- The user should be able to add and delete fields from templates at the local level
- The user interface must be point and click (Graphical User Interface [GUI])

Business Drivers

- Stakeholders need an easy way to manipulate data for purposes of data analysis and reporting.
- The OCN needs a quick method of providing information to non-stakeholders.
- Many reports will be dependent on queries.
- Information must be transferred between the courts and the state.

Technology Requirements

- The *solution* must have a non-technical environment which is menu driven (user chooses from list of fields, etc.) Priority = 1
- The *solution* must include *OLAP* computer processing that enables a user to easily and selectively extract and view data from different points-of-view. Priority = 3

Application: Standardized Reporting

Definition

As the data storage component of the Ohio Courts Network, the *data repository* must be designed in a manner to perform many functions. One of these functions will be reporting. Please note that requirements for ad hoc queries are located in a separate section. All reports produced will adhere to either a local or state level standard format if applicable.

Reporting will encompass any activity that gathers existing data in the repository and presents it as any output other than online query response. Reporting may be in the form of traditional paper reports, standardized forms, or electronic data for transmission as a replacement of standardized and required reports, to include *transactional reporting*.

Process

Users will select from the list of available standardized reports. The repository will support reporting functions in the following ways:

- Data must be reportable in summary or detail by the following categories, when available:
    - All Courts;
    - Specified Court Type i.e. Municipal or Domestic Relations;
    - County;
    - Individual Court;
    - Individual Judge;
    - Specified Case Type i.e. Traffic;
    - Specified Case;
    - Specified Party;
    - Specified Attorney;
    - Geographic Locations;
    - Political Subdivision, i.e. school district, village, township, etc.;
    - Key Case Processing Dates and Date Ranges;
    - Charges, including level and original/amended/reduced charges, arresting agency, categories of charges;
    - Dispositions;
    - Sentencing.
- Data must be stored in such a way that it can be reported in aggregate or summary report formats.
- Aggregate reports must have an option to be generated with supporting detail.
- Transaction reporting must be available in a sight readable format as supporting information for individual transactions.
- There will be *security layers* of standardized reporting
- There will be federal, state, county, and local standardized reports

- Government reports will match current government guidelines for content and format.
- All output must be modifiable and downloadable at the local level.

Business Drivers

- Achieve accurate, *timely*, and consistent reporting across all courts for fulfilling standardized reporting requirements.
- Coordinate changes in reporting requirements, minimizing the impact of system changes at the local level. Standardized reports are needed to pull data out of the OCN for decision making purposes.
- Standardized reports will…
  - Help other agencies (state, local, municipal) capture information they need to send to other agencies for funding or review processes.
  - Lower reporting costs for local courts
  - Provide the *agility* to respond to changes in reporting requirements without necessitating changes at the local level
  - Ensure reports are submitted accurately and *timely*
  - Provide additional capability for *data cleansing*
  - Include multiple venue and comparative information
  - Allow us to respond more effectively to political, education and media queries about the judicial branch as a whole (i.e. Issue 1, 2002)

Risks

- Unattended submission of required reports could result in incomplete and/or inaccurate reporting.
- Need for standardized vocabulary or classification of changes linked to local ordinance codes (Ohio Revised Code [ORC] covers most).
- Data may not be available, *timely*, consistent, complete, or accurate.

Dependencies

- Define security profiles to support the availability of the necessary reports, in the authorized technical format, to the appropriate users.
- Develop an approval process (governance, policy, etc.) for the gallery of standardized reports available.
- *ETL*
- Network
- *Data Repository*

Technology Requirements

- Reports must be available in a normalized data format suitable to be imported into another application. Examples include ASCII delimited, *XML*, comma delimited, .xls.

- Reports must be available in a read-only format such as PDF.
- The ability to generate standardized reports on an unattended, defined schedule and transmit them to a defined location(s)/user group is required.
- The ability to generate standardized reports on demand is required.
- Report parameters or filtering options are clearly available and displayed along with the date generated.
- The end user must have the option for approval of reports prior to the reports being finalized.
- The availability of graphical display of reports (charts, maps, graphs, etc.) is required.

Functionality Requirements

- Rapidly build, manage and deploy reports for real-time use.
- Support industry standards such as *XML*, .net, *java*, and web services.
- Ability to prioritize requests.
- Notification to end user of report completion or availability.
- Protect sensitive court information through a secure reporting environment.
- Automatically schedule reports for *timely* delivery to requestors.
- Empower end users with report viewing, printing, and exporting without Information Technology (IT) assistance.
- Drag and drop user interface to shorten the development process and eliminate the requirement for coding.
- Reports for the OCN should be standardized. (i.e. PDF, *XML*, HTML, Plain Text).
- Product enables the integration of hyperlink drill-downs to any other report, program, location, or multiple locations within *enterprise* reports. These hyperlink drill-downs are available in all support output formats, including HTML, Excel and PDF. Drill-down is possible from any report to any other report while remaining in context.
- Provides compound reporting capabilities for merging multiple reports into a single document.
- On-demand paging to enable simple and enhanced navigation through long reports.
- Automated creation of a table of contents within reports to enhance readability.
- Navigation and report viewing to help users go directly to relevant report information.
- Should securely manage and administer broad deployment of information to unlimited numbers of users within and outside the OCN.
- Provide a complete environment for management and administration facilities, enabling the OCN to build and deploy standard reports, provide ad hoc and *OLAP* capabilities to specified users, monitor usage, assign user groups, define access rights, schedule distribution, provide event-driven alerts and ensure security.
- Triggered alerts, notifications and exception-based reports.
- Software supports creation of static and dynamic reporting

- Versioning of static reports.
- Multiple sorts and subtotals within report.
- Capability to remotely review, correct and approve (for local courts) data in standardized and required reports prior to publication. Prelist reporting capabilities for published and required reports.
- The *solution* should have graphing/charting capabilities.

When/How often does it occur?

As needed

Priority Scale

1=Must Have

Portfolio, Program and Project Management

Application: Planning / Managing

Application Users: Technical and Business

Dependencies –
Operations

Technology Requirements –

- *Program Management* capabilities must be available
- *Issue Tracking* capabilities must be available

Priority Scale -
1=Must have.

Success Measures –

- An efficient, comprehensive project roll-out will be an indication of success.

Collaboration Executive Summary

Collaboration is defined as email and other types of software commonly referred to as *Groupware*. *Groupware* is a technology designed to facilitate the work of groups where the participants are in different and sometimes remote places. The group activities may take place at the same time or different times.
Some examples of collaborative software are:

- Email
- News groups and mailing lists
- *Workflow systems*
- *Hypertext* allowing authors to link text documents to each other
- Group calendars
- Shared *whiteboards*
- Video communications
- Chat systems
- *Decision support systems*

Collaboration:

- facilitates communication, making it faster, clearer, more persuasive
- enables communication where it would not otherwise be possible
- enables telecommuting
- cuts down on travel costs
- brings together multiple perspectives and expertise
- provides the ability to form groups with common interests where it would not be possible to gather a sufficient number of people face-to-face
- saves time and cost in coordinating group work
- facilitates group problem-solving

Collaboration will enable and should encourage statewide participation in projects of mutual interest. It is made possible by a high speed Ohio Courts Network.[3]

[3] Ideas taken from *http://www.usabilityfirst.com/groupware/intro.txl*

Application: Mail Transfer Agent

Definition –
(From *whatis.com*) A mail server (also known as a *mail transfer agent* or MTA, a mail transport agent, a mail router or an Internet mailer) is an application that receives incoming email from local users (people within the same domain) and remote senders and forwards outgoing e-mail for delivery. A computer dedicated to running such applications is also called a mail server.

The mail server works in conjunction with other programs to make up what is sometimes referred to as a *messaging system*. A *messaging system* includes all the applications necessary to keep email moving as it should. When you send an email message, your email program forwards the message to your mail server, which in turn forwards it either to another mail server or to a holding area on the same server called a message store to, be forwarded later. As a rule, the system uses *SMTP* (Simple Mail Transfer Protocol) or *ESMTP* (extended *SMTP*) for sending email, and either *POP3* (Post Office Protocol 3) or *IMAP* (Internet Message Access Protocol) for receiving email.

Note: Common email server application suites typically include other *groupware* and Customer Relationship Management (*CRM*) features such as calendaring, scheduling, *contact management* (address books), meeting planning and even information resource sharing.

Process –
The network and client operating system will be installed first to establish the OCN Information System infrastructure/environment. The email application with then be installed/configured to establish the email and collaboration infrastructure for internal OCN users, and potentially those with external access rights.

Business Drivers –
The OCN *enterprise* requires a locally based email environment in which local users can:

- Send and receive email, either inside the system or via the web (*extranet*)
- Schedule events and appointments, and share resource availability information
- Set up reminders and alerts for meetings and "flagged" items
- Plan and facilitate meetings with connected recipients

Implications –
The *solution* must provide a secure, *scalable* and robust email **-** *groupware* system for OCN staff and authorized external users.

However, there are few options in the *enterprise* messaging/*groupware* marketplace, each with their own strengths and shortfalls

Relationships –

- Directory integration: typically authentication for the email system is integrated with the existing network account directory, many of which support *LDAP*.
- Integration with the *portal-dashboard* application

Dependencies –

- The *NOS/OS* precedes all other application considerations
- It is assumed that the physical network infrastructure, server hardware, and client computer hardware are in place prior to installation and configuration of the *NOS/OS*
- There must be an existing account directory environment
- Internet access is required for collaboration
- Appropriate security infrastructure must be in place (*firewall*, DeMilitarized Zone (*DMZ*), etc.)
- The *DNS* must be registered and appropriate Mail Exchange Record (*MX*) host records defined
- Anti-virus, *spam* and *spyware* platforms must be confirmed, acquired and ready for deployment

Technology Requirements –

- The *solution* must have industry leading technical support and training
- The *solution* must have "*zero administration*" capabilities (automation, scripting and scheduling support)
- The *solution* must have broad compatibility/interoperability with applications, utilities and vendors; *API* support for backup vendors, fax, anti-virus and anti-*spam* systems
- The *solution* must have *minimal* proprietary components or dependencies
- The *solution* must include *extranet* features and *browser-based* access
- The *solution* must include broad protocol support (*TCP-IP*, *SMTP*, *POP3*, *LDAP*, Internet Protocol Version 6 (*IPv6*), Multipurpose Internet Mail Extensions (*MIME*), Secure MIME (*S/MIME*), *IMAP*, *FTP*, Network News Transport Protocol (*NNTP*), etc.)
- The *solution* must include industry leading security and auditing provisions
- The *solution* must include directory and account management services
- The *solution* must have policies for quickly changing a wide range of objects such as mailboxes
- The *solution* must have robust client logging and error reporting tools for faster problem resolution
- The *solution* must include *virtual memory* usage and monitoring
- The *solution* must include a robust application development platform
- The *solution* must include broad *DBMS* and *web server* support and integration
- The *solution* must be highly available and maximize server availability with *clustering*, *transaction logging*, *server fault recovery*, and automated diagnostic tools
- The *solution* must include archiving features for email and data assets
- The *solution* must include *compression support*

- The *solution* must include server-based message *rule processing*
- The *solution* must include built in *Instant Messaging* and *NNTP*
- The *solution* must include data sharing (delegate or proxy access)
- The *solution* must include capacity for *document management* features
- The *solution* must include capacity for *workflow management* features such as notifications
- The *solution* must include capacity for *message board* features

Priority Scale

1=Must Have

Governance and Policy

Service Level Management

Administration Executive Summary

Maintaining consistently high levels of service will be a priority of the OCN. Users of the system will expect data that they need, when they need it. They will expect consistency in performance and *timely* repair of defects, as well as technical help when they experience problems or need answers to questions. Solid administration is needed to maintain user expectations.

Administrative requirements of the OCN will be enormous in scope and will mandate a wide variety of applications and resources to ensure the availability, functionality and security of OCN products and services to users and staff. The OCN's primary administration applications will best be administered by the selection of specific products that organize, maintain, monitor, alert and manage the OCN.

The Critical Applications Work Group has defined the primary administration applications needed as:

- Administration
- *Enterprise* access management
- Monitoring
- Planning & Managing
- Securing

OCN users (internal and external personnel from the public and private sectors) will need a broad range of functionality from simple queries to sophisticated data transfers. Administration applications and *enterprise* access tools are designed to allow administrators to develop and implement the policies and access levels required in large installations. Internal personnel will install, implement and maintain various equipment and applications of the system. External users (judges, clerks, court administrators, lawyers, investigative services and the general public) will be accessing the OCN data. Monitoring and maintaining the security rights for these users will be administered by the applications acquired.

OCN administrators will monitor security and critical resources including servers, software, *firmware*, infrastructure, power management facilities and others.

Planning and managing will require applications to assist with organization and implementation of major projects, programs, upgrades, updates and subscriptions as required by the OCN. The applications will also aid financial planning, *capacity planning* and monitoring, forecasting, *issue tracking* and reporting, and *resource management*.

General Administration Requirements

- The OCN requires acquisition and implementation of goods & services from vendors and/or *project management* teams.

- Prior to implementation:
    - Processes, business rules and policies must be in place to ensure effectiveness of monitoring and auditing tools.
    - Standards and IT policies will be documented
    - A *test environment* mirroring the *production environment* will be created. This will protect the *production environment* from failures and performance problems introduced by changes to applications (including database versions and operating systems). Every change will be tested by the requestor and approved by signature before being migrated to the *production environment*. Test scripts will be created to ensure that changes do not impact functions that used to work correctly. The *test environment* will be resynchronized from the *production environment* regularly.
    - Compliance control and policy enforcement must be in place to protect against unauthorized access and change.
- System Requirements:
    - Consideration of budgeting and financial responsibilities (including forecasting and modeling) as well as financial and personnel *resource management*.
    - *Project management*, including project modeling, estimating, accounting, *Gantt chart* creation, time tracking, etc.
    - Ability to troubleshoot user problems and provide additional helpful information about access errors.
    - *Patch management*
    - Network scans to discover all network devices and groups and define dependencies.
    - Recovery initiation (restart apps/reboot devices/abort function/etc.
    - *Escalation* support – internal or third party support notification.
    - Integration with other *enterprise* monitoring *solutions*.
    - The ability to test multiple requirements – i.e. HIPAA compliance, server health, common server applications, mail services, dynamic web applications and Simple Network Management Protocol (SNMP) enabled quipment.
    - The ability to secure contractor accounts.
    - Examples of tracking required:
        - Accounts with blank passwords
        - Those that have expired
        - Those who have administration rights on domains and servers
        - Those who have breached security policy
        - Changes to key security groups
        - Sensitive file access (how often, who, when, unsuccessful attempts)
        - Late night accesses
    - Enforce standards and IT policies

  - To assist help desk personnel, a searchable knowledge base will be maintained. This will contain answers for previously problems and fixes as well as frequently asked questions.
- Applications
  - Will require *enterprise*-wide *contract management*.
  - Must provide *enterprise* reporting (automated monitoring, detail and summary, roll up (*Portal-dashboard*/network/apps/facilities), *issue tracking*, scheduling, defect tracking, *configuration management*, *revision control*.
  - Must provide metrics (*enterprise score carding*)
  - Must protect the configuration (administrative security) as well as tracking which users are viewing, adding or changing what information when, and must enforce rules that will minimize security risks.
  - Must provide standards and policy enforcement capability, including checking of permissions on sensitive files.

Application: Administrating

Process –

- The OCN will determine applications, contracts, etc. to be managed, and develop a plan to manage specific aspects.
- The applications will be configured, tested, and implemented

Risks

- Non-Interaction with other application managing packages will limit functionality

Relationships –

- OCN Staff
- Support agencies (telcos/3rd party support/etc.)
- *Monitoring Applications*

Dependencies –

- PMO/operations-critical dependency
- OCN Users
- Support agencies

Priority Scale –
1=Must have.

Success Measures –

- Implementation of projects and new roll-outs is *timely*
- The help desk *SLA* is in place

Application: Enterprise Access Management

Risks

- Users are improperly authorized to use applications
- The software could be functional for some but not all applications

Relationships

- Network/Security
- Governance
- OCN internal/external users, third party support

Dependencies

- Administrators
- OCN users
- Security and Network Architecture

Priority Scale **-**
1=Must have.

Application: Monitoring

Implications

- Efficiencies:
  - Monitoring can provide network and applications viability
- Risks:
  - Monitoring could bog-down system resources

Dependencies

- OCN staff operations
- OCN users

Technology Requirements –
Technologies used for *enterprise* systems monitoring include:

- Threshold level monitors
- Agent-based and agent-less
- *Monitoring maps*

Priority Scale -
1=Must have.

Success Measures

- Thresholds must not be breached (capacity/equipment/licenses/etc)

Support

Executive Summary

The successful operation of the OCN repository requires a variety of hardware, software and personnel services. The purpose of this section is to describe a minimum level of expected performance so that management, staff, vendors, and client courts know what to expect of the system.

The Help Desk/*Call Center* (HD/CC) will provide front-line support for the OCN to courts, external agencies, and the public.. Experienced personnel with superior communications skills will be vital to the success of the Help Desk. To maintain the high-quality service level OCN will provide,, tools will be needed to monitor hardware and software, identify and correct problems quickly, and alert customers as to the time they can expect system availability. The tools will also provide timely, proactive views of system performance so that potential problems are identified and resolved before they are noticed by the customers.

A web site will be designed to track the status of problems reported, as will as self-help tips, training and Frequently Asked Questions (FAQ).

Several skill sets required for the support of OCN are contained in this document. Where vendor assistance is needed, hourly rates will be provided for needed skill sets. Projects and the vendors project managers will be managed by OCN staff..

Service level agreements will be negotiated so that customers can expect system outages to be analyzed and repaired in a certain number of hours, defects to be resolved within a given time-frame and that analysis on additional requested functionality will be completed within a given time-frame.

Vendors are expected to provide the most economical hardware and software *solutions* with a minimum life expectancy of two years. Vendors will be provided with which functions need support as well as the level of support desired (24X7 or prime-time only).

Application: Application Support

This support application includes only OCN controlled servers which run software to perform data editing, storage, transformation, and retrieval according to approved business rules. It includes all hardware devices associated with those servers up to and including the network interface card. It includes all operating system software and application software running on those servers. It may also include server and network monitoring agents necessary for OCN system management. It also includes the programs, databases, and operating software of the OCN internet and intranet website and domain name servers.

This application support includes technical support for court agency staff related to using OCN enabled services.

The following outlines administrative requirements from vendors who will help develop and support OCN:

Requirements

- Vendor personnel may be located in offices supplied by OCN during prime time
- Vendor Status Reports will outline all activity, issues and hours expended
- When an extended outage occurs, vendors will provide communication on status of repair and when customers can expect OCN to be 'up'.
- Vendors will provide a written report within 5 working days after an unplanned extended downtime incident, detailing the problem definition, the *solution*, and appropriate recommendations to avoid a reoccurrence.
- The vendor must maintain a contract with computer hardware manufacturers for 24x7 maintenance and repair of the equipment.
- Repairs to applications caused by vendor production application defects will be provided to OCN without charge
- OCN will contract with vendors for specified contract periods for application and database support (including defect resolution) and for software required by the OCN
- Assist, train and provide system, application and database documentation to OCN technical staff.
- Provide consultation and implementation services for new OCN enhancements

Application Support Requirements:

- Technical support of OCN applications, including ETL and web 24/7
- Implementation of applications and changes into the test environment and migration to production after successful testing
- Version Control of all applications
- Management of process by which testing is completed and applications are migrated to production

- Creation and monitoring of baseline test cases for recursive testing to assure application quality
- Analyze, prioritize and implement changes needed for user requests, repair of defects, and performance improvement (including changes to business rules)
- Support, test and monitor data loading, both conversion and on-going.
- Security management, including test facilities and temporary databases
- Analysis of data quality from applications
- Installation of software patches, upgrades and runtimes for licensed client and server applications
- Maintenance of client and server software licenses

OCN Database Server Support Requirements

- Support the database servers and related hardware, operating software, database software and OCN data.
- Problem diagnosis and resolution, including database 'down' conditions.
- Preventative maintenance activities including:
  - Nightly backup of OCN data.
  - Transportation of OCN database data to secure offsite facility.
  - Security maintenance, addition/deletion of users as necessary.
  - Volume group maintenance, creation/modification of volume groups as necessary.
  - File system maintenance, creation/modification of files as necessary.
  - Monitoring of file system usage.
  - Creation/modification of administrative shell scripts.
  - Review of logs: error, backup and power., RAID (redundant Array of Independent Disks)
  - Periodic Re-Interrupt Priority Level (*IPL*) of the system.
  - Implementation of software upgrades/*patches* for database server.

OCN Database Administration and System Monitoring Requirements

- Establish, maintain and support of test and production
- Establish, test and monitor backups.
- Provide initial OCN data loads for new OCN enhancements.
- Provide sizing/placement/creation of database objects such as table spaces, tables, indexes, rollback segments, partitions.
- Create and manage user roles, profiles, and accounts.
- Create and maintain views
- Implement *referential integrity*.
- Maintain *schema* as directed by OCN.
- Proactively monitor performance, tune and troubleshoot
- Perform backups and offsite storage of any OCN developed programs, procedures and documentation.
- Provide enhancement support of the test and production databases by:

- Adding, deleting, and/or modifying tables, data elements and views.
- Performing reorganizations as required.
- Dropping/adding tables/indexes as required.

Application: Help Desk

Definition

From whatis.com

In a business *enterprise*, a help desk is a place that a user of information technology can call to get help with a problem. In many companies, a help desk is simply one person with a phone number and a more or less organized idea of how to handle the problems that come in. In larger companies, a help desk may consist of a group of experts using software to help track the status of problems and other special software to help analyze problems (for example, the status of a company's telecommunications network). Typically, the term is used for centralized help to users within an *enterprise*. A related term is *call center*, a place that customers call to place orders, track shipments, get help with products, and so forth.

The Web offers the possibility of a new, relatively inexpensive, and effectively standard user interface to help desks (as well as to *call centers*) and appears to be encouraging more automation in help desk service.

Some common names for a help desk include: computer support center, IT response center, customer support center, IT *solutions* center, resource center, information center, and technical support center.

Process

The help desk should be operational as OCN is being developed so that the transition to a production environment will be smooth. As usage increases, it will be necessary to increase staffing.

Business Drivers

To be successful, the OCN infrastructure must be available to:

- Act as a centralized *clearing house* for information about the system.
- Detect and escalate problems within the infrastructure.
- Provide training, education, and assistance for the users.

Implications

Needs

Provides a support environment for the OCN managed system. The geographical dispersion of the users and the equipment introduces considerable complexity to the task of support.

Risks

- Personnel are expensive.

- The OCN help desk/*call center* may be called to deal with issues that are not within scope. The caller may not fully understand or appreciate this fact. There may be gray areas of responsibility, or the problem may appear to be within scope and the time of the call, but later determined to be out of scope.

Relationships

The success or failure of the OCN will heavily depend on the level of customer service provided. The help desk will act as a liaison between the internal support groups and the users.

Dependencies

The OCN infrastructure must be installed and working prior to startup of the help desk. Infrastructure planning must incorporate the help desk requirements, including the ability to resolve problems remotely.

When/How often does it occur?

24/7/365

Priority Scale

1=Must have.

Success Measures

The help desk function should be rated by the users, internal support staff and vendors once every three months. The ratings should be published on the OCN intranet and reported to OCN management. The time to resolution should be tracked and reported on all calls for service. Quality assurance and the investigation of serious and/or persistent complaints should be performed by a group independent from the help desk management.

Business Requirements

- Customers will call a toll-free number for OCN support.. Call coverage should be based on user groups, hours TBD.
- Metrics will provide quality of service according to time of day, response time, ratio of closed calls to *escalation*, percentage of live voice support, end user satisfaction
- A web-based tracking application will be needed to log all support requests and to provide status and details of the support provided; this information will be communicated electronically to the requestor
- When the requestor approves the service for closure, a summary of the service details will be provided electronically, as well as a customer satisfaction questionnaire so that feedback can be given on the level of service provided.

- Support requests will be given priorities and support categories (hardware, application, training, etc) by qualified personnel
- Workflow software will be needed to route service requests to appropriate personnel
- Automatic escalation of requests not serviced within given times(TBD)
- Advance communication of any changes that will increase support calls (applications, operating system, network maintenance, etc)
- The ability to easily send group emails to various predefined geographical sections of the state.

A website will be developed to store:

- Site specific call detail reports by jurisdiction.
- Court specific inquiry detail that only a designated contact party for that court can see
- Inquiry summary and detail reports to evaluate performance against *service level agreements*.
- Self help features such as the ability to change user password and the ability to retrieve forgotten passwords using hint and email.
- FAQ and answers.
- Searchable technical notes.
- Customer service feedback
- Inquiry data to be downloaded to designated contact parties for local processing.
- Data in fixed format or comma delimited format. Depending on predefined roles and profiles, primary contact parties may only download users within their domain.
- Historical inquiry information for the prior 24 months or as specified in the *SLA*.

Application: Network Support

These requirements apply to all hardware, software, maintenance, management and consulting services for the OCN.

Network support includes:

- All communication devices such as routers, hubs, switches, network cables, network servers, internet *firewalls*.
- Email services.
- All personnel services, hardware, software, and network devices necessary to troubleshoot and proactively manage the entire OCN network and application servers.

Business Requirements

- Network Maintenance and Support
    - Hardware
        - The vendors are required to provide full maintenance and support on all components listed in the detail inventory spreadsheets. The required level of maintenance is documented by item on each line. If this item is blank, the vendor should assume that prime time maintenance is required.
        - The vendor must maintain an adequate inventory of spare parts to meet fix or replace requirements.
    - Software
        - The vendors are required to provide full network management as described below.
- Personnel/Responsibilities
    - Vendors must supply at least the following:
        - One full time project manager who may occupy an office provided by OCN management, and who shall:
            - Attend the regularly scheduled OCN project managers meeting (this may be an OCN users group meeting) for the purpose of reporting on and answering questions about network matters.
            - Plan, organize, direct, and control other network projects at the direction of the OCN project manager or his designate.
            - Attend other meetings as appropriate to represent the interests of the OCN users.
        - Network engineers, as needed, to work at the direction of the vendor project manager, and may occupy an office or offices provided by the OCN management.
        - Break/fix engineers, as needed, to meet response time requirements.

        - Personnel and network management software and hardware tools to proactively monitor and manage all OCN network assets from a centralized site.
        - Full management and support of the OCN *firewall* devices.
        - Personnel for full management, development, and support of the OCN web hosting platforms.

- Management
    - The vendors are required to provide full network management. This includes but is not limited to:
        - Troubleshooting network problems.
        - Real time network monitoring and tuning.
        - Reporting progress, call status, and *solution* details to Help Desk/*Call Center*.
        - Updating HC/CC call tracking system as appropriate.
        - Routine reports at the OCN project managers meeting.
        - Weekly unresolved report
- The vendor is required to provide written weekly status to the OCN network project manager on all trouble calls which have been unresolved for 5 working days. This status must include an estimated date and time to fix.
- The vendor is required to provide routine backup and file recovery tasks for servers. This includes offsite storage and retrieval as appropriate.
- The vendor is required to facilitate addition and deletion of accounts to the network as directed by the OCN network project manager.
- The vendor is required to facilitate moving OCN workstations from one site to another. There will be a maximum number of moves per month to be scheduled during business hours. Moves requested by OCN management outside of business hours shall be paid at out-of-scope hourly rates.
- The vendor shall provide monitoring and reporting on the status of the networks.
- The vendor shall provide planning and consultation on hardware and software upgrades and expansions.
- The vendor shall provide installation of hardware and software upgrades and expansions.
- The vendor shall provide in an annual “state of the networks” report, a written audit and assessment report of the supported networks with recommendations for improvement as appropriate. This report must be delivered to OCN management by the end of February each year.
- The vendor shall provide an annual physical inventory of all supported networks by June 30 of each contract period. The vendor shall deliver an accurate up-to-date spreadsheet containing all of the items on the network. Unless otherwise directed, the format shall be that of the attached inventory lists.
- The vendor shall keep the inventory database updated as items are added, deleted or moved. This inventory shall be the property of OCN management and shall be readily available to OCN management at all times.
- The vendor shall provide a report of monthly significant events, and significant known upcoming events.

Business Continuity

Business Continuity Executive Summary

Business continuity is defined as the degree to which an organization may achieve uninterrupted stability of systems and operational procedures. In this document, *business continuity* will refer to the OCN as the organization for *business continuity* and not as the local courts that provide data to the OCN. The Service Integration Work Group has separated *business continuity* into data recoverability and operations *failover*.

General Business Continuity Requirements

- The *solution* must *mitigate* loss in the event of an attack and expedite recovery **<1>**
- The *solution* must provide protection of data as a core business asset. **<1>**
- The *solution* must provide a *data-consistent point in time* from which to recover. **<1>**
- The *solution* must have the ability to do file level restores. **<1>**
- The *solution* should resolve "*backup window*" issues. **<2>**
- The *solution* should (if possible) replicate disks of data sources; thus eliminating the need for "*bare metal restore products*." (mirrored, hot-swappable disks) **<1>**
- The *solution* must incorporate *load balancing*. **<1>**
- The *solution* must perform *failover* operation automatically so that it is truly transparent to users. **<1>**

Application: Data Backup

Definition

A "backup" is the collection, copying and storing of the OCN data structures, operating system, and populated data elements, along with indexing methods and storage idioms, in a safe and easily retrievable location.

Procedure

- Creation of real-time data. Particular attention should be paid to issues of consistency, format, standardization and metadata description in the very beginning in order to maintain a high degree of efficiency.
- Acquisition and/or collection of data for backup
- Identification/cataloging of digital object for backup
- Storage
- Access to backup data (access mechanisms, rights management and security requirements)
- Scheduled test restore capabilities

- Backups should be checked regularly for integrity. Backup and recovery should be automatic.
- Backup plans and policies should also be checked on a regular basis for relevance and expected benefits. See Governance for more details.

Business Drivers

Stakeholders require 24/7 availability of critical applications and data. The OCN must provide a network that is not prone to downtime and provide a secure source for critical data.

When/How often does it occur?

The backup frequency is dependent on the *data recovery assessment*. The backup schedule will vary for each data source. There is the expectation of distributed backup in 88 counties from which the central repository can request resubmission of data. The goal would be restoration to a point in time no greater than 24 hours prior to the point of system loss. As an example:

Data Sources

• Database server	real time
• *Web server*	daily
• *Proxy server*	weekly
• Exchange server	daily
• Email server	daily

Technology Requirements

At some point in the planning process, the committee will need to settle on, and recommend purchase of, one particular database product.

Considerations at this phase include:

- Scalability **<1>**
- Universal market acceptance **<2>**
- Expectation of ongoing support **<1>**
- Maturity of the product **<2>**
- Options to take best advantage of chosen database product **<2>**
- Reasonably open licensing so as not to be economically prohibitive for use in this setting **<3>**
- Web-based interface (portlet) **<2>**
- Transactional (journal and logging) – that is, allowing full system backups while maintaining 24/7 availability. The repository will likely be made available to law enforcement agencies as well as the general public and therefore access cannot be restricted to normal court hours of operation. **<1>**
- Robust and fault tolerant – for the same reasons **<1>**

- Comprehensive and granular security must be native to the *RDBMS* **<1>**
- Backup and recovery operations can contend for the same network resources as production users, sometimes resulting in bandwidth saturation. **<2>**

Functionality Requirements

- Methodology for copying data from a database system to offline or online media for recovery should the database encounter an unexpected shutdown (crash). **<1>**
- Automated, scheduled, routine runs requiring *minimal* operator intervention. **<1>**
- Automated messaging regarding system events **<1>**
- Ability for manual intervention at any stage of the backup process. **<2>**
- Incremental (more frequent) and full (less frequent) database backups. **<1>**
- Live – up and running database (transactional) – backups as well as periodic, scheduled, shut down full database backups. **<1>**
- Methodology and schedule for validating the data backups for integrity. Multiple data types and the relationship among multiple files are critical to the integrity of the entire data set, and if that relationship is not preserved during backup, the entire data set could be rendered worthless. **<1>**
- Supported by online and offline log files to permit point-in-time recovery after a database failure. **<1>**
- *Remote access* to and management of backup and recovery tools. **<2>**

Application: Data Archiving

Definition

The procedure for providing long-term storage of OCN data that must be retained for either historic or legal purposes.

Process

- Creation of real-time data. Particular attention should be paid to issues of consistency, format, standardization and metadata description in the very beginning in order to maintain a high degree of efficiency.
- Acquisition and/or collection of data for archival
- Identification/cataloging of digital object to be *archived*
- Storage
- Preservation allowing for new hardware and software migration over time
- Access to *archived* data (access mechanisms, rights management and security requirements)

Business Drivers

Stakeholders require critical applications and data be *archived* yearly (i.e. end of fiscal year). The information/data will not be modifiable and will be viewable in its original state; and shall be retained as established by court rule before being destroyed. The *archive* will not be used to recover information/data in the event of system or equipment failure.

When/How often does it occur?

Archiving shall be performed on an ongoing basis based on performance and financial needs.

Risks

- There may be a discrepancy between local court archiving processes/obligations and the archiving policy of the OCN repository.
- Expungements (ex: record exists at OCN level but not at local level)
- Destruction (purging) of data requires a policy

Relationships

- Governance
- Network
- Critical Applications
- Standards
- Portal
- Security

Technology Requirements

At some point in the planning process, the committee will need to settle on, and recommend purchase of, one particular database product. Considerations at this phase include:

- Scalability **<1>**
- Universal market acceptance **<2>**
- Expectation of ongoing support **<1>**
- Maturity of the product **<2>**
- Options to take best advantage of chosen database product **<2>**
- Reasonably open licensing so as not to be economically prohibitive for use in this setting **<3>**
- Web-based interface (portlet) **<2>**
- Transactional (journal and logging) – that is, allowing *archive* processes while maintaining 24/7 availability (The repository will likely be made available to law enforcement agencies as well as the general public and therefore access cannot be restricted to normal court hours of operation) **<1>**
- Robust and fault tolerant – for the same reasons **<1>**
- Comprehensive and granular security must be native to the *RDBMS* **<1>**

Functionality Requirements

- Methodology for storing necessary, but infrequently used, data away from the daily and current data thus improving access times for the current data but at the expense of times required for the *archived* data retrieval. **<2>**

- Automated, rules-based process for creating and continuously or periodically updating the *archives*. Based on: **<2>**
    - Age
    - Size
    - Frequency of Use (Infrequency)
    - Records Retention Rules and Guidelines
    - Dynamic Scheduling
- Need for Trend Analysis **<2>**
- Data Compilations (e.g. reports) maintained intact for pre-determined time **<2>**

Application: Data Recoverability

Definition:
The purpose of data recoverability is to maintain or restore usable data in the event of a disaster. Data recoverability or *disaster recovery* consists of the precautions taken so that the effects of a disaster will be minimized, and the organization will be able to either maintain or quickly resume mission-critical functions.

Another definition of data recovery relates to the salvaging of data stored on damaged media. This is usually provided as a service from various vendors and is not within the scope of this study.

Typically, *disaster recovery* planning involves an analysis of business processes and continuity needs. *Disaster recovery* planning may be developed within an organization or purchased as a software application or a service. In today's IT environment an organization can spend as much as 25% (or more) of its IT budget on *disaster recovery*.

Failover:
Failover can be defined as a backup operation that automatically switches to a standby database, server or network if the primary system fails or is temporarily shut down for servicing. *Failover* automatically and transparently redirects requests from the failed or down system to the backup system that mimics the operations of the primary system.

Originally, stored data was connected to servers in very basic configurations: either point-to-point or cross-coupled. In such an environment, the failure (or even maintenance) of a single server frequently made data access impossible for a large number of users until the server was back online. More recent developments, such as the storage area network (*SAN*), make any-to-any connectivity possible among servers and data storage systems. In general, storage networks use many paths - each consisting of complete sets of all the components involved - between the server and the system. A failed path can result from the failure of any individual component of a path. Multiple connection paths, each with redundant components, are used to help ensure that the connection is still viable even if one (or more) paths fail. The capacity for automatic *failover* means that normal functions can be maintained despite the inevitable interruptions caused by problems with equipment. Different *failover* objectives include path *failover*, server *failover* and application monitoring *failover*.

Failover should be considered for those systems that are judged to be mission-critical and which are relied upon for constant accessibility

Process

- The maximum downtime in the event of a catastrophic incident should be 7-10 consecutive days

Other questions that have to be answered are:

- What is the organization's *Recovery Point Objective* (RPO)?
    - 7-10 consecutive days
- How much administration time will be allocated?
    - 1 full time relationship manager, managing an outsource *solution*
- Is *hot site capability* required or economically feasible? (hot/warm/cold)
    - Yes, *mission critical applications* and *minimal footprint* are required for the hot site and all others on data center storage
- What technologies would yield the most benefit to the OCN?
    - Hot site
    - *Minimal Footprint*
    - *Replication*
    - Tape backup for non-critical systems
    - *SAN*/Network-Attached Storage (NAS)/Internet Small Computer System Interface (ISCSI)
- What is the *ROI*?
    - *Multiple I/O* and *load balancing* would result in better performance.
    - A *high availability* system would also have a high price tag that may be cost prohibitive.

Once these questions are answered priorities can be assigned as to different data sources (email server, *DNS* server etc.)

Relationships

Data recoverability or *disaster recovery* is a subset of *business continuity* and the type of response is determined by the degree of availability that is required.

Dependencies

- The network, servers and storage architecture must be in place and the operating systems installed.
- A basic *data recovery assessment* to determine the organization's *RTO*, *RPO*, *backup window* and return on investment (*ROI*). See Above.

Technology Requirements

- The *solution* must have a centralized *failover*/storage management control point. **<1>**
- The *solution* must replicate open files. **<1>**
- The *solution* must have automatic error detection and notification including a *watchdog/heartbeat line* for server *failover*. **<1>**
- The *solution* must have support for *SCSI* and Fiber Channel. **<1>**
- The *solution* should periodically probe inactive paths to check for failure. **<2>**
- The *solution* should incorporate automatic renaming/mapping for server *failover*. **<2>**
- The *solution* should auto discover storage paths upon installation. **<2>**

Priority Scale

1=Must Have

Success Measures

A test of data recoverability should be performed at least once a year to determine the success of the recovery plan. A testing window should be scheduled.   The test should be unscripted if possible.

Security

Application: Securing

Process –

- *Security audits* should be in place as soon as the OCN is ready for public use
- OCN staff will determine security levels and build matrix
- OCN staff will review deficiencies
- OCN staff will review and adjust deficiencies

Business Drivers –

- *Intrusion detection* must be in place.

Implications –

Risks include

- With large networks the ability to recognize problems becomes masked by compliance requirements, complexity, and operational requirements.
- There can be gaps in compliance auditing – in configuring and implementing monitoring and auditing software, small details can be missed that present large problems.
- *Intrusions*

Relationships –

- The *solution* must interface with all applications
- The *solution* must allow *remote vendor* access control

Dependencies –

- OCN operations
- Trusted partners (other agencies, courts)
- OCN users

Priority Scale

1=Must have.

Success Measures –

- Non intrusion from hackers/malicious programs/viruses
- Approach to performance optimization will be disciplined and effective (securing networks, appliances and applications)

Security Introduction

The OCN will be *enterprise* class infrastructure that obtains information from all of the courts in Ohio in a central repository. The information pulled into the OCN *data warehouse* ranges from public record information to confidential information. The stakeholders have outlined high level security requirements for the *solution* which are outlined in this document. The scope of the OCN's *enterprise* environment should be reviewed when architecting the components of the *security layers* for the OCN.

Scope

At the basic level the OCN must:

- Protect the *data repository* and applications, along with local courts, from network attacks (network *firewall*)
- Identify security risks and proactively protect the infrastructure and applications of the OCN (*intrusion prevention* services)
- Provide secure transport (Secure Sockets Layer [*SSL*] *encryption*)
- Protect applications from *HyperText Transfer Protocol* (HTTP) attacks (*application firewall*)
- Protect data (*business continuity*/DR/identity management)
- Protect people (authentication/authorization)
- Provide effective service level management processes (operations)

Out of the OCN Scope

Any functionality (hardware/software/management) from the local court's point of service to the local court's core is "out of scope" for the OCN. All control of hardware and software acquisition and management of the local court's infrastructure is the responsibility of each local court.

OCN 12 Security Principles

Please keep in mind these security principles when delivering your recommendations:

- **The principle of diversified risk**: Items of value should be separated from other items of value and access rights determined by need-to-know basis;
- **The principle of defense in depth:** Multiple layers and kinds of security are better than single layers and security should be as close to the items as possible;
- **The principle of detection:** Tools and mechanisms should be in place to detect misuse and anomalous activities on both a real time and periodic basis;
- **The principle of incident response:** A response plan should be in place which details actions required when a violation to the security policy is detected (including the responsible parties);
- **The principle of measure:** Security can only be relied upon if it has been measured (tested) following implementation and whenever a security or application system change takes place;

- **The principle of scheduled audit:** A periodic review against polices, standards and procedures should be preformed to ensure compliance;
- **The principle of recovery:** Tools and mechanisms should be in place to ensure recoverability of all items of value;
- **The principle of reliable records:** Secure chronological records should be maintained for all significant activity on the network and import systems;
- **The principle of awareness:** Users represent the best line of defense when they have been properly educated about OCN policies and practices and how to adhere to them;
- **The principle of minimum services:** Entities (systems, devices, etc.) should contain only applications or services for which business reasons exist;
- **The principle of appropriate system configuration:** All known system vulnerabilities that can be eliminated without reducing functionality should be repaired;
- **The principle of least-privilege:** No entity (including systems and applications) should have any rights or privileges without having a related business reason.

Patch Management

- The *solution* must be able to manage *patches* for operating systems, vendor supplied and *in-house applications*, network devices, and *firmware*;
- The *solution* must have the ability to acquire, test, install, and rollback multiple *patches* (code changes);
- The *solution* must maintain a current knowledge base of available and currently installed *patches* and software;
- The *solution* must identify which *patches* are for which systems in the infrastructure;
- The *solution* must document all associated procedures and configurations;
- The *solution* must be able to develop a list of *patch prioritizations* based on risk as assigned by the OCN;
- The *solution* must be able to deploy different sets of *patches* to multiple environments (i.e. development, test, production and training);
- The *solution* must be interoperable with *testing software*;
- The *solution* must be interoperable with *change management software*;
- The *solution* must be interoperable with *help desk software*;
- The *solution* must be interoperable with *security layers*;
- The *solution* must be interoperable with *monitoring applications*;
- The *solution* must be *open standards based*.

Please Note: It is recommended that this functionality come from a “suite” of related applications to ensure interoperability.

Secure Transport

- The *solution* must be able to secure data over the internet with at least 128 bit symmetric key *encryption* and at least 1024 bit asymmetric key *encryption* with selectable key lengths;
- The *solution* must have *portable access* – initial entry from any system that has a browser;
- The *solution* must have the ability to interact with reporting and monitoring software;
- The *solution* must have the ability for "*after-use data cleanup*";
- The *solution* must have the ability to create "*classes of access*" not only by user right, but also by ascertaining the trustworthiness of the network and system from which the *remote user* is attempting a connection;
- The *solution* must have the capacity to create centralized certificate management at a single source;
- The *solution* must have the ability to perform traffic management decisions for both *HTTP* and HTTPS traffic, regardless of IP address;
- The *solution* must have *SSL* reverse proxy including *cookie* persistence, *cookie* switching, *HTTP* header switching, etc.;
- The *solution* must have the ability for optional high speed interfaces.

Application Protection

- The *solution* must protect against *HTTP* attacks in conjunction with a network *firewall* and *intrusion prevention* (defense in depth) layers of the network and be capable of *SSL* reverse proxy;
- The *solution* must have the ability to block viruses and worms tunneling in through a *SSL*/*Virtual Private Network* (VPN) connection;
- The *solution* must accommodate current web standards;
- The *solution* must allow client side scripting;
- The *solution* must provide administration and management across the *enterprise*
- The *solution* must include role based management (security)
- The *solution* must allow for segregation and granular security setting for each application being used in the infrastructure.

Service Level Management (SLM)

[Please note this section overlaps with operations. It should be noted that proper SLM is critical to effective security for the OCN *enterprise*.]

- The *solution* must provide *incident management*;
- The *solution* must provide *change management*;
- The *solution* must be able to monitor approved baseline and track changes;
- The *solution* must provide monitoring and reporting to authorized users;
- The *solution* must provide *profile management*.

Authentication and Authorization

- The *solution* must allow for flexible role based management and granular access control;
- The *solution* must support two forms of identification;
- The *solution* must provide logging of all accesses of the system;
- The *solution* must provide single sign on.

Network Protection

- The *solution* must protect from network based attacks;
- The *solution* must prevent network based attacks;
- The *solution* must protect from *malware*;
- The *solution* must provide content filtering and *spam* filtering.

Related Definitions

Balanced Score Card

Balanced score card methodology is an analysis technique designed to translate an organization’s mission statement and overall business strategy into specific, quantifiable goals and to monitor the organization’s performance in terms of achieving these goals.

Capability Maturity Model

The capability maturity model (CMM) is a methodology used to develop and refine an organization’s software development, *project management* and organizational process. The model describes a five-level evolutionary path of increasingly organized and systematically more mature processes. An example of the software maturity levels follows.

CMM’s Five Maturity Levels of Software Processes

- At the initial level, processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable, because processes would not be sufficiently defined and documented to allow them to be replicated.
- At the repeatable level, basic *project management* techniques are established, and successes could be repeated, because the requisite processes would have been made established, defined, and documented.
- At the defined level, an organization has developed its own standard software process through greater attention to documentation, standardization, and integration.
- At the managed level, an organization monitors and controls its own processes through data collection and analysis.
- At the optimizing level, processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization’s particular needs

Deployment Environment

To deploy is “to spread out or arrange strategically.” Long used in the context of military strategy, it has now gained currency in information technology. In its IT context, deployment encompasses all the processes involved in getting new software or hardware up and running properly in its correct environment, including installation, configuration, running, testing, and making necessary changes. The word implementation is sometimes used to mean the same thing. In the context of this document a deployment environment “deploys” the change to the OCN’s baseline to the appropriate environment. An example process would be in the following sequence: (1) *development environment*; (2) deployment environment; (3) *test environment*; (4) deployment environment; (5a) *production environment*; (5b) *training environment*.

Incident Response Plan
Incident response is defined as a plan that is written to *mitigate* risk for the *enterprise* (i.e. when a problem occurs, it is identified and then you respond to it.) Incident response plans tend to have the following characteristics:

- **Communicating the incident** is the most important item. If an incident occurs, make sure that it is communicated to the team leader so that the plan can be implemented.
- **Containing the damage and then minimizing the risk** is critical to an incident. For instance, if the incident in your initial assessment is a worm that is self-replicating across your network, then you can contain the damage by unplugging the workstation that is affected from the switch or hub. This contains the damage and minimizes the risk
- **Identifying the type and severity of the compromise** is essential to see what kind of resources you need to put on it. If you have a very large problem that may cost the company millions (or worse yet put it out of business), you need to label it as such and give it a severity level like “high priority.” You should attempt to determine the exact nature of the attack. Also, try to determine the attack point of origin – where exactly is it coming from and directly after, try to identify the systems that have been compromised.
- **Protecting evidence** is essential for a couple of reasons. For one, you never want to contaminate the evidence yourself; you may also want to make sure that someone else does not damage it intentionally.
- **Notifying external agencies** like law enforcement is something you need to plan for. Hopefully it won’t need to come to this, but if it does, you need to know how to deal with it and who to contact. Most law enforcement agencies these days are either building or have built some form of cybercrimes division.
- **Recovering systems** is one of the most critical incident plan steps, because after the incident you have to get your systems back online.
- **Assessing incident damage and cost** is something you need to do for the company you work for. Especially with companies that are held publicly by stockholders, if a major loss occurs, this will be very critical data to have. This needs to be done by a leader in the incident response team.
- **Reviewing the response and updating policies** on a regular basis is a necessary part of the strategy. A plan is no good unless it is up to date and well prepared.

Updating your plan after an actual response is a good idea so you can assess the plan and how you may have been able to do things better.

Remote Access Server
A server that is dedicated to handling users that are not on a Local Area Network (LAN)/Metro Area Network (MAN) but need *remote access* to it. The *remote access* server allows users to gain access to files and print services on the LAN from a remote location. For example, a user who dials into a network from home using an analog modem or a broadband connection will connect to a *remote access* server. Once the user is authenticated he can access shared drives and printers as if he were physically connected to the office LAN.

Vendor Supplied Applications
A program or group of programs designed for end users that are created and supported by commercial application developers. Software can be divided into two general classes: systems software and application software. Systems software consists of low-level programs that interact with the computer at a very basic level. This includes operating systems, compilers, and utilities for managing computer resources. In contrast, applications software (also called end-user programs) includes database programs, word processors, and spreadsheets. Figuratively speaking, applications software sits on top of systems software because it is unable to run without the operating system and system utilities.

Glossary

ACH	An electronic funds transfer system used for bill presentation and payment via automated means through a third party, the ACH. Members wire instructions to the Automated Clearing House which then wires funds to the appropriate receiving entity.
ADA	A 1990 federal law that forbids discrimination against persons who are disabled. (Google)
Administrative Applications	Administrative applications are those used to manage a wide variety of equipment and application contracts, Service Level Agreements (SLA's) and other third party support contracts. (Not including: Planning & Management; Human Resources)
After-Use Data Cleanup	Refers to the practice of Data Management, more specifically keeping the OCN's storage lean. What this means is keeping storage clean of out-of-scope and obsolete files. Examples include files such as out of scope photos, resumes, stock files, gaming files, etc.
Agility	In the context of technology, the ability of an application to rapidly change to meet evolving user needs
ANSI	American National Standards Institute: Standard setting body
API	Application Programming Interface – the protocols and standards of software used to access the functionalities of an operating system and other services hosted on a computer which allows system level integration between the software programs. This inter-working facilitates data sharing between products and across different platforms which facilitates interoperability.
Application Firewall	a reduced application that allows filtering of input for a specific service to allow only desired input. By defining what is acceptable and what is not, it can abort abnormal sessions of a protocol and stop them from continuing on to the actual application. (http://www.eeye.com/html/Research/Papers/DS20010322.html)
Application Layer Protocols	the ways in which different applications (like e-mail programs, web servers and browsers, etc.) talk to each other. (http://dsv.su.se/jpalme/abook/)
Archive	a bundle of other files contained in one file itself. (thefreedictionary.com)
Backup Window	a time period during which a backup can occur. (thefreedicionary.com)
Bare Metal Restore Products	mirrored, hot-swappable disks
Browser-Based	In software engineering, a web application is an application delivered to users from a web server over a network such as the World Wide Web or an intranet. Web applications are popular due to the ubiquity of the web browser as a client, sometimes called a thin client. (Google)
Business Continuity	the degree to which an organization may achieve uninterrupted stability of systems and operation procedures.

	(thefreedictionary.com)
Business Intelligence	a broad category of application programs and technologies for gathering, storing, analyzing, and providing access to data to help enterprise users make better business decisions. BI applications include the activities of decision support, query and reporting, online analytical processing (OLAP), statistical analysis, forecasting, and data mining. (www.sauder.ubc.ca/cgs/itm/itm_glossary.html)
Capacity Planning	The process of determining the amount of capacity required to produce in the future. This process may be performed at an aggregate or product-line level (resource requirements planning), at the master-scheduling level (rough-cut capacity planning), and at the material requirements planning level (capacity requirements planning). (Google)
Change Management	Change management is a systematic approach to dealing with change, both from the perspective of an organization and on the individual level. A somewhat ambiguous term, change management has at least three different aspects, including: adapting to change, controlling change, and effecting change. A proactive approach to dealing with change is at the core of all three aspects. For an organization, change management means defining and implementing procedures and/or technologies to deal with changes in the business environment and to profit from changing opportunities.
Change Management Software	An application used to deliver comprehensive policy, process management, and planning capabilities as well as impact, risk and resource requirements associated with any changes.
Classes of Access	A privilege to use computer information in some manner. For example, a user might be granted read access to a file, meaning that the user can read the file but cannot modify or delete it. Most operating systems have several different types of access privileges that can be granted or denied to specific users or groups of users.
Clustering	Group of independent systems working together as a single system. Clustering technology allows groups of servers to access a single disk array containing applications and data. (Google)
Common Gateway Interface (CGI)	A standard mechanism for extending Web server functionality by executing programs or scripts on the Web server in response to Web browser requests. A common use of CGI is in form processing, where the browser sends the form data to a CGI script on the server, and the script integrates the data with a database and sends back a results page as HTML. (website.armmnet.net/faq/glossary.html)
Compression Support	data compression available through the modem service to speed data transfer. (Google)
Configuration Management	A management of software configurations, upgrades, patches, and which can also audit the infrastructure to ensure consistency with specified configurations over time to avoid configuration drift.

	Configuration management can require a significant investment in the delivery of software projects, and the lack of automated configuration management systems can cause projects to fail.
Contact Management	Address books
Contract Management	Contract management is a principal supplier management task and comprises: • The set of activities concerned with the implementation of the contract, operational management of the supplier within the framework set by the contract, relationship and compliance management. • Contract management is characterized by frequent contact with the supplier over the life of the contract. • The establishment and promulgation of “standards” for example the establishment of PC and PC software standards both to the supplier and within the buying organization. • Periodic review of how well both parties are complying with the requirements of the contract. (Google)
Cookie	A small text file of information that certain Web sites attach to a user's hard drive while the user is browsing the Web site. A Cookie can contain information such as user ID, user preferences, archive shopping cart information, etc. (Google)
CRM	Customer Relationship Management - An integrated information system that is used to plan, schedule and control the presales and postsales activities in an organization. CRM embraces all aspects of dealing with prospects and customers, including the call center, sales force, marketing, technical support and field service. The primary goal of CRM is to improve long-term growth and profitability through a better understanding of customer behavior. CRM aims to provide more effective feedback and improved integration to better gauge the return on investment (ROI) in these areas. (thefreedictionary.com)
Data Cleansing	Also referred to as data scrubbing, the acts of detecting and removing and/or correcting a database’s dirty data (i.e., data that is incorrect, out-of-date, redundant, incomplete, or formatted incorrectly). The goal of data cleansing is not just to clean up the data in a database but also to bring consistency to different sets of data that have been merged from separate databases. Sophisticated software applications are available to clean a database’s data using algorithms, rules and look-up tables, a task that was once done manually and therefore still subject to human error. Source – Webopedia.com: http://www.webopedia.com/TERM/D/data_cleansing.html
Data-Consistent Point In Time	a power-outage-consistent or crash-consistent copy of the data at the remote mirror site, suitable for emergency restart, guaranteeing no partial transactions, thus assuring database integrity. (http://www.redbooks.ibm.com/redpapers/pdfs/redp4063.pdf)
Data Definition Language	The SQL syntax used to define the way the database is physically organized. (Google)

Data Recovery Assessment	a process to determine the ability/vulnerability to restore data from disks, tapes, CDs, etc that have been damaged by accidents, natural disasters, power surges and malfunctioning electronics. (thefreedictionary.com)
Data Repository	A database acting as an information storage facility. Although often used synonymously with data warehouse, a repository does not have the analysis or querying functionality of a warehouse. (Google)
Data Warehouse	A data warehouse is, primarily, a record of an enterprise's past transactional and operational information, stored in a database designed to favor efficient data analysis and reporting. Data warehousing is not meant for current "live" data
DBMS	Database Management System
Decision Support Systems	Software used to aid management decision making. Telecommuting: Working at home and communicating with the office by electronic means. (thefreedictionary.com)
Development Environment	In computer program and software product development, the development environment is the set of processes and programming tools used to create the program or software product. The term may sometimes also imply the physical environment (as this case). An integrated development environment is one in which the processes and tools are coordinated to provide developers an orderly interface to and convenient view of the development process (or at least the processes of writing code, testing it, and packaging it for use). An example of an IDE product is Microsoft's Visual Studio .NET. The term computer-assisted software environment (CASE) is generally used to describe a set of tools and practices that facilitate management of a software development project. For the purposes of this paper the OCN Development Environment is the physical environment where all of OCN's development takes place using some type of programming tools.
Disaster Recovery	a plan for duplicating computer operations after a catastrophe occurs, such as a fire or earthquake. It includes routine off-site backup as well as a procedure for activating vital information systems in a new location. (thefreedictionary.com)
Distributed Administration	Enabling project deployment to many different employees at different locations.
DMZ	DeMilitarized Zone. A middle ground between an organization's trusted internal network and an untrusted, external network such as the Internet. Also called a "perimeter network," the DMZ is a subnetwork (subnet) that may sit between firewalls or off one leg of a firewall. Organizations typically place their Web, mail and authentication servers in the DMZ. DMZ is a military term that refers to the area between two enemies. (thefreedictionary.com)
DNS	The name resolution system that lets users locate computers on a Unix network or the Internet (TCP/IP network) by domain name. (thefreedictionary.com)

Document Management	software that provides check-in, check-out, storage and retrieval of electronic documents often in the form of word processor files and the like. workflow management **-** the operational aspect of a work procedure: how tasks are structured, who perfoms them, what their relative order is, how they are synchronized, how information flows to support the tasks and how tasks are being tracked. (thefreedictionary.com)
EBIS	enterprise business intelligence solution
Encryption	Encryption is the conversion of data into a form, called a ciphertext , that cannot be easily understood by unauthorized people (whatis.com)
Enterprise	Word used to describe a very large, complex system that spans the entire organization, in this case the entire judicial branch. Describes multiple processes often in multiple geographic locations used by different individuals, departments and units for different purposes. System wide. Also the name of the spaceship on Star Trek.
Enterprise Score Carding	Enterprise score carding allows you to track performance in real time and establish accountability throughout the organization. (http://www.deltek.com/deltekweb.asp?id=686)
Escalation	Indicates that the Specialist was unable to resolve the problem and has forwarded it for additional assistance. (Google)
ESMTP	Extended Simple Mail Transfer Protocol.
ETL	Extract, Transform and Load software extracts records/fields from one data source, converts the data to new formats and provides the ability to load the data to other target destinations. This data handling and processing precedes final storage in the data repository.
Extranet	two or more intranets with network connectivity. (thefreedictionary.com)
Failover	the capability to switch over automatically to a redundant or standby computer server, system, or network upon the failure or abnormal termination of the previously active server, system, or network. Failover happens without human intervention and generally without warning, unlike switchover. (thefreedictionary.com)
FIPS 180-2	FIPS 180-2 secure hash algorithm: Federal Information Processing Standards issued by the National Institute of Standards and Technology. The purpose of a hash algorithm is to prove that a message has not been altered
Firewall	The primary method for keeping a computer secure from intruders. A firewall allows or blocks traffic into and out of a private network or the user's computer. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network. Firewalls are also used to keep internal network segments secure; for example, the accounting network might be vulnerable to snooping from within the enterprise. (thefreedictionary.com)
Firmware	Firmware is programming that is inserted into programmable read-

	only memory (programmable ROM), thus becoming a permanent part of a computing device. Firmware is created and tested like software (using microcode simulation). When ready, it can be distributed like other software and, using a special user interface, installed in the programmable read-only memory by the user. Firmware is sometimes distributed for printers, modems, and other computer devices. IBM prefers the term microcode.
Footprint	the portion of computing resources, typically RAM, CPU time and disk space that a piece of software requires in order to operate. (thefreedictionary.com)
Fragile Artifacts	pivotal failure points
FTP	File Transfer Protocol - a software standard for transferring computer files between machines with widely different operating systems. (thefreedictionary.com)
Gantt Chart	A scheduling tool used to display the status of a project's tasks. A Gantt chart shows each task's duration as a horizontal line. The ends of the lines correspond to the task's start and end dates. (Google)
Genetic Data Environment	a program that runs programs. (http://home.cc.umanitoba.ca/~psgendb/GDE/gde.html)
GJXDM	Global Justice XML Data Model. The XML standard adopted by the Department of Justice and by the ACTC Standards Subcommittee. A standard for exchanging information between computer systems that describe activities in the justice process (i.e. Incident, Arrest, Indict, Sentence, Incarcerate, Parole)
Graphic User Interface	Pronounced gooey. A method of controlling software using on-screen icons, menus, dialog boxes, and objects that can be moved or resized, usually with a pointing device such as a mouse. (Google)
Groupware	a technology designed to facilitate the work of groups where the participants are in different and sometimes remote places.
Help Desk Software	An application that automates the ability to submit, monitor, and manage help desk cases. It also indicates which services are impacted by a given incident or problem. A help desk solution will enable users to search FAQs, known solutions, and workarounds to common issues to encourage user self-sufficiency and reduce call volumes.
Heuristic	involving or serving as an aid to learning, discovery, or problem-solving by experimental and especially trial-and-error methods (heuristic techniques, a heuristic assumption); also: of or relating to exploratory problem-solving techniques that utilize self-educating techniques (as the evaluation of feedback) to improve performance (a heuristic computer program)
High Availability	a multiprocessing system that can quickly recover from a failure. There may be a minute or two of downtime while one system switches over to another, but processing will continue. This is not the same as fault tolerant, in which redundant components are designed for continuous processing without skipping a heartbeat. (thefreedictionary.com)

Hot Site Capability	a fully equipped data processing facility maintained on a standby basis for use in a resumption operation. (Google)
Human Factors	Human capabilities and limitations to the design and organization of the work environment. Primarily attributed to errors, but also a consideration in the design of workflow and processes. The study of human factors can help identify operations susceptible to human error and improve working conditions to reduce fatigue and inattention. (Google)
Hypertext	Text allowing documents to link to each other
HyperText Markup Language	the coding language used to create hypertext documents for the World Wide Web. In HTML, a block of text can be surrounded with tags that indicate how it should appear (for example, in bold face or italics). Also, in HTML a word, a block of text, or an image can be linked to another file on the Web. HTML files are viewed with a World Wide Web browser. (www.starrsites.com/glossary.htm)
HyperText Transfer Protocol (HTTP)	The protocol for moving hypertext files across the Internet. (Google)
IMAP	Internet Message Access Protocol **-** A standard interface between an e-mail client program and the mail server. IMAP4 and POP3 are the two common access protocols used for Internet e-mail. IMAP4 provides a message store that holds incoming e-mail until users log on and download it. (thefreedictionary.com)
Incident Management	The process of managing a crisis event. (Google)
Information Security System Managers (ISSM)	"The activities of *Information Security System Managers (ISSM)* can be broken down into the following five categories: functional security; coordination; documentation; configuration management and certification and accreditation; and risk management. Accomplishing all of the tasks associated with these five areas ensures an ISSM is limiting his/her organization's liability, and is accomplishing due diligence in support of the organization as well as any customers associated with the organization." (Shelley Bard, CISSP senior security network engineer, Federal Network Systems. Bard is an info security professor and has briefed the Whitehouse, Department of Defense, interest groups, industry and academia.)[4]
In-House Applications	Applications that are developed by programmers employed by the end users. This class of software is usually intended for a very specific purpose that cannot be met by vendor supplied applications. The cost to develop and continue to maintain this type of application can be very high depending on the complexity of its tasking. If the intended application is not subject to upgrades, changes in complexity and operation and must be extremely task oriented then the cost to develop and maintain it can be less than commercially procured applications.

[4] http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci948651,00.html

Intrusion Detection	Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network. (Google)
Intrusion Prevention	Intrusion prevention is a preemptive approach to network security used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) monitors network traffic. However, because an exploit may be carried out very quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate action, based on a set of rules established by the network administrator. For example, an IPS might drop a packet that it determines to be malicious and block all further traffic from that IP address or port.
Intrusions	Any sets of actions that attempt to compromise the integrity, confidentiality or availability of a resource. (Google)
I/O	Input/Output **-** a system of communication for information processing systems. (thefreedictionary.com)
IPv6	Internet Protocol version 6 **-** is a network layer standard that governs the addressing and routing of data packets through a network. (thefreedictionary.com)
Instant Messaging	Instant Messaging is a form of electronic communication which involves immediate correspondence between two or more users who are all online simultaneously. (Google)
Issue Tracking	computer software packages that manage and maintain lists of issues, as needed by an organization. Issue tracking systems are commonly used in an organization's customer support call center to create, update, and resolve reported customer issues, or even issues reported by that organization's others employees. An issue tracking system often also contains a knowledge base containing information on each customer, resolutions to common problems, and other such data. (http://en.wikipedia.org/wiki/Issue_tracking_system)
Java	A standards based programming language designed to run programs on a wide variety of operating systems (i.e. Windows, Linix) and Internet Browsers (i.e. Internet Explorer, Firefox)
KPI	Key Performance Indicators: Measure or metric used to objectively judge the effectiveness of a process
LDAP	Lightweight Directory Access Protocol **-** A protocol used to access a directory listing. LDAP support is being implemented in Web browsers and e-mail programs, which can query an LDAP-compliant directory.
Load Balancing	Dividing the amount of work that a computer has to do between two or more computers so that more work gets done in the same amount of time and, in general, all users get served faster. Load balancing can be implemented with hardware, software, or a combination of both.(What is.com)
Mail Transfer Agent (MTA)	a computer program or software agent which transfers electronic mail messages from one computer to another.

	(thefreedictionary.com)
Malware	Hardware, software, or firmware that is intentionally included or inserted in a system for a harmful purpose. (Google)
Message Board	a web application which provides for discussion. Commonly referred to as web forums, discussion boards, discussion groups, internet forums or simply forums. (thefreedictionary.com)
Messaging System	all the applications necessary to keep e-mail moving as it should.
MIME	Multipurpose Internet Mail Extensions - an internet standard specifying message formats for transmission of different types of data by electronic email. (thefreedictionary.com)
Minimal	the least possible; "needed to enforce minimal standards"; "her grades were minimal"; "minimum wage"; "a minimal charge for the service" (Google)
Mission Critical Applications	Applications usually required for business-critical services such as point-of-sale, command and control, real-time data feeds, wireless back-up, push-to-talk and more. (Google)
Mitigate	To lessen the severity. (Google)
Monitoring Applications	Software that automatically and continually discovers which resources are used by which applications, and presents end-to-end monitoring information within a management interface that is unified from an application perspective. By monitoring critical applications proactively it helps to prevent application failures and identify degradations early.
Monitoring Maps	Diagrams that can be used to monitor network and application functions (http://www.cisco.com/univercd/cc/td/doc/product/wireless/wcs/wcscfg32/wcsmaps.htm)
Multiple I/O	multiple paths to data through the network and multiple disks on which data is stored. (http://www.parl.clemson.edu/pvfs/desc.html)
MX	An entry in a DNS database that points to the mail server for that domain. (thefreedictionary.com)
NNTP	Network News Transfer Protocol - an Internet application protocol used primarily for reading and posting Usenet articles, as well as transferring news among servers. (thefreedictionary.com)
NOS/OS	Network Operating System/Operating System
OLAP	On-Line Analytical Processing… allows users to derive information and business intelligence from Data Warehouse systems by providing tools for querying and analyzing the information in the Warehouse. In particular, OLAP allows multidimensional views and analysis of the data for decision support processes. (planning.ucsc.edu/irps/dwh/DWHGLOSS.HTM)
Ontology	The creation of a systematically ordered data structure that enhances exchange of information between computers and scientists. Ontologies enable the definition and sharing of domain-specific vocabularies. (Google)
Open Standards	Open Standards is the concept of people working together openly to

Based	collaboratively develop solutions for addressing common requirements and goals. Often they work together in committees through open standards organizations, such as the Internet Engineering Task Force (IETF) or the World Wide Web Consortium (W3C). Open standards permit everyone to utilize the resulting specification to build infrastructure and various solutions. This creates the opportunity for unlimited vendors competing on the quality of their implementations and their ability to meet the diverse needs of the end-users in the markets utilizing the open standards.
Operations Monitoring	providing a consolidated view of individual activities across diverse and complex infrastructures
OS	Operating System **-** The master control program that runs the computer.
Patch Management	Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. Patch management tasks include: maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configurations required. Patch Management includes the following processes (1) Acquiring the patches, (2) Testing the Patches, (3) install the patches to production, (4) and rollback of the patches if there is an issue.
Patch Prioritizations	Patch prioritization aids in determining critical security patches from functionality patches and updates. A prioritization plan helps the organization deal with the prioritization and scheduling of updates that, by their nature, must be deployed in a more immediate fashion. A number of factors are routinely considered when determining patch priority and scheduling urgency. Vendor-reported criticality (e.g. high, medium, low) is a key input for calculating a patch's significance and priority, as is the existence of a known exploit or other malicious code that uses the vulnerability being patched as an attack vector. Other factors that should be taken into account when scheduling and prioritizing patches are system criticality (e.g. the relative importance of the applications and data the system supports to the overall business) and system exposure (e.g. DMZ systems vs. internal file servers vs. client workstations).
Patches	Code changes
Platform-Neutral	should run on any machine that has a compatible virtual machine. (http://www.crazysquirrel.com/computing/software/refas/help/platformNeutral.jspx)
Policy-Based Automation	the ability to dynamically allocate resources to applications based on pre-defined policies and real-time business needs. (http://www.gridtoday.com/03/1117/102261.html)
POP3	Post Office Protocol 3 **-** A standard interface between an e-mail

	client program and the mail server. POP3 and IMAP4 are the two common access protocols used for Internet e-mail. POP3 provides a message store that holds incoming e-mail until users log on and download it. (thefreedictionary.com)
Portable Access	When used to describe hardware, portable means small and lightweight. A portable computer is a computer small enough to carry. Portable computers include notebook and subnotebook computers, hand-held computers, palmtops, and PDAs. When used to describe software, portable means that the software has the ability to run on a variety of computers. Portable and machine independent mean the same thing—that the software does not depend on a particular type of hardware.
Portable Document Format	PDF is the de facto standard for the secure and reliable distribution and exchange of electronic documents and forms around the world, with a ten-year track record. PDF is a universal file format that preserves the fonts, images, graphics, and layout of any source document, regardless of the application and platform used to create it. Adobe¨ PDF files are compact and complete, and can be shared, viewed, and printed by anyone with free Adobe Reader¨ software. (www.data-core.com/glossary-of-terms.htm)
Portal-Dashboard	a user interface, similar to an automobile's dashboard, which organizes and presents information in a way that is easy to read. It provides the front-end interface between the user and the system for all applications, features, and services provided. Portal-dashboards can leverage enterprise data resources to present users with clear, actionable information. A customized user interface for access to web based tools and systems; i.e.: reporting tools, portal tools and business intelligence tools. The portal-dashboard is the visual representation of the tool.
Production Environment	The production environment is the physical environment that houses the approved baseline configuration of all applications and hardware that customers use on a daily basis. This environment is where the majority of activity takes place in the OCN infrastructure.
Profile Management	Profile Management consists of the ability for End Users to manage their profile from a web browser so there is no need for an administrator. (Management for profiles is pushed down to the agencies to administrator their own users.) Profile Management consists of a login page where a user can create an account, update an account profile, change passwords and an automated way for the end user to receive a "hint" or some other method of remembering or getting their current password (i.e. e-mail with user name and password sent out to the end user.
Profile Managers	The Profile Manager is used to create and dynamically manage browser and desktop automatic configuration settings. (Google)
Program Management	The coordinated management of a portfolio of projects to achieve a set of business objectives is called program management. Or, a

	program might refer to an ongoing set of activities internal to the organization, for example, a Total Quality Management program, workplace safety program, supplier development program, etc. (Google)
Project Management	The application of knowledge, skills, tools and techniques to a broad range of activities to meet the requirements of the particular project. Project management knowledge and practices are best described in terms of their component processes. These processes can be placed into five process groups (initiating, planning, executing, controlling and closing) and nine knowledge areas (project integration management, project scope management, project time management, project cost management, project quality management, project human resource management, project communications management, project risk management and project procurement management). (Google)
Proxy Server	Where a high level of security of required, a proxy web server may be used to provide a gateway between a local area network and the internet. The local network is protected by firewall software installed on the proxy server. This software enables the proxy server to keep the two worlds separate. All outward HTTP requests from the local network pass through the proxy server and similarly all information retrieved comes back in via the proxy server and is then passed back to the client. Using the options or preferences, web browsers can be configured to point to the proxy (Google)
RDBMS	Relational DataBase Management System
Recovery Point Objective	The point in time to which data must be restored in order to resume processing transactions. (Google)
Recovery Time Objective (RTO)	the time goal for the re-establishment and recover of business function or resource during the execution of disaster recovery. (thefreedictionary.com)
Referential Integrity	An integrity constraint specifying that the value (or existence) of an attribute in one relation depends on the value (or existence) of an attribute in the same or another relation. (Google)
Release Management	In the context of SOA, release management defines the model to ensure the "deploy once run from everywhere" promise can be realized in the SOA environment that becomes exponentially more complicated as services are added. (Google)
Remote Access	Remote access is the ability to log onto a network from a distant location using a computer, a connection, and some remote access software to connect to the network. Remote access means that the remote computer actually becomes a full-fledged host on the network. The remote access software connects directly to the network server.
Remote User	Remote User refers to a person who uses technology that enables them to connect, in geographically dispersed locations, and access resources as if from on-site. This access is typically over some kind

	of dial-up or broadband connection (may also include WAN connections).
Remote Vendor	vendors utilizing the same VPN connection as an employee (http://www.e-dmzsecurity.com/pr/2006-02-14.html)
Replication	the provision of redundant resources (software or hardware components) to improve reliability and fault-tolerance. (thefreedictionary.com)
Resource Management	The handling of all materials as being of inherent value. The placement of all or any material in a re-use hierarchy. (Google)
Revision Control	Revision Control is the management and storage of document and software revisions. It is primarily concerned with ensuring that previous versions of information are not lost. (Google)
Risk Management	Decisions to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls. (Google)
ROI	Return on Investment **-** a calculation used to determine whether a proposed investment is wise, and how well it will repay the investor. The calculation of the ratio of the amount gained or lost relative to the basis. (thefreedictionary.com)
RSS Feed	Rich Site Summary, or Really Simple Syndication – A simple XML format for distributing news headlines and other content on the Web
Rule Processing	Rule processing enables an authority to describe what constitutes an intrusion in his or her network. (http://www.cse.seas.wustl.edu/techreportfiles/getreport.asp?429)
SAN (Storage Area Network)	a network designed to attach computer storage devices such as disk array controllers and tape libraries to servers. (thefreedictionary.com)
Scalable	supports different monitoring architectures and numbers of users
Schema	indicates a formal index or table of contents that describes what, where and how information is stored and accessed in a database.
Scorecard	an application or custom user interface that helps manage an organization's performance by optimizing and aligning organizational units, business processes and individuals. It should also provide internal and industry benchmarks, as well as goals and targets that help individuals understand their contributions to the organization. The use of scorecards spans the operational, tactical and strategic aspects of the business and its decisions. (www.dmreview.com)
Script Capable	Capable of running scripts
SCSI	Small Computer System Interface - pronounced "scuzzy" is a hardware interface that allows for the connection of up to 15 peripheral devices to a single PCI board called a "SCSI host adapter" that plugs into the motherboard. (thefreedictionary.com)
Security Audits	searches through a computer system for security problems and vulnerabilities. (Google)
Security Layers	Using multiple layers in a security model is the most effective method of securing and deterring unauthorized use of computer systems and network services. Every layer provides some protection

	from intrusion, and the defeat of one layer may not lead to the compromise your whole organization. Each layer has some inter-dependence on other layers. For example, the intrusion detection systems and the incident response plan have some interdependencies. The most common security model will likely be built upon the following layers: • Security policy of your organization • Host system security • Auditing • Router security • Firewalls • Intrusion detection systems
Semantic	of or relating to meaning or the study of meaning (Google)
Server Fault Recovery	restarts servers automatically without administrator intervention (http://www-306.ibm.com/software/success/cssdb.nsf/CS/EHON-5JJK2P?OpenDocument&Site=default)
Service Level Agreements (SLA)	A binding contract which formally specifies end-user expectation about the solution and tolerances. It is a collection of service level requirements that have been negotiated and mutually agreed upon by the information providers and the information consumers. The SLA has three attributes: STRUCTURE, PRECISION, AND FEASIBILITY. This agreement establishes expectations and impacts the design of the components of the data warehouse solution.
S/MIME	Secure Multipurpose Internet Mail Extensions - a standard for public key encryption and signing of e-mail encapsulated in MIME. (thefreedictionary.com)
SMTP	Simple Mail Transfer Protocol: The standard e-mail protocol on the Internet and part of the TCP/IP protocol suite. SMTP defines the message format and the message transfer agent (MTA), which stores and forwards the mail. SMTP was originally designed for only plain text (ASCII text), but MIME and other encoding methods enable executable programs and multimedia files to be attached to and transported with the e-mail message. (thefreedictionary.com)
Solution	This is used often in business IT marketing. IDC defines an "IT solution" as a combination of hardware, software, and services, which is designed to solve a specific business problem and sold as a complete package or bundle to a customer
Spam	Stupid Pointless Annoying Messages - unsolicited bulk electronic messages, such as email spam. (thefreedictionary.com)
Spyware	a broad category of malicious software intended to intercept or take partial control of a computer's operation with out the user's informed consent. (thefreedictionary.com)
SSL	Secure Socket Layer - A commonly used protocol that provides a connection between a client and a server which encrypts the data being transmitted over the internet to assure its confidentiality.
Structured Query	pronounced "sequel", is a language that provides an interface to

Language (SQL)	relational database systems. It was developed by IBM in the 1970s for use in System R. SQL is a de facto standard, as well as an ISO and ANSI standard. (www.orafaq.com/glossary/faqgloss.htm)
Syntactic	of or relating to or conforming to the rules of syntax; "the syntactic rules of a language" (Google)
TCP-IP	The basic protocols controlling applications on the Internet; it stands for "transmission control protocol/Internet protocol."
Test Environment	A test environment is an environment that simulates and protects your production environment. The purpose of a test environment is to test hardware, operating systems, or applications designed to run together before introducing them into your production environment. Any changes to the OCN's production environment will need to be tested in the test environment before deployment.
Testing Software	An application used for validating the functionality, performance, and reliability of applications, patches, and or upgrades prior to the actual implementation.
TIFF	Tagged Image File Format – (abbreviated TIFF) A file format used mainly for storing a scanned image as a file. It allows for a flexible set of information fields called tags.
Timely	happening at the right time in the right manner.
Training Environment	A training environment will be needed if the OCN has a business need to provide instructor led training, web based training, or computer based training for the applications being used on its infrastructure. A training environment allows the creation of a baseline with prepared data. It also allows end users to go through a training process and then allows OCN staff to return the environment to the original baseline for the next user or class.
Transaction Logging	Method that provides recovery protection if a failure occurs as data is actually written to the database during the transaction. (Google)
Transactional Reporting	systems generally require having some reports on transactions, providing detailed reports used to validate the correctness of records. (http://linuxfinances.info/info/workkinds.html)
UDDI	UDDI (Universal Description, Discovery, and Integration) is an XML-based registry for businesses worldwide to list themselves on the Internet. Its ultimate goal is to streamline online transactions by enabling companies to find one another on the Web and make their systems interoperable for e-commerce (whatis.com)
Virtual Memory	This is system memory that is simulated by the hard drive. When all the RAM is being used (for example if there are many programs open at the same time) the computer will swap data to the hard drive and back to give the impression that there is slightly more memory. (Google)
Virtual Private Network	A data network that uses the public telecommunications infrastructure, but maintains privacy through the use of a tunneling protocol and security procedures. A VPN gives a company the same capabilities as a system of owned or leased lines to which that

	company has exclusive access. However, costs are much lower because the VPN uses the shared public infrastructure rather than exclusive line access. (Google)
Watchdog/Heartbeat Line	a periodic signal generated by hardware or software to indicate that it is still running. (thefreedictionary.com)
Web Server	A computer, including software package, that provides a specific kind of service to client software running on other computers. More specifically, a server is a computer that manages and shares web based applications accessible anytime from any computer connected to the Internet. (Google)
Whiteboards	The electronic equivalent of chalk and blackboard, but between remote users. Whiteboard systems allow network participants to simultaneously view one or more users drawing on an on-screen blackboard or running an application. This is not the same as application sharing where two or more users can interactively work in the application. Only one user is actually running the application from his or her computer. In many desktop systems, the application is not viewable interactively. A copy of the current application window is pasted into the whiteboard, which then becomes a static image for interactive annotation (thefreedictionary.com)
Workflow Management	The automatic routing of documents to the users responsible for working on them. (thefreedictionary.com)
Workflow Systems	use group support software for scheduling, routing, and monitoring specific tasks throughout an organization. (Google)
XML	Extensible Markup Language – a programming meta-language that allows web developers to create customized tags that will organize and deliver content efficiently and thus expands the amount and kinds of information that can be provided about the data held in documents
XSLT	eXtensible Stylesheet Language Transformations: XSLT is a standard subset language of XML designed to allow one XML data structure to be transformed into another. For example, XML files can be transformed into HTML (i.e. standard Web pages.)
Zero Administration	An umbrella term for improved network administration functions in Windows products. (thefreedictionary.com)