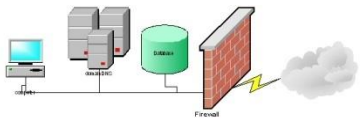
5. Maintenance policy

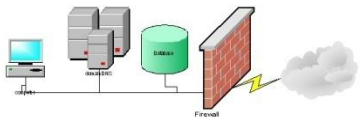
- 5.1 System maintenance ethic
- 5.2 Naming policy
- 5.3 Disaster recovery
- 5.4 Change management
- 5.5 IT security policy



5.1 System maintenance ethic

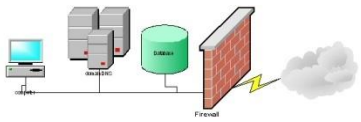
Ethics are the principles of conduct that govern a group of people. *Morals* are a proclamation of what is right and good.

People should understand the rules under which they are living.



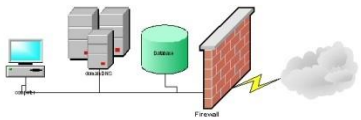
System Administrator's Code of Ethics

The League of Professional System Administrators is pleased to announce that we are co-branding the System Administrator's Code of Ethics together with the USENIX Association.



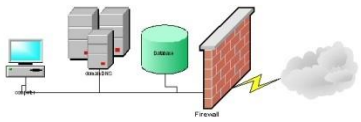
THE SYSTEM ADMINISTRATORS' CODE OF ETHICS

We as professional System Administrators do hereby commit ourselves to the highest standards of ethical and professional conduct, and agree to be guided by this code of ethics, and encourage every System Administrator to do the same.



System maintenance ethic

- Some users need privileged access to do their jobs.The ability to write and debug device drivers, install sw for more than just yourself and perform many other tasks all require root or administrator access. Organizations need special codes of conduct for these people.
  - Professional codes of conduct
  - User codes of conduct
  - Privileged access codes of conduct

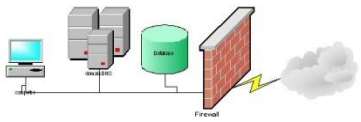


The system administrator

Has to know the relevant law and rules:

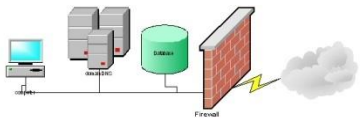
- Data security,
- E- commerce,
- copyrights
- Certificates and standards,

People with privileged access should sign a statement saying that they have read the code of conduct for privileged users and they sould be given a copy of it for their files.



General expectations

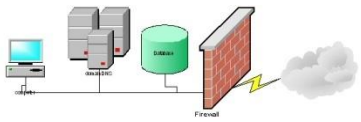
- Naming policy
- Security and reliability-policy
- Disaster recovery
- Modification handling
- Service modification



5.2 Naming-policy

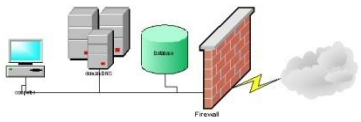
What is namespace?

- *namespace*: A **namespace** is an abstract container or environment created to hold a logical grouping of unique identifiers or symbols. In an operating system, an example of namespace is a directory.
- As a rule, names in a namespace cannot have more than one meaning, that is, two or more things cannot share the same name.



Naming-policy

- A namespace is also called a context, as the valid meaning of a name can change depending on what namespace applies.
- Names in it can represent objects as well as concept, whether it is a natural or ethnic language, a constructed language, the technical terminology of a profession, a dialect, a sociolect, or an artificial language (e.g., a programming language).

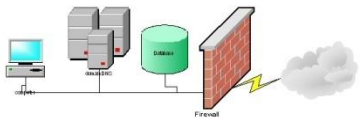


Concrete and abstract namespaces

- abstract namespace:
  coherent names
  - „account” types
  - List of service names

- concrete namespace:

  - List of „user ID”
  - Printer identifiers
  - Servers indentifiers
  - Ethernet network identifiers



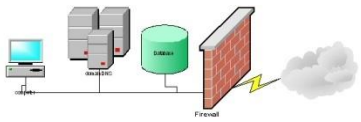
Flat and hierarchical namespaces

Flat:

- The units of namespace have only one representation.

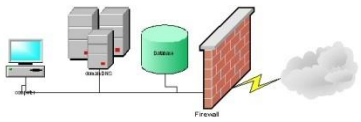
Hierarchical :

- Contains a sort of containers (eg. directory: in one directory not allowed to be two same names, but in two different directories can be)



Naming-policy

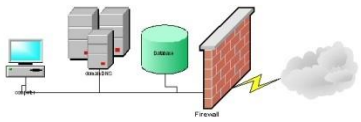
- The larger and more sophisticated an enviroment becomes, the more important it is that namespaces are managed formally.
- The faulty namespace can cause a piles of data.



Naming-policy

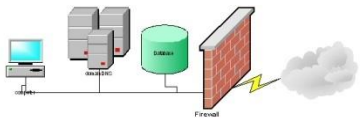
It needs

- namespace-policy
- namespace procedures
- (centralized) namespace management



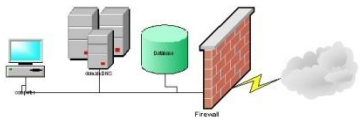
Naming-policy

- Namespaces should be controlled by policies more than they are controlled by any technological system.
- The larger your SA team is, the more importatnt it is for these to be written policies.
  - mandatory recommendations (eg. naming, life time, expitarion)
  - Mandatory procedures (for creation, for modification and for delete)
  - management (centralized -- non centralized)



Naming-policy extension

- *Naming policy*
- *Longevity policy*
- *Scope policy*
- *Consistency policy*
- *Reuse policy*
- *Protection policy*

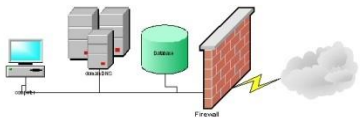


Naming-policy

- What names are permitted?
- What names are not permitted?
- How are names selected?
- How are collisions resolved?

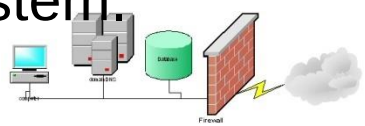
One needs rules for what names can go into a namespace.

  - Technology rules, eg. Unix login ID can be only alphanumeric + a limited number of symbols
  - Corporate rules, eg. login IDs shouldn't be offensive however that may be defined
  - standards, eg. RFC 1123



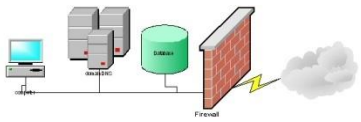
RFC 1123: Host Names and Numbers

- The definition of a host name is defined in rfc 952, but modified by rfc 1035, rfc 1123 and rfc 2181.
- This RFC is an official specification for the Internet community. It incorporates by reference, amends, corrects, and supplements the primary protocol standards documents relating to hosts.
- should a label have minimum of one alphanumeric character or two
- Host software MUST handle host names of up to 63 characters and SHOULD handle host names of up to 255 characters.
- Whenever a user inputs the identity of an Internet host, it SHOULD be possible to enter either (1) a host name or (2) an IPv4 address in dotted-decimal ("#.#.#.#") form or (3) an IPv6 address as groups of 4 hexadecimal characters with colon separators. The host SHOULD check the string syntactically for an IPv4 or IPv6 number before looking it up in the Domain Name System.



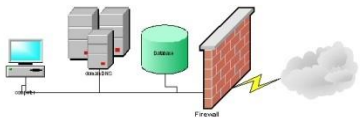
Methodes of selecting names

- Formula
- Theme
- Functional
- „No method”



Methodes of selecting names

- Formula :
  Names fit a stict formula
  eg: pc + 4 digit, login name: first six letters of last name + first initial + n digit identifier number
- Theme :
  All names fit a theme, such as naming all servers after planets (and using planet names from science fiction when you run out of real planet names)
- Functional :
  names have functions (admin, secretary, guest)
  hostnames that reflect the duties of the machine (dns, cpuserver12, web001)
  disk partitions that reflect the project for which they store data (/finance, /development, /contracts)
- „No method” :
  Sometimes the formula is no formula. Everyone picks what they want. Conflicts and collisions are resolved by first come, first-serve policies.

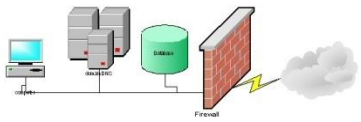


Typical categories

- User namespace
- Picture namespace
- Form namespace
- Category namespace
- Help namespace
- Wiki namespace

etc.

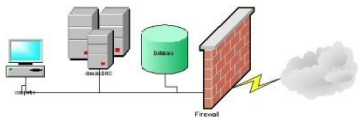
To summarize: „main” namespace



Namespace schema

namespace schema

- a schema-type definition
- It contains only names and definitions which we use in our system
- We can refer to definitons form other standard namespaces

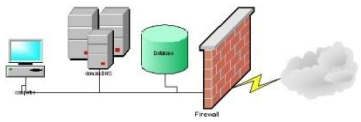


Application profile

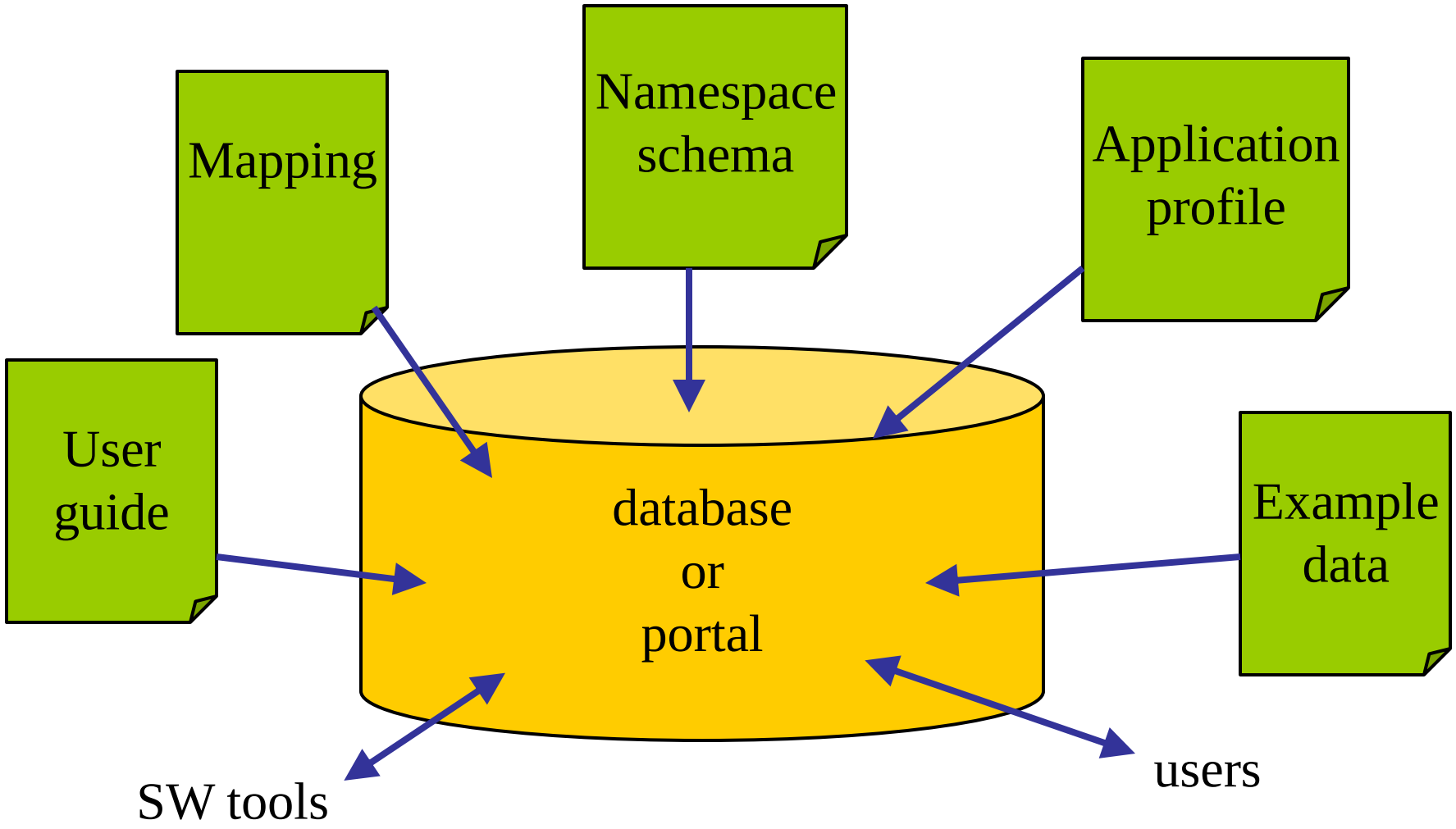
application profile

- Apply a schema-type
- Define the used name

- Name elements-usage directives
- Reuse policy
- Combine more namespace in an application profile
- Contain a scemantic defintion
- Give a name element usage authorisaton

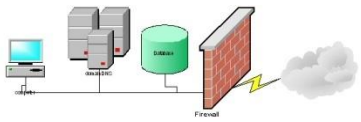


Schema registry



Schema registry

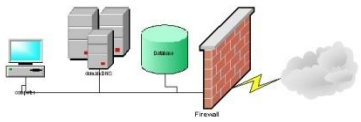
- Store and access solution of namespace-elements, -schemas and application profiles
  - federal name element definitions
  - name element - utilization rules
  - comments



Schema registry

Contain

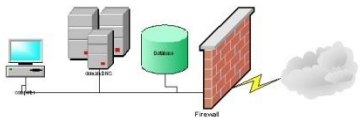
- namespce-schemas
- Mapping
- Application profiles
- schema-comments
- guidelines
- Controlled dictionary, thesaurus



5.3 Disaster recovery

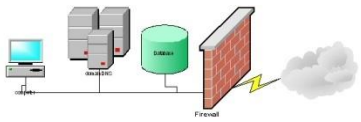
- Catastrophe plan:

  A disaster recovery plan looks at what disasters could hit the company and sets out a plan for responding to those disasters. Disaster recovery planning also involves implementing ways to mitigate potential disasters and making preparations to enable quick restoration of key services. It also identifies what those key services are and how quickly they need to be restored.



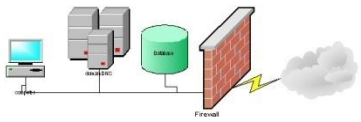
Disaster recovery

- What is „IT catastrophe”?
- Risk summing up and handling
- Legal requirements
- Preparation
- Organizational effects
- Media connections



What is „IT disaster”?

A disaster is a catastrophic event that causes a massive outage affecting an entire building or site. It can be a natural disaster such as an eartquake, hurricane, tornado, plague, lightning strike, fire or flood. Or it can be a man-made disaster such as a bomb, a massive loos of power, or the ever increasing problem of idiots with backhoes. It is anything that has a significant inpact on your company’s ability to do business.

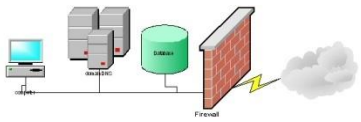


Risk analysis

A risk analysis involves determining what disasters the company is at risk of experiencing and what the chances are of those disasters occurring. The risk analyst than looks at the likely cost to the company if a disaster of each type occured. The company than uses this information to determine approximately how much money is reasonable to spend on trying to mitigate the effects of each type of disaster.

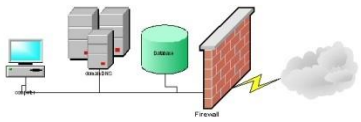
<u>The approximate budget for risk mitigation is:</u>

(probable cost of disaster-probable cost of after mitigation) x risk of disaster



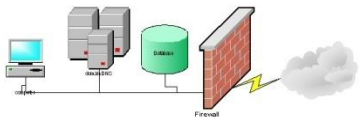
Risk handling

- Define risk handling level!
- The most important aspect of disaster planning is understanding what services are the most critical to the business and what the time constraints are for restoring those services.
- The disaster planner also needs to know what disaster are likely to happen and how costly they would be before he can complete a risk analysis and determine the compny’s budget for limiting the demage.



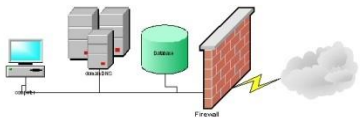
Defence commensurable to risk

- The disaster planner also needs to know what disaster are likely to happen and how costly they would be before he can complete a risk analysis and determine the company’s budget for limiting the demage.



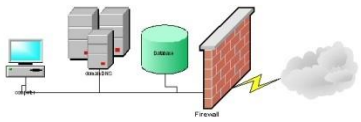
Legal obligations

- Commercial companies have legal obligations to their vendors customers and ashareholders in terms of meeting contract obligations.
- Public companies have to abide by the laws of the stock markets on which they are treated.
- The legal department should be able to elaborate on these obligations.
- Restoring individual parts of the company to working order before th entire infrasructure is operational requires an indepth understanding of what pieces infrastructure those parts relay on and a detailed plan of how to get them working.



5.4 Change handling

Change management is the process that ensures effective planning, implementation and postevent analysis of changes made to a system. It means that changes are well documented, have a back-out plan and are reproducible. Change management yields an audit trial that can be used to determine what was done when and why.

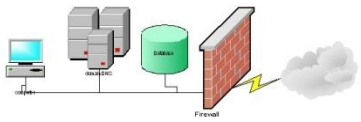


Change handling

Change management is one of the core processes of a mature system administration team.

Change management is a valuable tool that is used at mature sites to increase the reliability of the site.

Change management also helps with debugging problems because changes are tracked and can be reviewed when a problem arises.



Tipical change handling procedure

1: Preparation

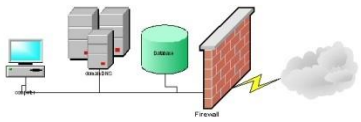
- **Necessity of change**
- **Change handling project plan**
- **Surveying communication tasks**
- **Define partners, participants**
- **Define fullfilment criterias**
- **Data collection**
- **Measuring readiness**
- **Commit concerned**

2: Execution

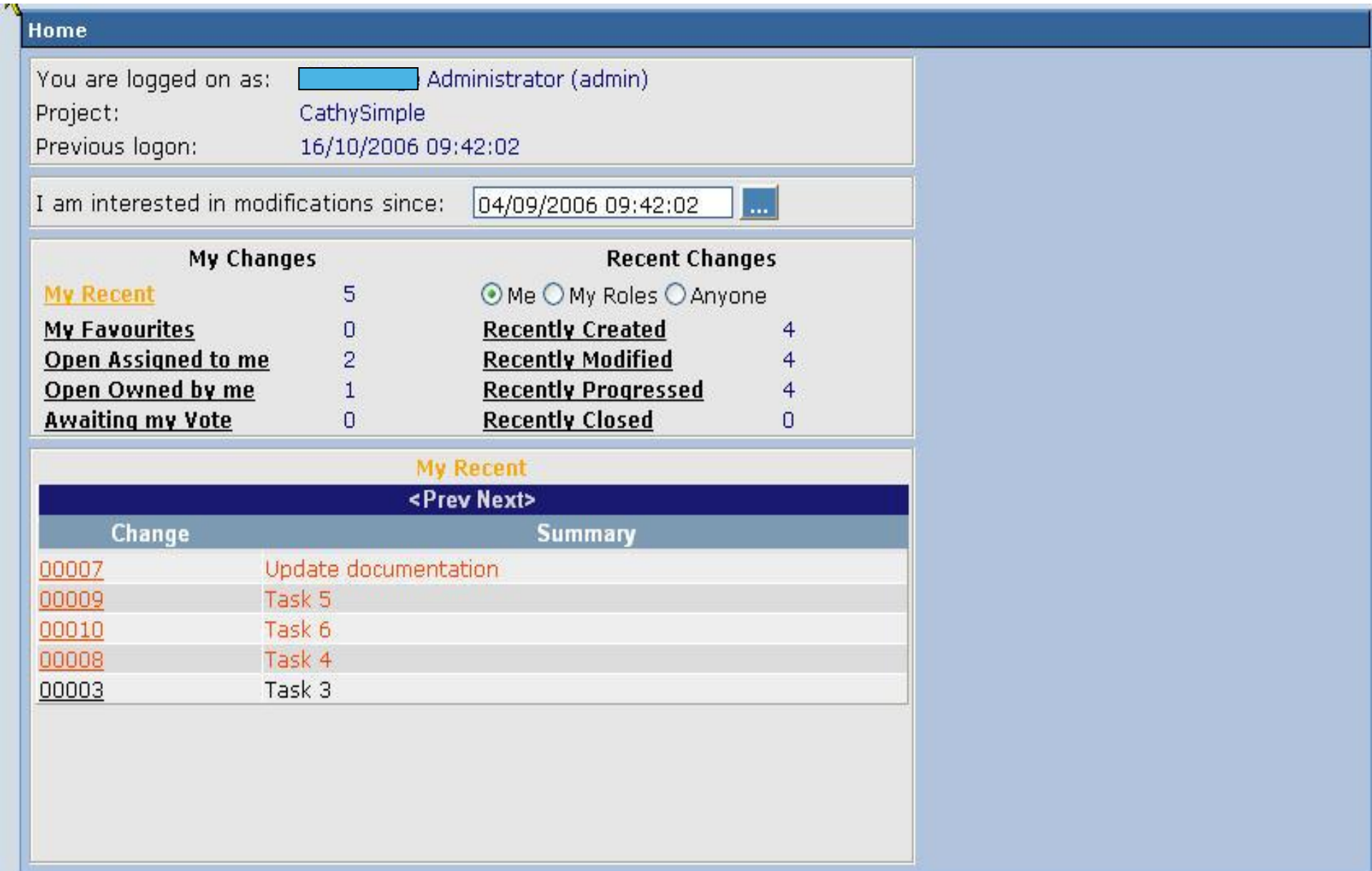
- **Advancement monitoring**
- **Reaction to opposition**
- **Draw a lesson**
- **Replanning**
- **Communication**
- **Documentation**
- **Training**

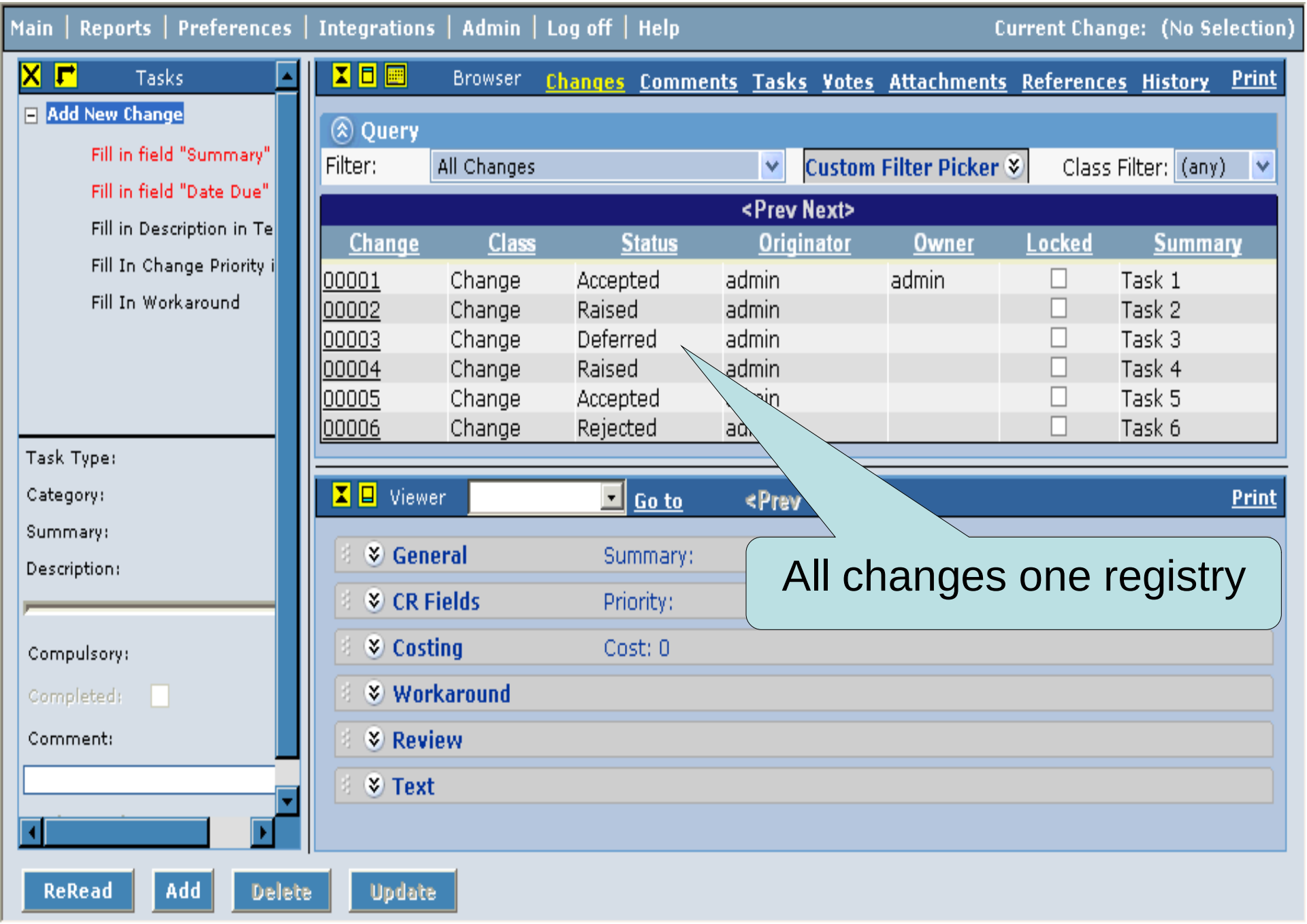
3: Edification

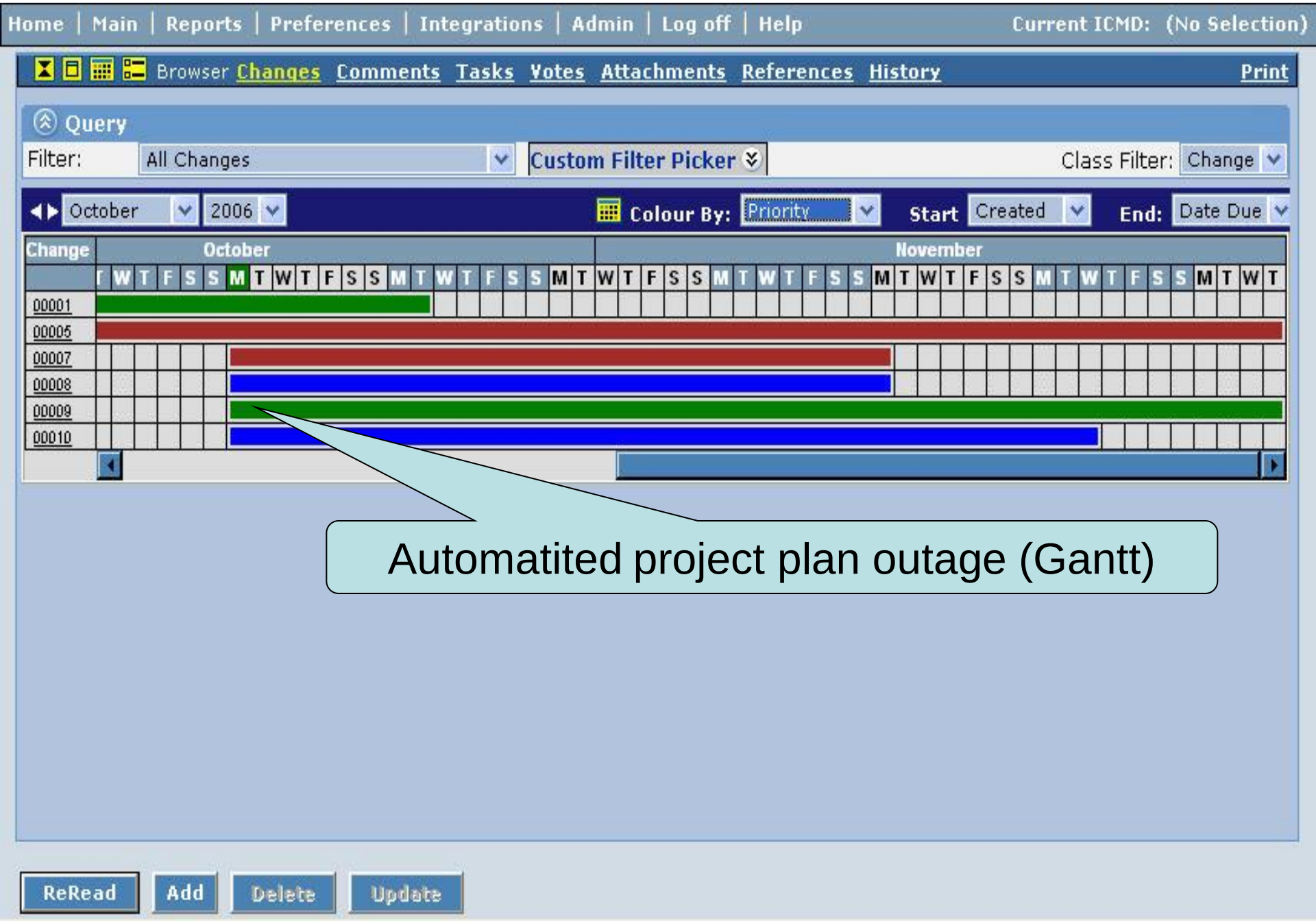
- **Institutionalized the results**
- **Record in policies, procedures, trainings, etc.**
- **Rules from edifications**
- **Communicate the successes**

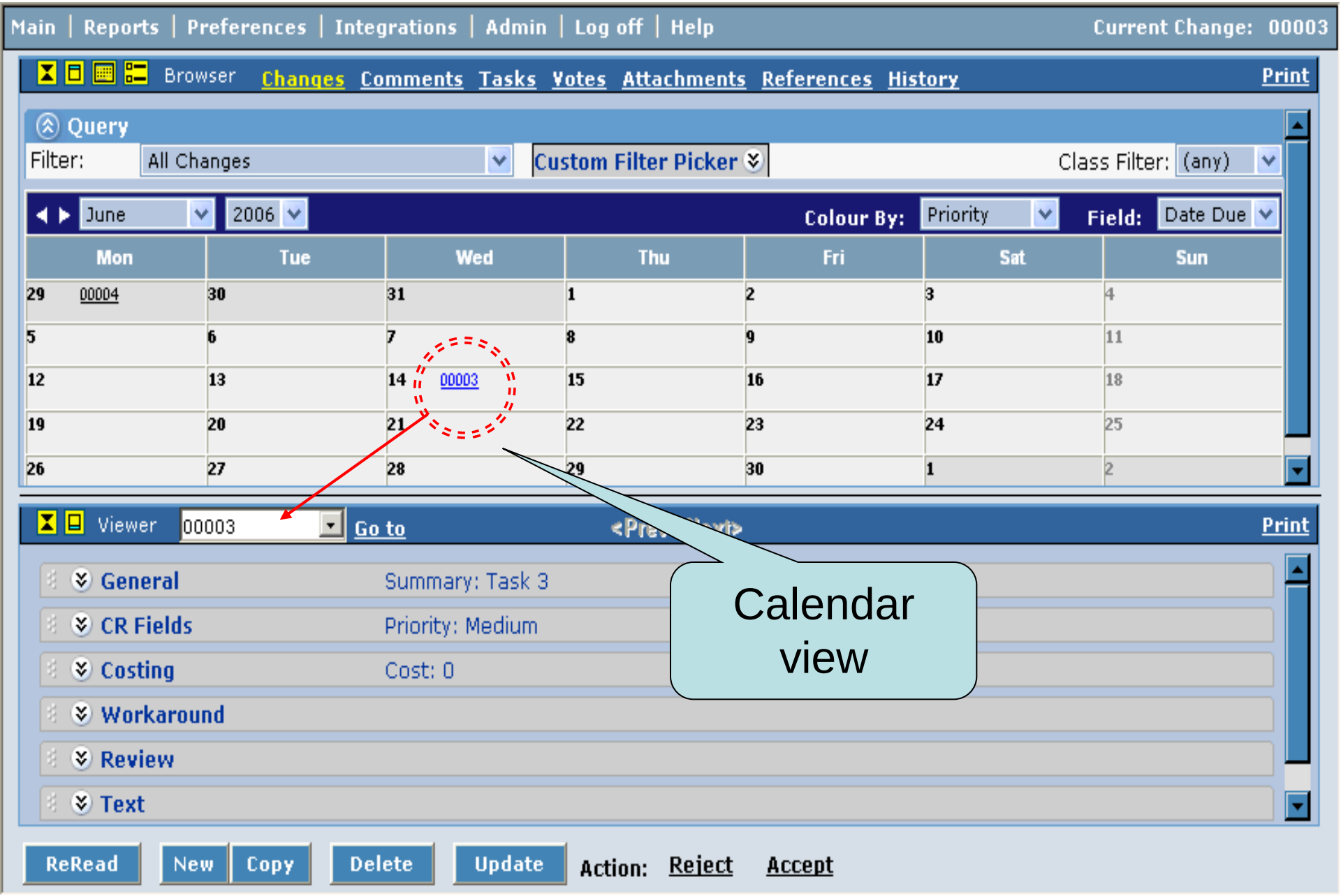


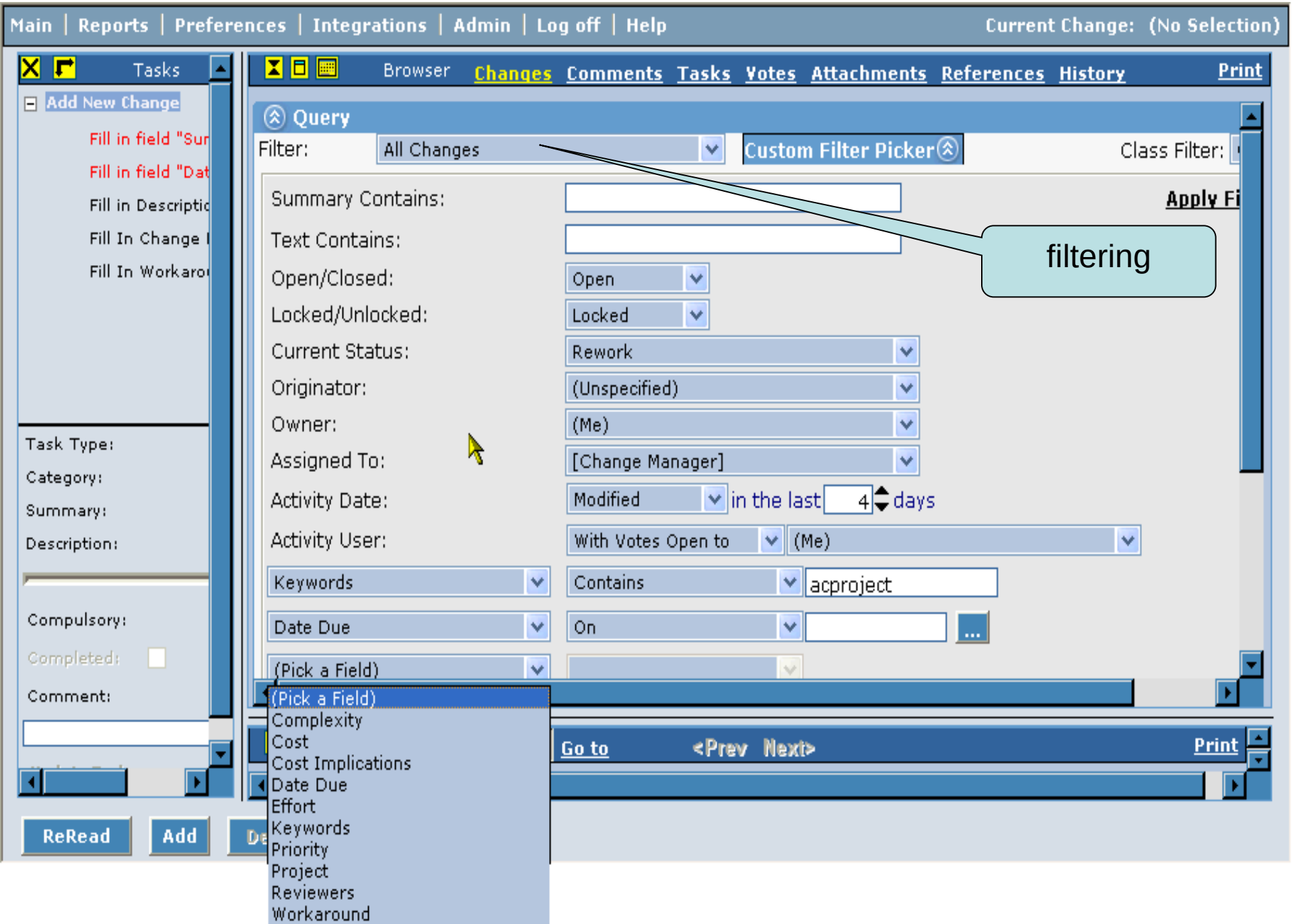
Example: simple change management SW

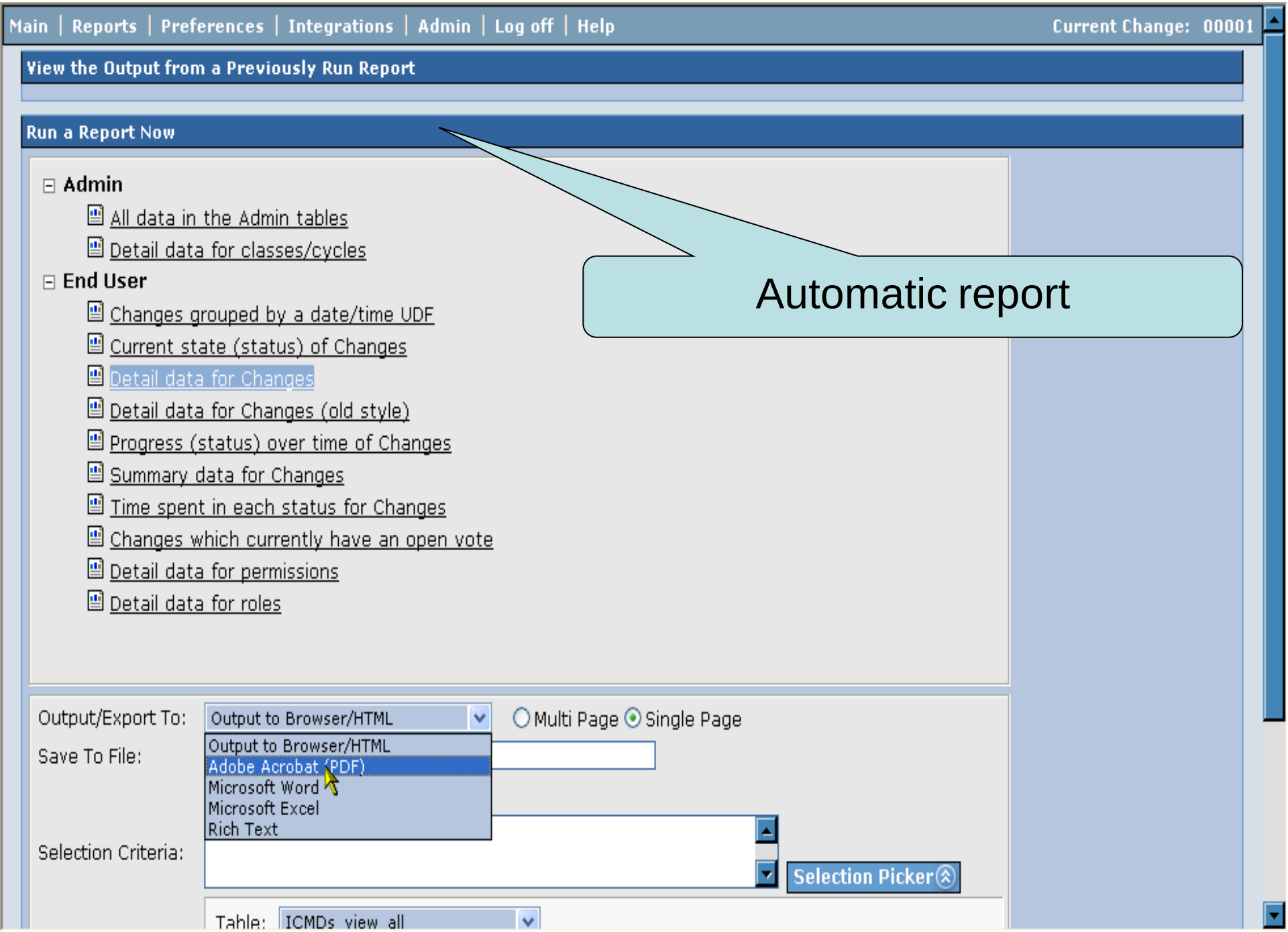


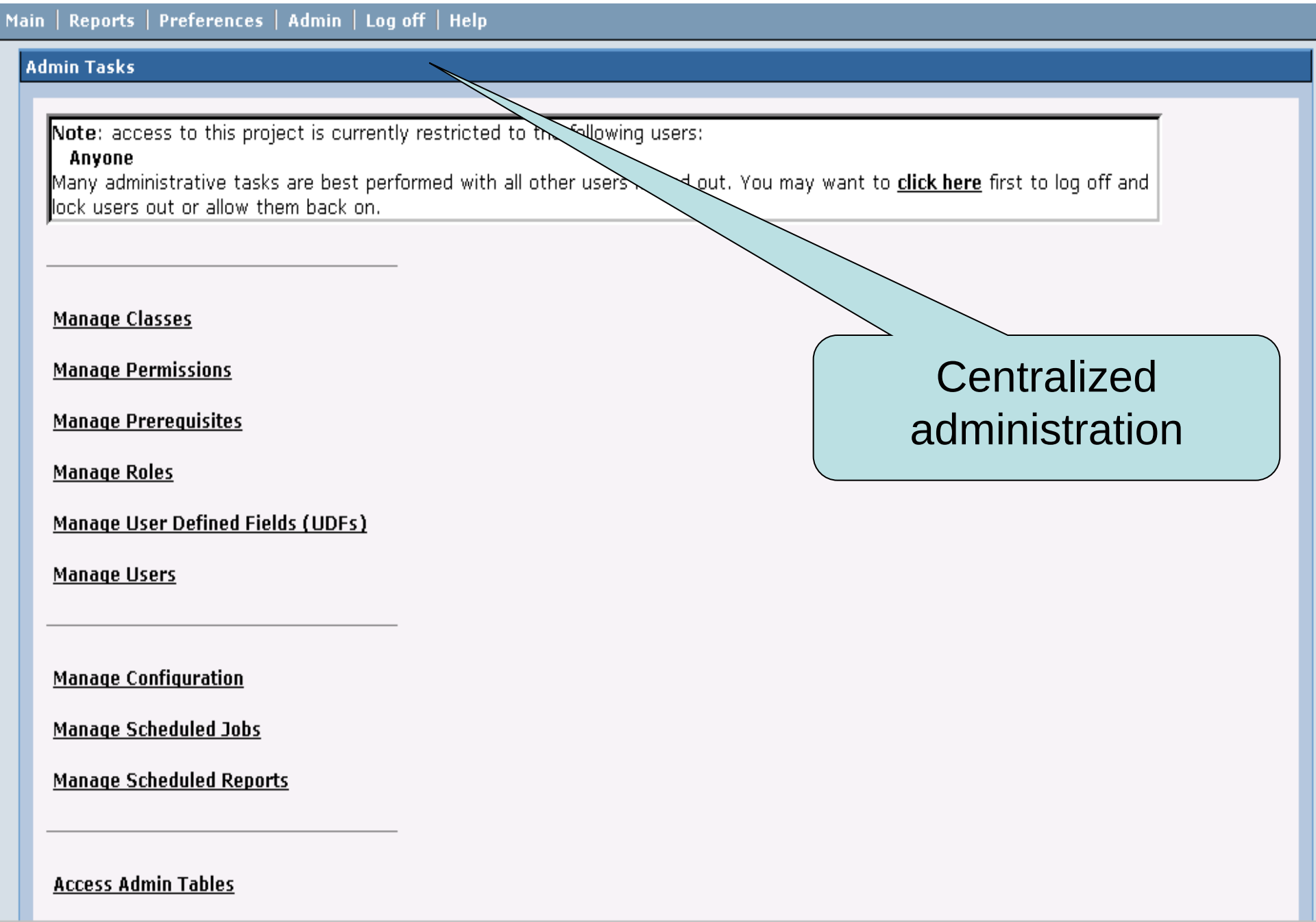

Main | Reports | Preferences | Integrations | Admin | Log off | Help
Current Change: (No Selection)
Tasks
Add New Change
Fill in field "Summary"
Fill in field "Date Due"
Fill in Description in Te
Fill In Change Priority i
Fill In Workaround
Task Type:
Category:
Summary:
Description:
Compulsory:
Completed:
Comment:
Browser
Changes
Comments
Tasks
Votes
Attachments
References
History
Print
Query
Filter:
All Changes
Custom Filter Picker
Class Filter:
(any)
<Prev Next>
Change
Class
Status
Originator
Owner
Locked
Summary
00001 Change Accepted admin admin Task 1
00002 Change Raised admin Task 2
00003 Change Deferred admin Task 3
00004 Change Raised admin Task 4
00005 Change Accepted Task 5
00006 Change Rejected Task 6
Viewer
Go to
<Prev
Print
General
Summary:
CR Fields
Priority:
Costing
Cost: 0
Workaround
Review
Text
All changes one registry
ReRead
Add
Delete
Update

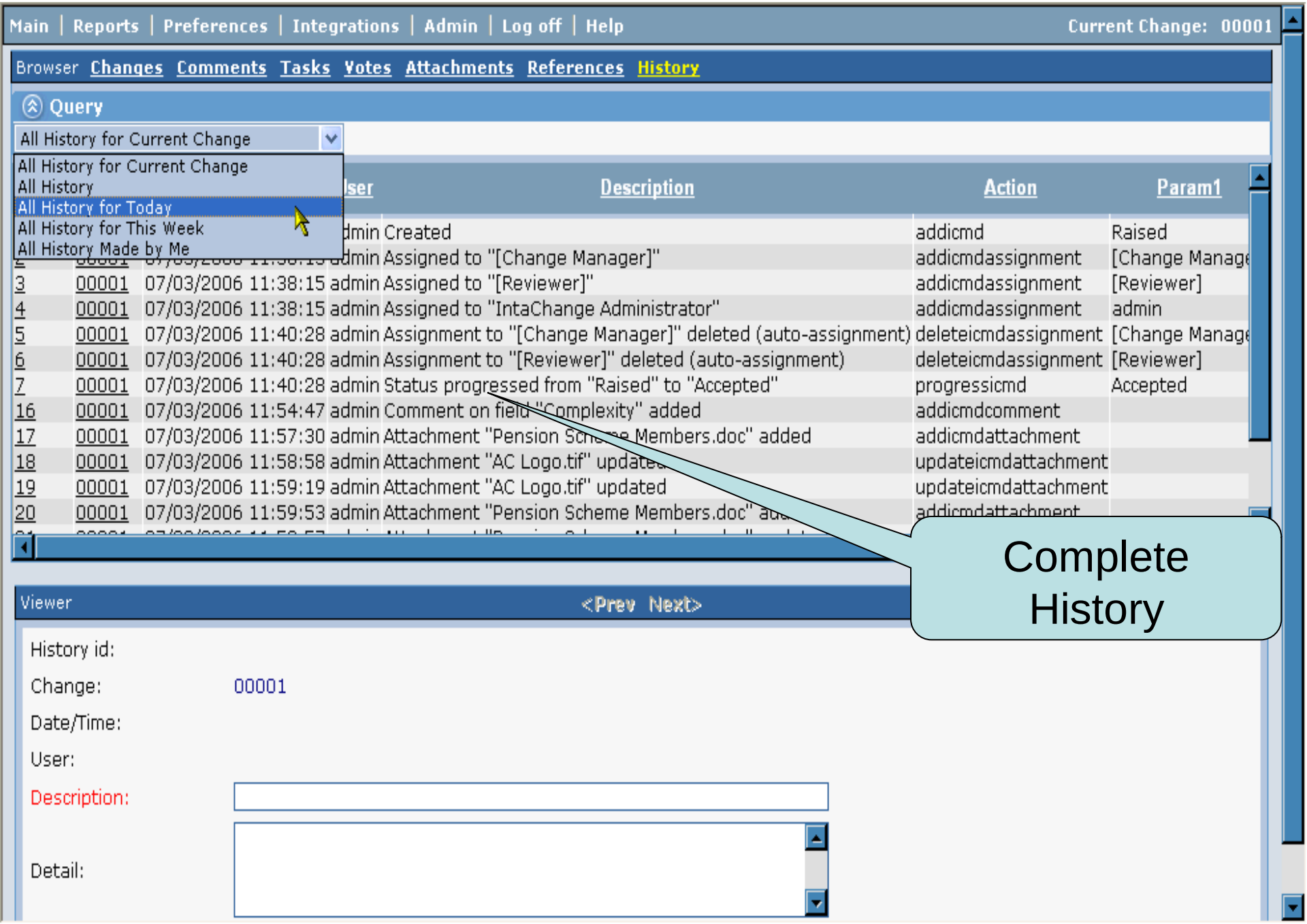

Home | Main | Reports | Preferences | Integrations | Admin | Log off | Help
Current ICMD: (No Selection)
Browser Changes Comments Tasks Votes Attachments References History
Print
Query
Filter: All Changes
Custom Filter Picker
Class Filter: Change
October 2006
Colour By: Priority
Start Created
End: Date Due
Change
October
November
00001
00005
00007
00008
00009
00010
Automatited project plan outage (Gantt)
ReRead
Add
Delete
Update


Main | Reports | Preferences | Integrations | Admin | Log off | Help
Current Change: 00003
Browser Changes Comments Tasks Votes Attachments References History
Print
Query
Filter: All Changes
Custom Filter Picker
Class Filter: (any)
June 2006
Colour By: Priority
Field: Date Due
Mon Tue Wed Thu Fri Sat Sun
29 00004 30 31 1 2 3 4
5 6 7 8 9 10 11
12 13 14 00003 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 1 2
Viewer 00003
Go to
Print
General Summary: Task 3
CR Fields Priority: Medium
Costing Cost: 0
Workaround
Review
Text
ReRead
New
Copy
Delete
Update
Action: Reject Accept
Calendar view


Main | Reports | Preferences | Integrations | Admin | Log off | Help
Current Change: (No Selection)
Tasks
Add New Change
Fill in field "Sur
Fill in field "Dat
Fill in Descriptic
Fill In Change
Fill In Workaro
Task Type:
Category:
Summary:
Description:
Compulsory:
Completed:
Comment:
ReRead
Add
Browser
Changes
Comments
Tasks
Votes
Attachments
References
History
Print
Query
Filter:
All Changes
Custom Filter Picker
Class Filter:
Summary Contains:
Apply Fi
Text Contains:
Open/Closed:
Open
Locked/Unlocked:
Locked
Current Status:
Rework
Originator:
(Unspecified)
Owner:
(Me)
Assigned To:
[Change Manager]
Activity Date:
Modified
in the last
4
days
Activity User:
With Votes Open to
(Me)
Keywords
Contains
acproject
Date Due
On
(Pick a Field)
(Pick a Field)
Complexity
Cost
Cost Implications
Date Due
Effort
Keywords
Priority
Project
Reviewers
Workaround
Go to
<Prev
Next>
Print
filtering

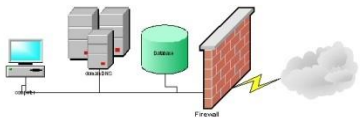

Main | Reports | Preferences | Integrations | Admin | Log off | Help
Current Change: 00001
View the Output from a Previously Run Report
Run a Report Now
Admin
All data in the Admin tables
Detail data for classes/cycles
End User
Changes grouped by a date/time UDF
Current state (status) of Changes
Detail data for Changes
Detail data for Changes (old style)
Progress (status) over time of Changes
Summary data for Changes
Time spent in each status for Changes
Changes which currently have an open vote
Detail data for permissions
Detail data for roles
Automatic report
Output/Export To:
Output to Browser/HTML
Multi Page
Single Page
Save To File:
Output to Browser/HTML
Adobe Acrobat (PDF)
Microsoft Word
Microsoft Excel
Rich Text
Selection Criteria:
Selection Picker
Table:
ICMDs view all


Main | Reports | Preferences | Admin | Log off | Help
Admin Tasks
Note: access to this project is currently restricted to th following users:
Anyone
Many administrative tasks are best performed with all other users d out. You may want to click here first to log off and lock users out or allow them back on.
Manage Classes
Manage Permissions
Manage Prerequisites
Manage Roles
Manage User Defined Fields (UDFs)
Manage Users
Manage Configuration
Manage Scheduled Jobs
Manage Scheduled Reports
Access Admin Tables
Centralized administration

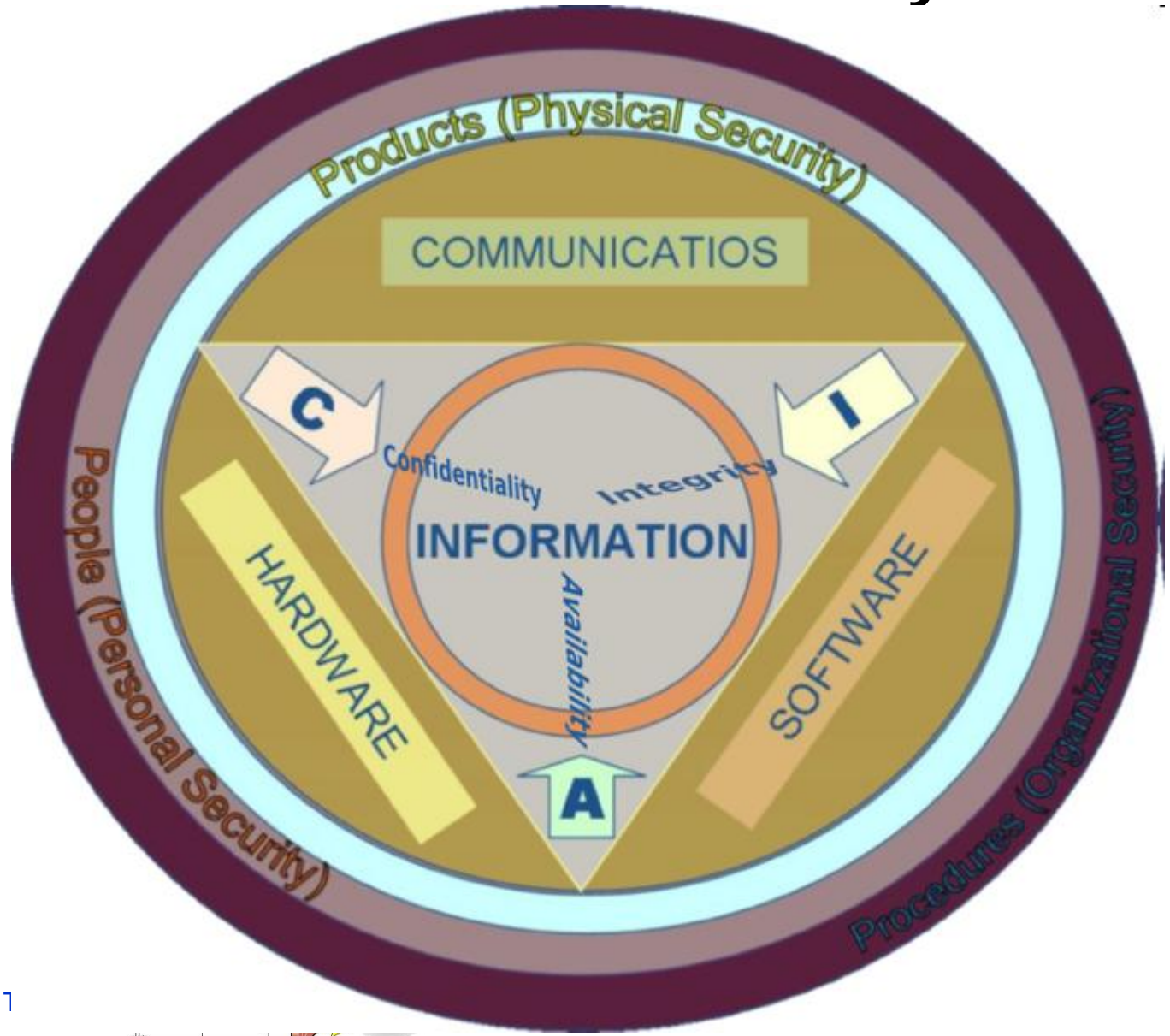

Main | Reports | Preferences | Integrations | Admin | Log off | Help
Current Change: 00001
Browser Changes Comments Tasks Votes Attachments References History
Query
All History for Current Change
All History for Current Change
All History
All History for Today
All History for This Week
All History Made by Me
User
Description
Action
Param1
3 00001 07/03/2006 11:38:15 admin Assigned to "[Reviewer]" addicmdassignment [Reviewer]
4 00001 07/03/2006 11:38:15 admin Assigned to "IntaChange Administrator" addicmdassignment admin
5 00001 07/03/2006 11:40:28 admin Assignment to "[Change Manager]" deleted (auto-assignment) deleteicmdassignment
6 00001 07/03/2006 11:40:28 admin Assignment to "[Reviewer]" deleted (auto-assignment) deleteicmdassignment [Reviewer]
7 00001 07/03/2006 11:40:28 admin Status progressed from "Raised" to "Accepted" progressicmd Accepted
16 00001 07/03/2006 11:54:47 admin Comment on field "Complexity" added addicmdcomment
17 00001 07/03/2006 11:57:30 admin Attachment "Pension Members.doc" added addicmdattachment
18 00001 07/03/2006 11:58:58 admin Attachment "AC Logo.tif" updateicmdattachment
19 00001 07/03/2006 11:59:19 admin Attachment "AC Logo.tif" updated updateicmdattachment
20 00001 07/03/2006 11:59:53 admin Attachment "Pension Scheme Members.doc"
Complete History
Viewer
<Prev Next>
History id:
Change: 00001
Date/Time:
User:
Description:
Detail:

5.5 IT security policy

- IT maintenance security regulation
- Information security roles
- Maintenance security
- Internet and e-mail security
- Logical access handling
- Infrastructure security
- Incident handling

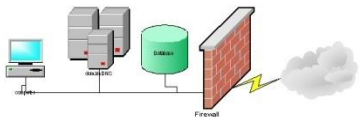


Information security



Information security

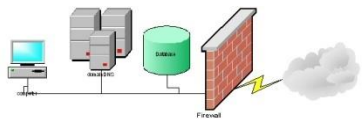
- **Confidentiality:** "ensuring that information is accessible only to those authorized to have access"
- **Integrity**: is consistency of actions, values, methods, measures, principles, expectations and outcome.
- **Availability:** availability is the proportion of time a system is in a functioning condition.



Information security

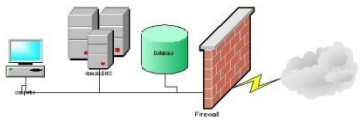
- Security =
  - Confidentiality +
  - Integrity +
  - Availability

- **Information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

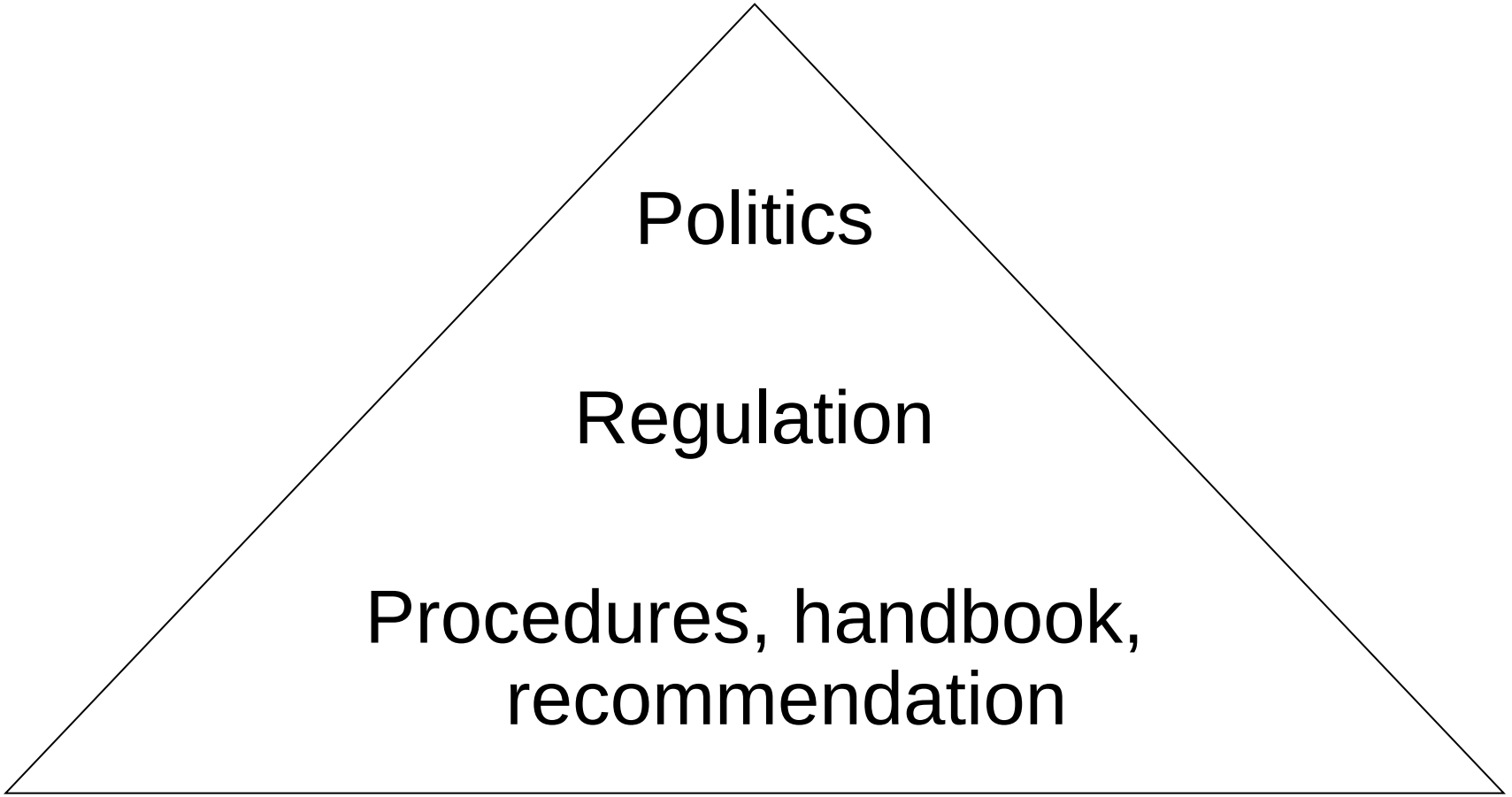


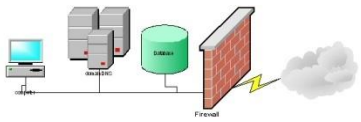
Information security

- Standards
  - MSZ ISO17799, ISO17799:2005, ISO27002 –
  - MSZ ISO/IEC 27001, ISO27001 –C
  - Cobit v4 – Control Objectives for Information and Related Technology



Regulation

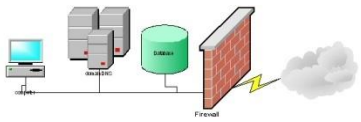

Politics
Regulation
Procedures, handbook,
recommendation



Maintenance security

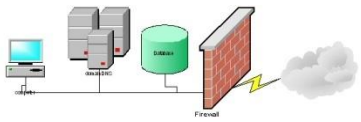
- Document the maintenance procedures

- Typical maintenance security tasks
  - Storage and Archiving
  - Logging
  - Security updates
  - Data medium handling



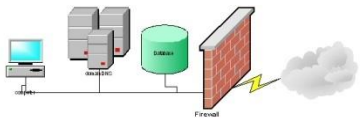
Maintenance security

- Periodical Storage and conservation
  - define acceptable data loss windows
- Data owner responsibility
- Periodical testing
- Storage outsource



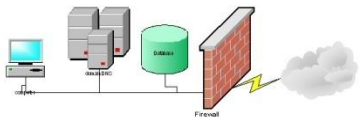
Maintenance security - Logging

- What do we collect?
  - All data which can be important at a security event
  - Confidential data canot be stored (eg. psw)
  - Log files size!



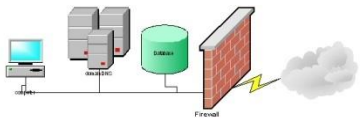
Maintenance security - Logging

- What do we log?
  - Event type
  - Date
  - User identifier
  - IP address



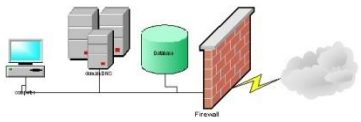
Maintenance security– security updates

- Update
  - SW or security
- The SWs contain security leak
- Solution: periodic security update
- Critical: the period of the update
  - Zero-day attack
- Critical, non critical patch
- In accordance with change management



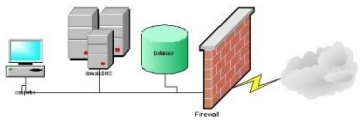
Maintenance security– security updates

- Manual or automatic
- Patch management procedure
  - Monitor new patches
    - From authentic source
  - Risk analysis under critical level
  - Risk minimalization
    - Apply patch



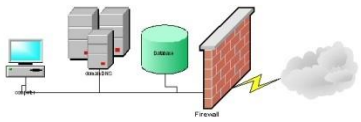
Maintenance security – security updates

- Patch management procedure (cont.)
  - Testing
    - Funcional
    - Security
    - Rollback plan
  - Apply in live system
  - Verification



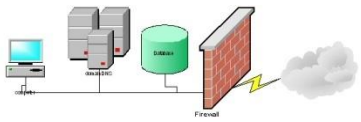
Maintenance security – Data medium handling

- Problem
  - Data leakage
- Changable/portable data medium handling
  - USB devices
  - CD/DVD
- Encryption
  - Store confidental data



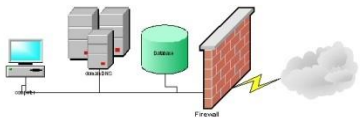
Maintenance security – Data medium handling

- Security destruction
  - DVD/CD
  - Back up storage
- Security handling of data media
- Security delivery of data media



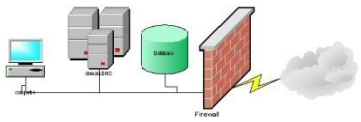
Internet security

- Internet, Intranet, Extranet
- Has to defend the internal IT infrastructure from public network segment
- Background security
  - firewalls,
  - IDS/IPS
- Access to outside connection only across permitted connections
  - Modems and wifi devices



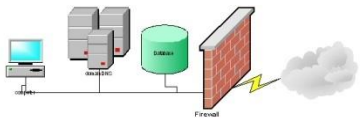
Internet security

- Protocols
  - HTTPS, SSL, SSH, SFTP,SNMPv3
  - FTP, Telnet, SNMPv1, NFS
- Web-server
  - Dedicated server in DMZ
- VPN (IPSec, SSL)
- Encryption



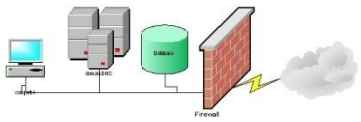
E-mail security

- e-mail messages are generally not encrypted;
- many Internet Service Providers (ISP) store copies of your e-mail messages on their mail servers before they are delivered. The backups of these can remain up to several months on their server, even if you delete them in your mailbox;
- fields and other information in the e-mail can often identify the sender, preventing anonymous communication.



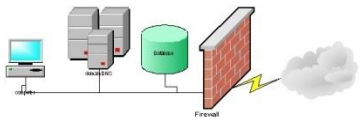
E-mail security

- Solutions - actions
  - Spam filtering
  - E-mail relaying
  - Antivirus gateway
  - End-user techniques
  - Trainig
  - Content filtering



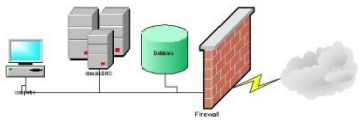
Logical access handling

Access control is the ability to permit or deny the use of a particular resource by a particular entity. Access control mechanisms can be used in managing physical resources (such as a movie theater, to which only ticketholders should be admitted), logical resources (a bank account, with a limited number of people authorized to make a withdrawal), or digital resources (for example, a private text document on a computer, which only certain users should be able to read).



Logical access handling

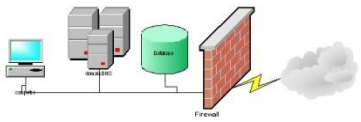
Identification and authentication (I&A) is the process of verifying that an identity is bound to the entity that asserts it. The I&A process assumes that there was an initial vetting of the identity, during which an authenticator was established. Subsequently, the entity asserts an identity together with an authenticator as a means for validation. The only requirements for the identifier is that it must be unique within its security domain.



Logical access handling

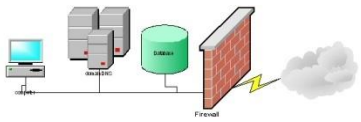
Authorization

- Authorization applies to subjects rather than to users (the association between a user and the subjects initially controlled by that user having been determined by I&A). Authorization determines what a subject can do on the system.



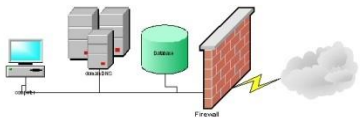
Logical access handling – handling password

- A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource
- **Design of the protected software:**
  - Not echoing the password on the display screen as it is being entered or obscuring it as it is typed by using asterisks (*) or bullets (•).
  - Allowing passwords of adequate length
  - Requiring users to re-enter their password after a period of inactivity
  - Requiring periodic password changes.
  - Requiring minimum or maximum password lengths.
  - Limiting the number of allowed failures within a given time period
  - Some systems require characters from various character classes in a password

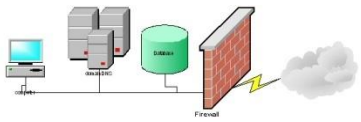


Incident management (ITIL)

The goal of Incident Management is to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 'Normal service operation' is defined here as service operation within Service Level Agreement (SLA) limits.



Incident management - Procedure



Incident handling

- Confirmity
  - MSZ ISO17799, ISO17799:2005, ISO27002
  - Cobit v4 – Control Objectives for Information and Related Technology
  - ITIL - Information Technology Infrastructure Library
  - NIST - National Institute for Standards and Technology