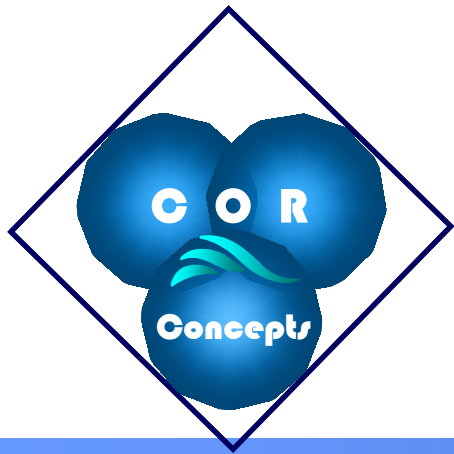


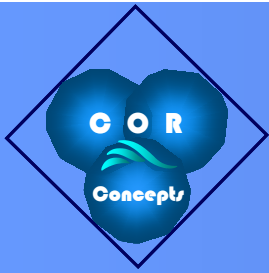


Gauteng Department of Sports Arts and Culture (DSAC)

Records Management workshop July 2012

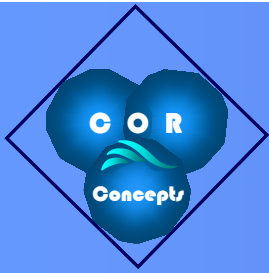
Paul Mullan

paulm@corconcepts.co.za



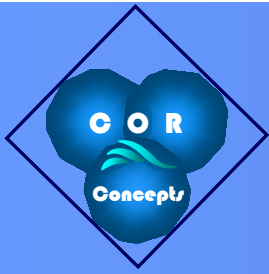
Agenda

- Understand the legislation as it pertains to e-mails and electronic documents
- Determining retention periods for e-mails
- Rules for determining which e-mails are records
- Rules for filing and storage of e-mail
- E-mail etiquette (How to create and use business e-mail)
- Policies and procedures impacting on e-mail
- E-mail archiving
- The role of IT in managing e-mail
- Other important considerations for the creation and management of electronic documents



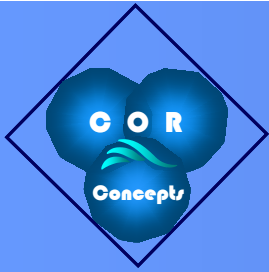
Rules and thoughts

- I will facilitate, stimulate thinking and provide guidance
- You MUST provide input regarding your situation:
 - Attitudes and philosophies to electronic documents and e-mail
 - Current practices in your organisations
 - Restrictions – things/resources holding you back
- It MUST work for your Dept. or organisation



Legal Framework

- The legislative universe
 - ECT Act
 - NARS Act
 - New Companies Act
 - Protection of personal information bill
 - Promotion of Access to Information (PAIA)
 - General & industry specific implications
- Impact of legislation on electronic records

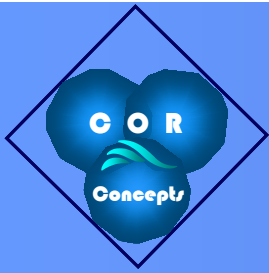


Government: Legislative Mandates

- The Constitution of the RSA
- The Public Service Act of 1994.
- The Labour Relations Act
- Public Finance Management Act – provides a regulatory framework for Financial Management in the Public Service

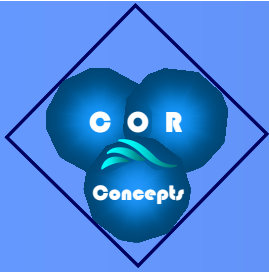
And

- National Archives and Records Services Act
- Promotion of Access to Information Act
- Promotion of Administrative Justice Act
- National Minimum Information Requirements (NMIR)
- Minimum Information Security Standard (MISS)
- Companies Act
- Others



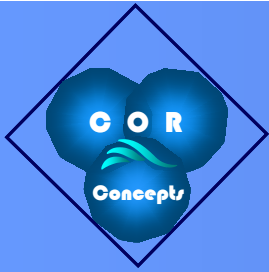
Public sector records

- Governed by the National Archives and Records Service Act, 1996 (NARS)
- Provinces to promulgate their own legislation (in alignment to NARS)
- Stems from the Constitution
- A public record is: A record created or received by a governmental body in pursuance of its activities, **regardless of form or medium.**



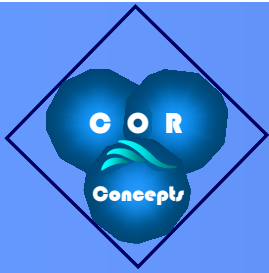
National Archives and Records Service of South Africa Act, 1996

- Section 13(2)(a)
 - No public record may be
 - transferred to an archives repository;
 - destroyed;
 - erased; or
 - otherwise disposed of
 - Without the written authorization of the National Archivist



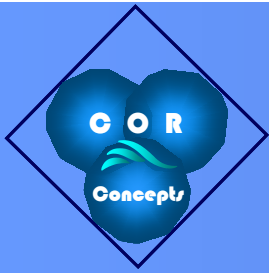
National Archives and Records Service of South Africa Act, 1996

- The National Archivist shall determine the conditions subject to which
 - electronic records systems shall be managed
 - records may be reproduced electronically
- Conditions contained in *Managing electronic records in governmental bodies: Policy Guidelines*



The law: National Archives requirements

- Formulate and implement a *records management policy* and related *records management procedures*
- Designate a *records manager* to take responsibility for records management in the office
- Attend *training sessions* offered or approved by NARS
- Compile and maintain *approved records classification system(s)* for paper-based and electronic records
- Manage electronic correspondence systems, e-mail and websites with an *Integrated Document and Records Management Solution*

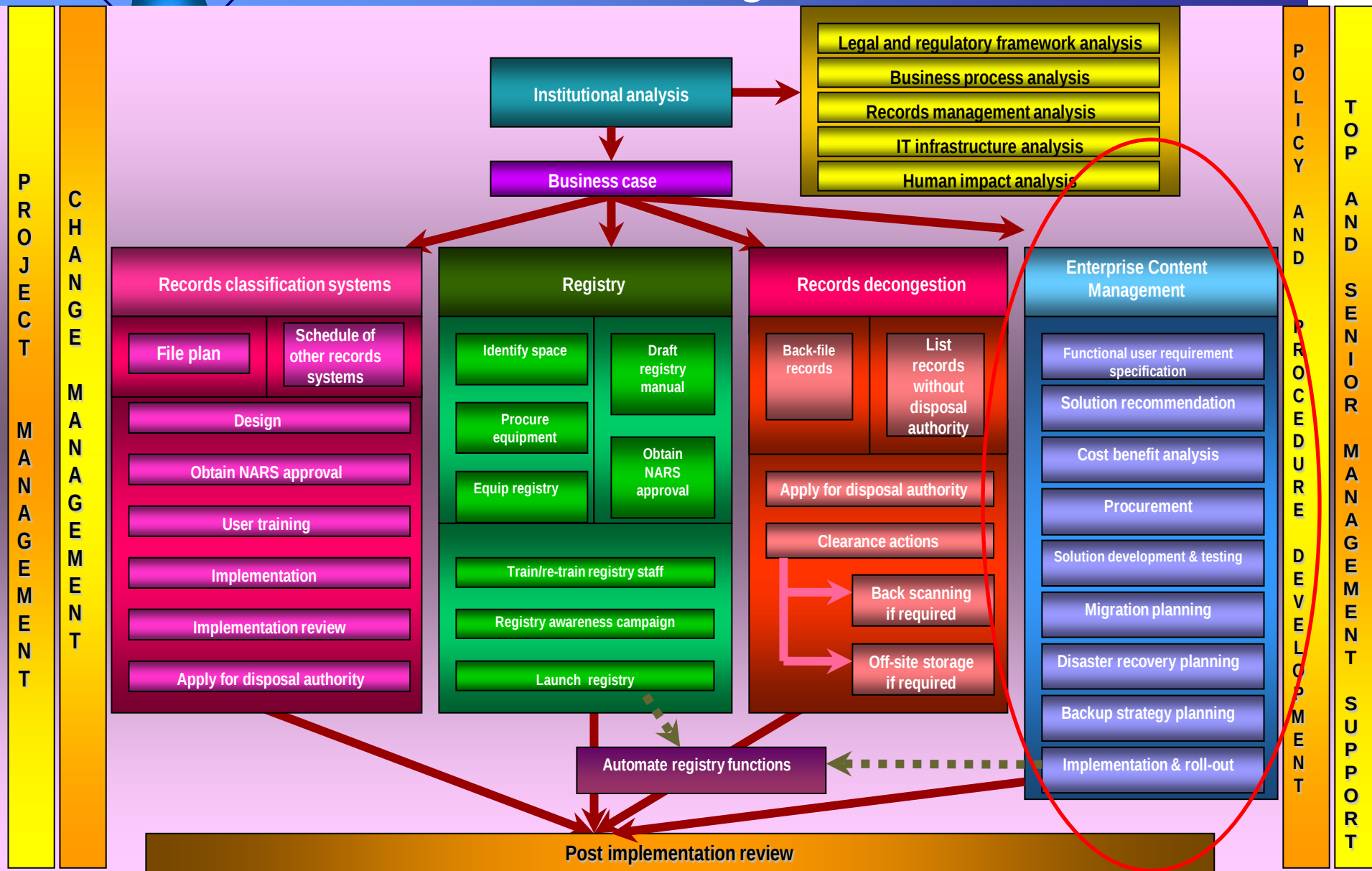


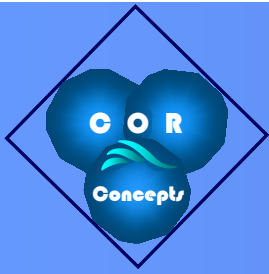
The law: National Archives requirements

- Create a retention schedule and implement *systematic disposal programmes* to reduce storage cost involved in storing records no longer required
- Keep all records in *safe custody*
- Inspect sub-offices to ensure that sound records management practices are followed
- Ensure that *staff are trained* to apply the proper procedures to facilitate sound management of records
- *Train creators of records* to allocate file reference numbers/subjects to records according to an approved classification system.
- Let's discuss the implications of these statements for electronic records and e-mails



NARS Records Management Improvement Programme

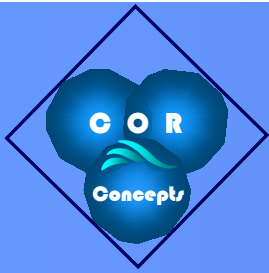




Related current and pending legislation

- New Companies Act
- ECT Act under review
- Promotion of Access to Information Act (PAIA)
- Protection of Personal Information Bill



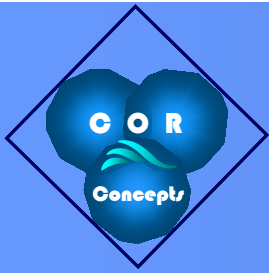


Protection of Personal Information Bill – Data Protection/Privacy

Information must be:

- obtained fairly and lawfully;
- used only for the specified purpose for which it was originally obtained;
- adequate, relevant and not excessive to purpose;
- accurate and up to date;
- accessible to the subject;
- kept secure; and
- destroyed after its purpose is completed.



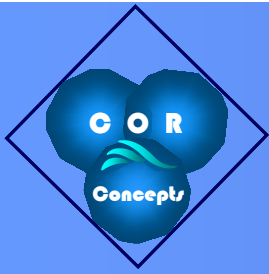


Promotion of Access to Information Act (PAIA)

Who must comply?

All so-called public and private bodies.

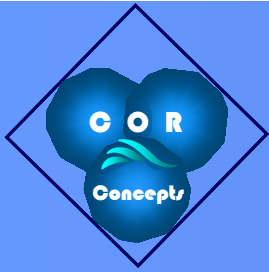
- A requester must be given access to any record of a private body if—
 - that record is required for the exercise or protection of any rights;
 - that person complies with the procedural requirements in this Act relating to a request for access to that record; and
 - access to that record is not refused in terms of any ground for refusal contemplated in



PAIA Compliance

All organisations must:

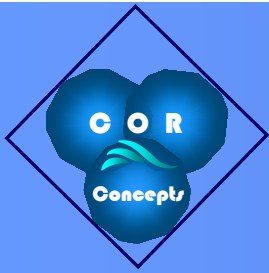
- Review document management procedures and practices
- Map all records (at a high level)
- Categorize record types
- Develop clear availability policies
- Implement procedures and forms to deal with requests
- Appoint, educate and empower personnel to deal with requests
- Develop clear categorization and storage policies
- Ensure that the all staff adhere to the procedures and policies



The Companies Act 71 of 2008

- Form and standards for company records
- Location of company records
- Access to company records



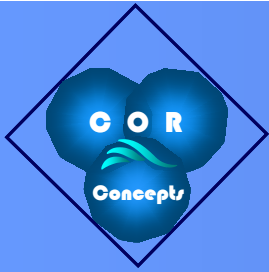


The Companies Act 71 of 2008

It is an offence for *a company*—

- (i) with an intention to deceive or mislead any person—
 - *to fail to keep accurate or complete accounting records;*
 - *to keep records other than in the prescribed manner and form, if any;*
 - (ii) to falsify any of its accounting records, or permit any person to do so; or
 - *(b) any person to falsify a company's accounting records.*

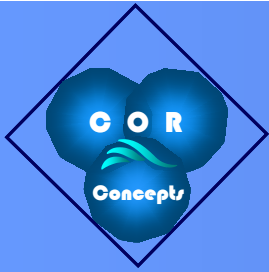




The Companies Act 71 of 2008

S7. An **unaltered** electronically or mechanically generated reproduction of any document, other than a share certificate, may be substituted for the original for any purpose for which the original could be used in terms of this Act *if that reproduction satisfies any applicable prescribed requirements as to the form or manner or reproduction**

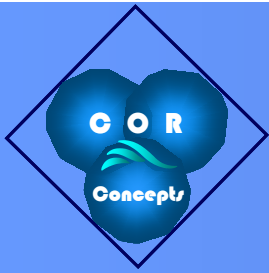
**Companies Amendment Act 2011*



The Companies Act 71 of 2008

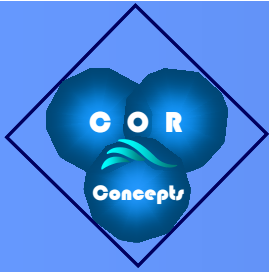
Any documents, accounts, books, writing, records or other information

- that a company is required to keep in terms of this Act or any other public regulation must be kept—
- *(a) in written form, or other form or manner that allows that information to be converted into written form within a reasonable time; and*
- *(b) for a period of seven years, or any longer period of time specified in any other applicable public regulation...*



The Companies Act 71 of 2008

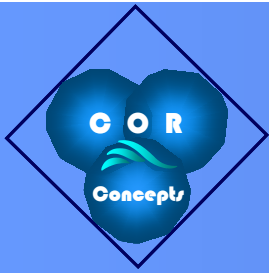
- If, in terms of this Act, a notice is required or permitted to be given or published to any person, it is sufficient if the notice is transmitted electronically directly to that person in a manner and form such that the notice can conveniently be printed by the recipient within a reasonable time and at a reasonable cost.



The Companies Act 71 of 2008

If, in terms of this Act, a document, record or statement, other than a notice is required—

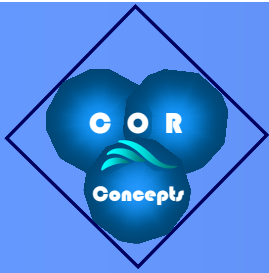
- *(a) to be retained, it is sufficient if an electronic original or reproduction of that document is retained as provided for in section 15 of the Electronic Communications and Transactions Act; or*



Companies Regulations December 2010

The accounting records required to be kept by the Act and this regulation must be kept in such a manner as-

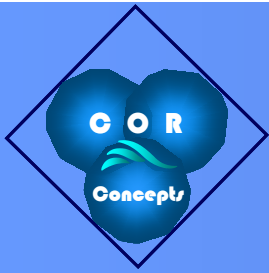
- a) to provide adequate precautions against-
 - i) theft, loss or intentional or accidental damage or destruction; and
 - ii) falsification; and
- b) to facilitate the discovery of any falsification; and
- c) to comply with any other applicable law dealing with accounting records, access to information, or confidentiality.



Companies Regulations December 2010

If a company keeps any of its accounting records in electronic form, the company must

- (a) provide adequate precautions against loss of the records as a result of damage to, or failure of, the media on which the records are kept; and
- (b) ensure that the records are at all times capable of being retrieved to a readable and printable form, including by converting the records from legacy to later storage media, or software, to the extent necessary from time to time.



Companies Regulations December 2010

- *Conducting business electronically*

1) A notice announcing the availability of a document, record or statement, as contemplated in [section 6 \(11\)\(b\)\(ii\)](#), must-

a) be in writing and delivered to each intended recipient of the document, record or statement either-

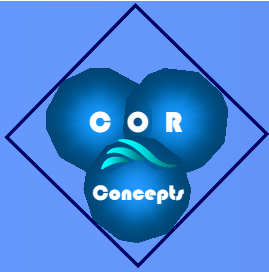
i) in paper form at the intended recipient's last known delivery address; **or**

ii) in electronic form at their last known electronic mail address;

2) A document, record or statement, the availability of which is being announced as contemplated in section 6 (11)(b)(ii), must be made available to intended recipients either-

a) in paper copy, or in a printed version of an electronic original produced by or on behalf of the company on demand by an intended recipient; **or**

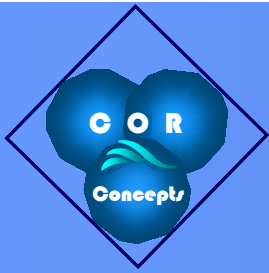
b) electronically in a manner and form such that it can conveniently be accessed and printed by the recipient within a reasonable time and at a reasonable cost.



Corporate Governance: King III and records management

- The board has a duty to establish structures and processes, with appropriate checks and balances that enable directors to discharge their legal responsibilities
- The board should ensure that the company implements an effective compliance framework and effective processes
 - without contravention of any laws and regulations
(*regulatory universe and retention requirements become important*)

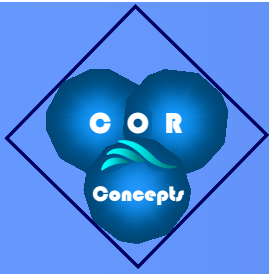
King III (and the Act) require many reports. Accurate, timeous access to information is critical to fulfil this requirement.



King III Principles

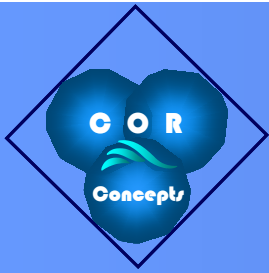
- Internal audits should be Risk-based
- Risk of loss of information should be one of the components of the audit.
- IT Governance is critical. *“The risks involved in IT governance have become significant”*.





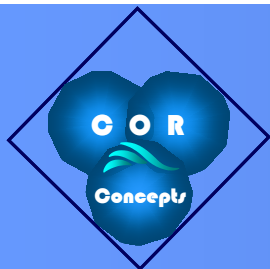
King III - Information security

- confidentiality: *ensuring that information is accessible only to those authorised to have access;*
- integrity: *safeguarding the accuracy and completeness of information and processing methods; and*
- availability: *ensuring that authorised users have access to information and associated assets when required.*



King III - Information Security

- Information security deals with the protection of information, in its electronic and paper-based forms, as it progresses through the information lifecycle for capture, processing, use, storage, and destruction. For this reason, information security has to address people-, process- and technology-related dimensions in order to be truly effective.



Can documents be managed electronically?

NEWS

• DAILY NEWS **PAGE 3**
FRIDAY MARCH 4 2005

Judge allows computer copy

ESTELLE ELLIS

LEAD prosecutor Billy Downer SC got permission today from the Durban High Court to confront Schabir Shaik with a document found on the hard drive of one of his company's computers.

Yesterday, Shaik's first reaction to the document was one of ignorance. His counsel, Francois van Zyl SC, then objected to the admission of the document.

One of the main points of dispute was that the document was not seized in its hard copy form but in its electronic format on a hard drive.

But Judge Hilary Squires ruled this morning that in terms of the Electronic Communications and Transactions Act, the document is on an equal footing with a hard copy version.

He said the situation was no different than when a prosecutor wished to confront a witness with statements taken down on paper.

"I have concluded eventually, and to my own surprise, that Mr Downer was correct," Judge Squires said.

He explained that his surprise was triggered not by Downer being correct (in general) but by what he had discovered about the law on electronic documents. Squires' examination will continue.

The prosecution had asked the court to allow them to use the document to prove that Shaik was "the author" of a letter he has denied ever seeing.

The application followed a series of questions asked of Shaik by Downer dealing with the Point Development in Durban.

The State is using Shaik's alleged involvement with the



**THE
Shaik
SAGA**

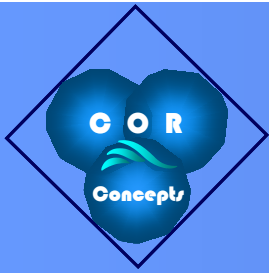
Point Development and Zuma's alleged assistance in this regard, to try to prove that there was a "general corrupt relationship" between the two. In short it is alleged that Shaik paid to keep Zuma in politics and in turn Zuma helped Shaik promote his business interests.

Downer is using a series of documents in his cross-examination of Shaik, supplied to the Scorpions by David Wilson, formerly from Renong, and other documentation seized. Shaik denied that he had ever seen one of the letters.

The specific letter was written on a letterhead of the "Ministry of Economic Affairs and Tourism, Province of Kwa-Zulu-Natal".

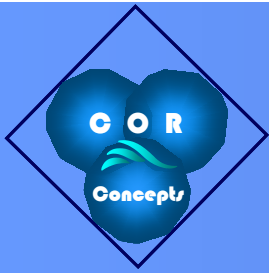
It is addressed to the chairman of Renong, Tun Sri Halim Saad, and ostensibly written by Zuma, but not signed. Shaik had earlier admitted that this letter was found at Nkobi. In the letter Zuma asked Saad for a meeting to discuss who the best "local partner" for him would be to work with on the Point Development.

"It is the first time that I have seen this letter," Shaik said.



Can documents be managed electronically?

- Yes, but only if the conditions of the Electronic Communications & Transactions Act are met.
- Those conditions are found in sections on “retention”, “original” and “evidence”



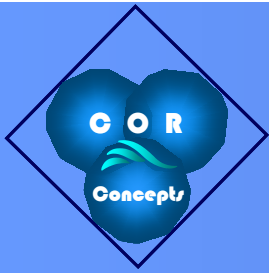
ECT Act

Originality of documents

- **If the law requires information to be presented in its original form, a data message meets this requirement if:**
- (a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment
- (b) that information is capable of being displayed or produced to the person to whom it is to be presented.

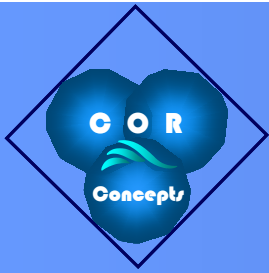
The integrity must be assessed—

- (a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
- (b) in the light of the purpose for which the information was generated; and
- (c) having regard to all other relevant circumstances.



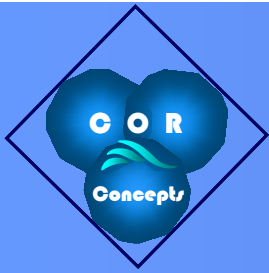
ECT Act: Admissibility & evidential weight

- ... Rules of evidence must not be applied so as to deny the admissibility of a data message.....
 - on the mere grounds that it is constituted by a data message
 - Is the best possible evidence if not in it's original form
- ...regard must be had to—
 - the reliability of the manner in which the data message was generated, stored or communicated;
 - the reliability of the manner in which the integrity of the data message was maintained;
 - the manner in which its originator was identified



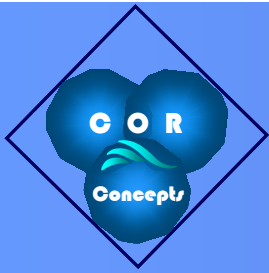
ECT Act: Retention

- Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if—
 - the information contained in the data message is accessible so as to be useable for subsequent reference;
 - the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
 - the origin and destination of that data message and the date and time it was sent or received can be determined.



Summary of the law

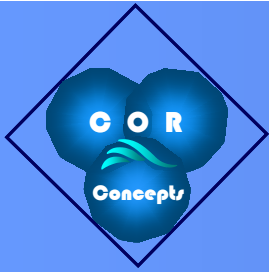
- The law seldom differentiates between paper and electronic records
- The NARS Act specifically includes electronic records
- We are already conducting business electronically
- The questions we need to ask are: Which e-mails are records, and how long should they be retained?



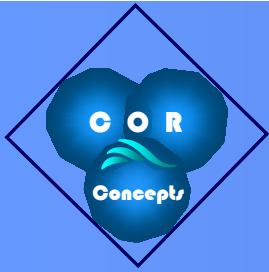
Which records should be kept?

Those which:

- *Provide evidence & information about the organisation's policies & actions*
- *Provide evidence & information about the interaction with the community*
- *Document the rights & obligations of individuals and organisations*
- *Contribute to the memory of the organisation for scientific, cultural or historical purposes*
- *Contain evidence & information about activities of interest to internal & external stakeholders*

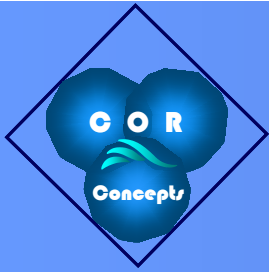


Specific challenges with e-mail record retention



E-Mail policies

- Policies, Procedures, Processes, Practice
- Practice = Education and Enforcement
- E-mail policies must be consistent with your records management policy
 - E-mail is just another record
 - Most correspondence will be (or already is) on e-mail



The “HMCWISKAFHL” Continuums

“Help Me Choose What I Should Keep And For How Long”

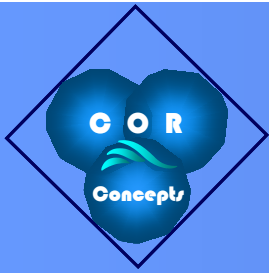


Need to make decisions up front

What information should be kept?

How long should it be kept?

How rigidly should rules be enforced?



The “HMCWISKAFHL” Continuums



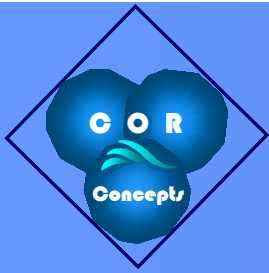
What Should I Keep?”

Keep Nothing

- Lowest cost
- No rules
- Valueless
- High Risk
- Loss of company information
- Baby goes with the bathwater

Keep Everything

- Highest cost
- No rules
- Too difficult to search
- Risk of incriminating stuff
- Lots of junk
- The baby's there – you just can't find it



“HMCWISKAFHL” Continued



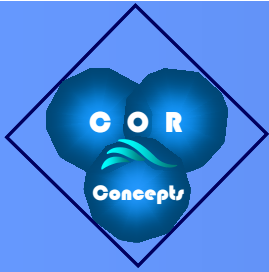
How long should I keep it?”

Destroy Immediately

- Lowest cost
- No rules
- Valueless
- High Risk
- Loss of company information
- Baby goes with the bathwater

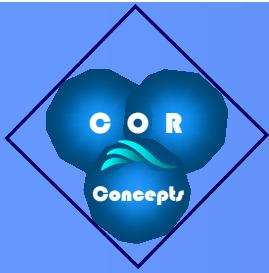
Keep Forever

- Highest cost
- One rule
- Too difficult to search
- Risk of incriminating stuff
- Too much information
- The baby's drowned by the time you find it



What about personal e-mails?

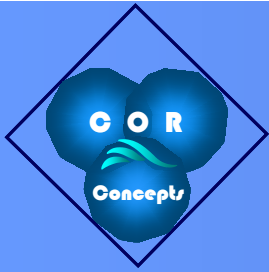
- Should we allow personal e-mails in our corporate systems?
- Should IT be backing up personal e-mails?
- Should they be allowed to intercept personal e-mails?



Retention rules

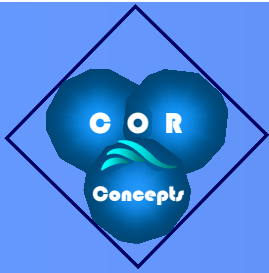
Retention rules must be based on your classification system as with any other record





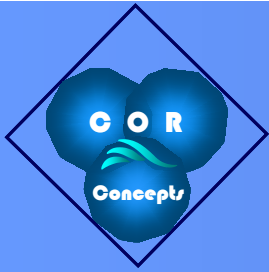
Retention rules

- Classification
 - Evaluate and act based on content
 - Determine value
 - Retain according to value
 - Personal mails get destroyed?
- Transmission
 - Destination and content are important



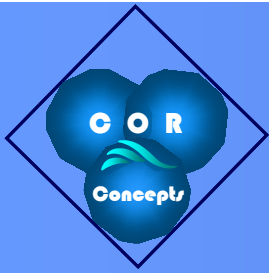
Retention rules

- Protection
 - Failure to protect isn't an option
 - Risk is too high
- Centralisation
 - Essential to reduce duplication
 - Adds evidentiary weight
 - Increases discoverability at lower cost



Retention rules

- Metadata is key
 - Must keep information about the e-mails
 - Who sent what where and when
 - Audit trails

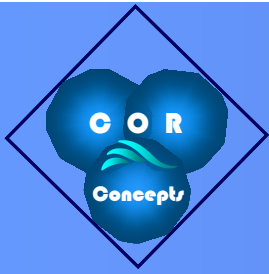


What is an e-mail business record?

- Not every e-mail is a business record
- Must establish clear definitions
- Communicate those definitions clearly

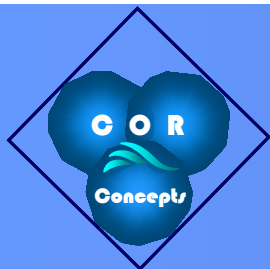
A business record is:

*Evidence of business-related activities, events, and transactions
With on-going business, legal, compliance, operational, or
Historical value*



Is it a business record?

- Not all business records need to be retained for the same duration
- Don't all have the same value
- Must ask:
 - *Would you keep it if it wasn't an e-mail?*
 - *Would you hand it over to the "records" department or registry if it arrived via snail mail?*
 - *Does it identify who participated in a certain activity?*
 - *Does it provide evidence of business activities?*
 - *Does it have business, legal or operational value?*
 - *How does the value change over time – might there be historical value?*



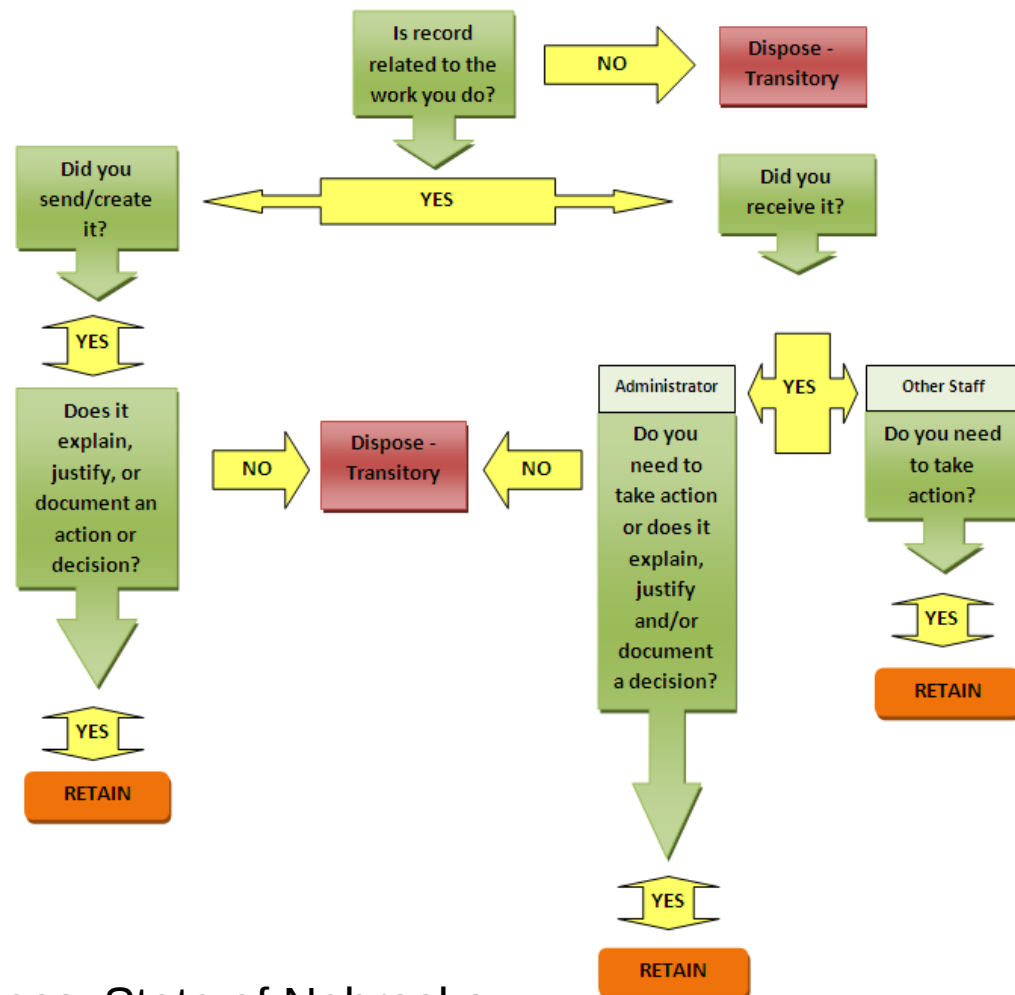
E-mail retention decisions

RECORD DECISION TREE

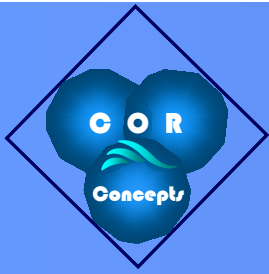
Mary R. Ott, RIM Specialist

NE Sec. of State - Records Management Division

3/28/11

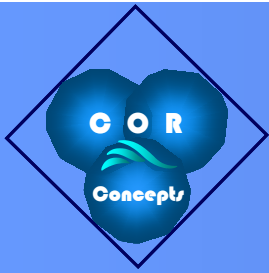


Example of the retention decision process: State of Nebraska



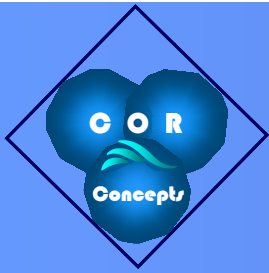
Which media to use for retention?

- E-mail contains unique attributes:
 - Header information
 - Addresses, server names, routing info, dates
 - Content
 - Text, graphics, sound, hyperlinks, other code that has little meaning out of context
 - Attachments, (including potential for viruses)
 - Digital signatures



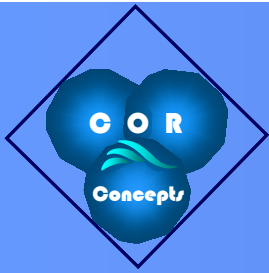
Information necessary for retention

- Creator identification
- Creation and/or transmission date/time
- Receipt date and time
- Recipient identification
- Routing information
- In addition to “Content” information



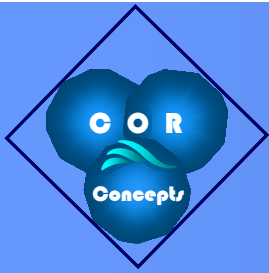
Storing electronically

- Benefits:
 - Easy search and retrieval
 - Multiple ways to search
 - Ability to access metadata and audit trails
 - User or “rule” based retention
 - Can automate – take the pain from the users
 - Is the only true “original” – ECT Act s14
- Disadvantages
 - High “Per seat” cost
 - Cost of software and hardware
 - IT skills and technology needed throughout the records “life cycle”
 - Enhanced searchability may produce undesirable e-mails
 - Training costs may be high
 - Potentially high discovery costs



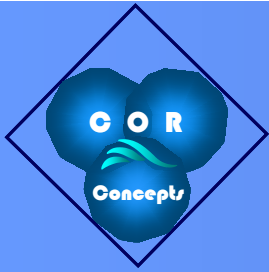
Storing on paper

- Rules have to be developed:
 - When and what should be printed?
 - Where and how should the printouts be stored?
- Guidelines:
 - Print message with metadata
 - Store with related records
 - Properly organise. Label and store in a recognised indexing regime
 - Protect confidential material



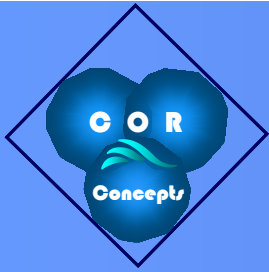
Storing on paper

- Benefits:
 - Easy to implement and train
 - Eliminate masses of electronically stored mail
 - Limited storage costs
 - Fewer technology resources required
 - Reduces the need to migrate data over time
 - Limit discovery exposure
 - Inexpensive to implement
 - Easy to apply retention rules



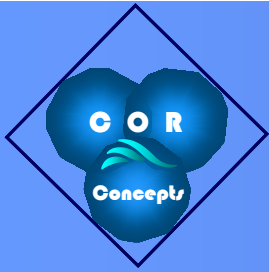
Storing on paper

- Disadvantages:
 - Reduced evidentiary weight of paper copies?
 - Printed metadata for each record is required
 - No electronic searching
 - Requires compliance and involvement from all employees
 - May not be acceptable to all courts? How to choose if a paper version and different electronic version are presented?
 - Potential for losing embedded information
 - Attachments will need to be separately presented.



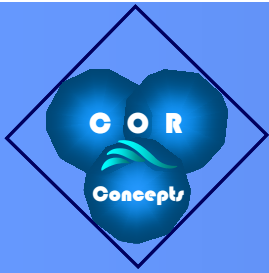
Evidential weight

- Enforcement of rules is essential
 - The law appreciates consistency
 - Leave no room for interpretation
 - Simple to understand, easy to enforce



Rules for disposing of e-mail

- Retention rules must be considered before destroying
- Employees to be aware of and enforce “hold” rules
- If confidential, all copies must be permanently purged.



E-mail etiquette



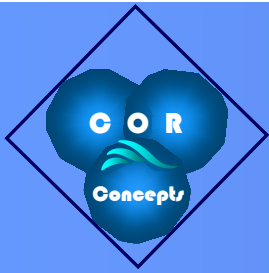
DON'T

“Reply to All” on your work e-mails if your message isn’t relevant to everyone



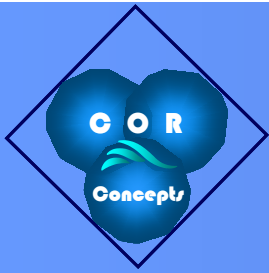
DO

Double-check your response before sending to multiple recipients



Why is it important?

- **Professionalism:** by using proper email language your organisation will convey a professional image.
- **Efficiency:** emails that get to the point are much more effective than poorly worded emails.
- **Protection from liability:** employee awareness of email risks will protect your organisation from potential court cases.



E-mail etiquette

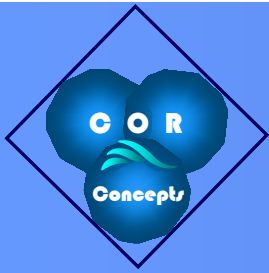
1. Be concise and to the point.

- Do not make an e-mail longer than it needs to be. Remember that reading an e-mail is harder than reading printed communications.

2. Answer all questions, and pre-empt further questions.

- An email reply must answer all questions, and pre-empt further questions – If you do not answer all the questions in the original email, you will receive further e-mails regarding the unanswered questions

...

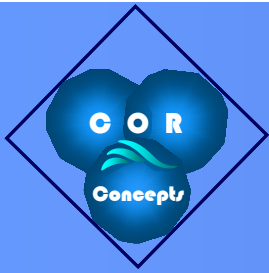


E-mail etiquette

3. Use proper spelling, grammar & punctuation.

- This is not only important because improper spelling, grammar and punctuation give a bad impression of your organisation, it is also important for conveying the message properly.
- E-mails with no full stops or commas are difficult to read and can sometimes even change the meaning of the text. And, if your program has a spell checking option, why not use it?
- SMS type of communication isn't acceptable.

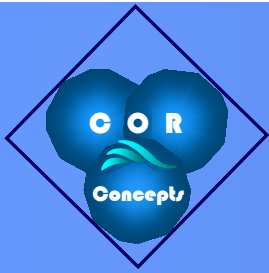
I wntd 2 go hm ASAP, 2C my M8s again



E-mail etiquette

4. Make it personal.

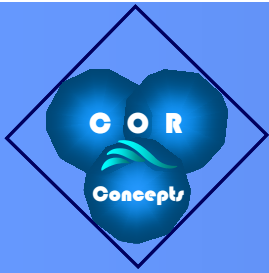
- Not only should the e-mail be personally addressed, it should also include personal i.e. customized content. For this reason auto replies are usually not very effective. However, templates can be used effectively in this way, see next tip.



E-mail etiquette

5. Use templates for frequently used responses.

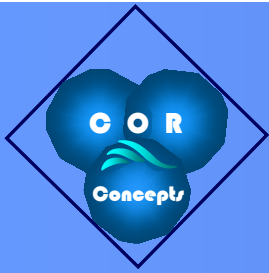
- Some questions you get over and over again, such as directions to your office or how to subscribe to your newsletter. Save these texts as response templates and paste these into your message when you need them. You can save your templates in a Word document, or use pre-formatted emails.



E-mail etiquette

6. Answer swiftly.

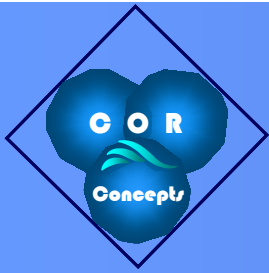
- Customers send an e-mail because they wish to receive a quick response. If they did not want a quick response they would send a letter or a fax. Therefore, each e-mail should be replied to within at least 24 hours, and preferably within the same working day. If the email is complicated, just send an email back saying that you have received it and that you will get back to them. This will put the customer's mind at rest and usually customers will then be very patient!



E-mail etiquette

7. Do not attach unnecessary files.

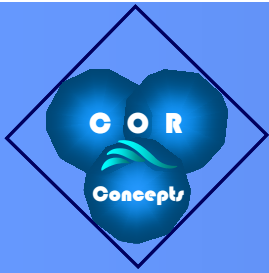
- By sending large attachments you can annoy people and even bring down their e-mail system. Wherever possible try to compress attachments and only send attachments when they are necessary.
- Moreover, you need to have a good virus scanner in place since your recipients will not be very happy if you send them documents full of viruses!



E-mail etiquette

8. Use proper structure & layout.

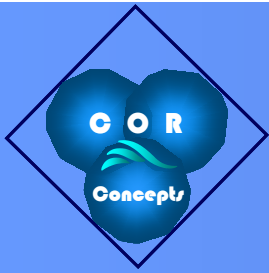
- Since reading from a screen is more difficult than reading from paper, the structure and layout is very important for e-mail messages. Use short paragraphs and blank lines between each paragraph. When making points, number them or mark each point as separate to keep the overview.



E-mail etiquette

9. Do not overuse the high priority option.

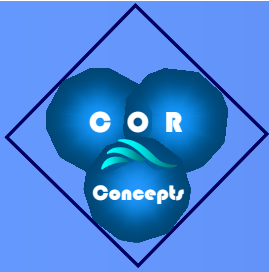
- We all know the story of the boy who cried wolf. If you overuse the high priority option, it will lose its function when you really need it.
- Even if a mail has high priority, your message will come across as slightly aggressive if you flag it as 'high priority'.



E-mail etiquette

10. Do not write in CAPITALS.

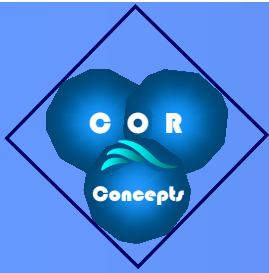
- IF YOU WRITE IN CAPITALS IT SEEMS AS IF YOU ARE SHOUTING. This can be highly annoying and might trigger the wrong response. Therefore, try not to send any email text in capitals.



E-mail etiquette

11. Don't leave out the message thread.

- When you reply to an email, you must include the original mail in your reply, in other words click 'Reply', instead of 'New Mail'.

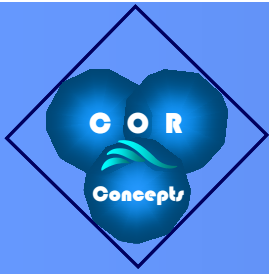


E-mail etiquette

12. Add disclaimers to your emails.

- Adding disclaimers to your internal and external mails can help protect from liability.

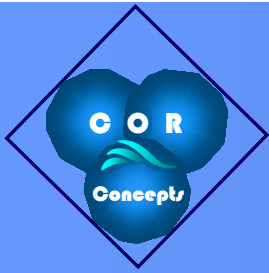
In terms of SA law, an employer may be held liable for the damages caused by a virus that was attached to an employee's email message.



E-mail etiquette

13. Read the email before you send it.

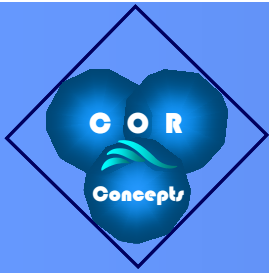
- A lot of people don't bother to read an email before they send it out, as can be seen from the many spelling and grammar mistakes contained in emails.
- Reading your email through the eyes of the recipient will help you send a more effective message and avoid misunderstandings and inappropriate comments.



E-mail etiquette

14. Do not overuse Reply to All.

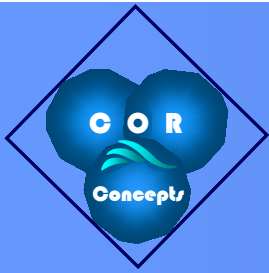
- Only use Reply to All if you really need your message to be seen by each person who received the original message.



E-mail etiquette

15. Use the Bcc: field carefully.

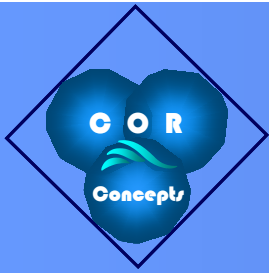
- Make sure when using Bcc: that your intentions are proper. To send Bcc: copies to others as a way of talking behind someone's back is inconsiderate.
- Only consider Bcc if you risk publicizing someone else's email address without their permission. Even then rather use mail merge or Groups.



E-mail etiquette

16. Take care with abbreviations and emoticons. (see earlier comment)

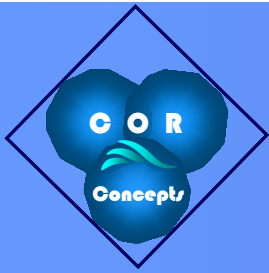
- In business emails, try not to use abbreviations such as BTW (by the way) and LOL (laugh out loud). The recipient might not be aware of the meanings of the abbreviations and in business emails these are generally not appropriate.
- The same goes for emoticons, such as the smiley :-). If you are not sure whether your recipient knows what it means, it is better not to use it.



E-mail etiquette

17. Be careful with formatting.

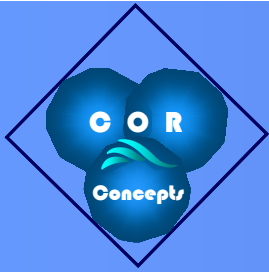
- Remember that when you use formatting in your emails, the recipient might not be able to view formatting, or might see different fonts than you had intended. When using colours, use a colour that is easy to read on the background.
- Don't use fancy coloured backgrounds.



E-mail etiquette

18. Take care with rich text and HTML messages.

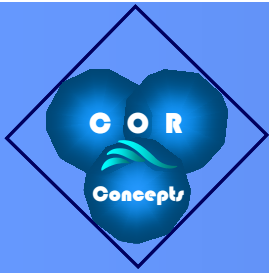
- Be aware that when you send an email in rich text or HTML format, the recipient might only be able to receive plain text emails. If this is the case, the recipient will receive your message as a .txt attachment. Most email clients however, including Microsoft Outlook, are able to receive HTML and rich text messages.



E-mail etiquette

19. Do not forward chain letters.

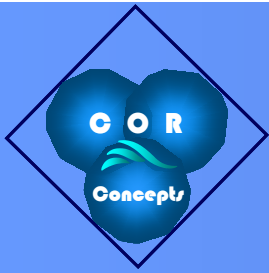
- Do not forward chain letters. We can safely say that all of them are hoaxes. Just delete the letters as soon as you receive them.



E-mail etiquette

20. Do not request delivery and read receipts all the time.

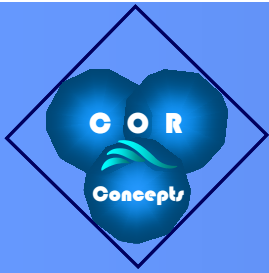
- This will almost always annoy your recipient before he or she has even read your message.
- The recipient can ignore it anyway.
- If you want to know whether an email was received it is better to ask the recipient to let you know if it was received.



E-mail etiquette

21. Do not ask to recall a message.

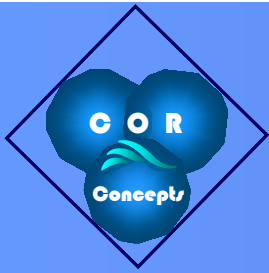
- Biggest chances are that your message has already been delivered and read. A recall request would look very silly in that case wouldn't it?
- It is better just to send an email to say that you have made a mistake. This will look much more honest than trying to recall a message.



E-mail etiquette

22. Do not copy a message or attachment without permission.

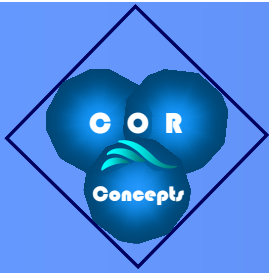
- Do not copy a message or attachment belonging to another user without permission of the originator. If you do not ask permission first, you might be infringing on copyright laws.



E-mail etiquette

23. Do not use email to discuss confidential information.

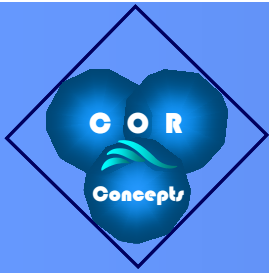
- Sending an email is like sending a postcard. If you don't want your email to be displayed on a bulletin board, don't send it. Moreover, never make or forward any libelous, sexist or racially discriminating comments in emails, even if they are meant to be a joke.



E-mail etiquette

24. Use a meaningful subject.

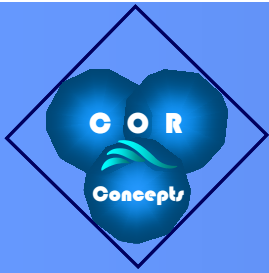
- Try to use a subject that is meaningful to the recipient as well as yourself. For instance, when you send an email to a organisation requesting information about a product, it is better to mention the actual name of the product, e.g. 'Product A information' than to just say 'product information' or the organisation's name in the subject.



E-mail etiquette

25. Avoid using URGENT and IMPORTANT.

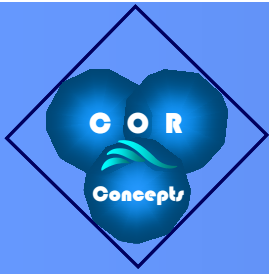
- Even more so than the high-priority option, you must at all times try to avoid these types of words in an email or subject line. Only use this if it is a really, really urgent or important message.



E-mail etiquette

26. Avoid long sentences.

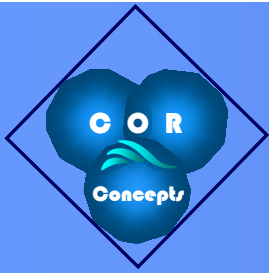
- Try to keep your sentences to a maximum of 15-20 words. Email is meant to be a quick medium and requires a different kind of writing than letters.



E-mail etiquette

27. Don't forward virus hoaxes and chain letters.

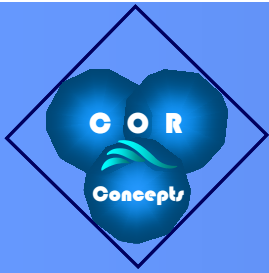
- If you receive an email message warning you of a new unstoppable virus that will immediately delete everything from your computer, this is most probably a hoax.
- By forwarding hoaxes you use valuable bandwidth and sometimes virus hoaxes contain viruses themselves, by attaching a so-called file that will stop the dangerous virus.
- Since it is impossible to find out whether a chain letter is real or not, the best place for it is the recycle bin.



E-mail etiquette

28. Keep your language gender neutral.

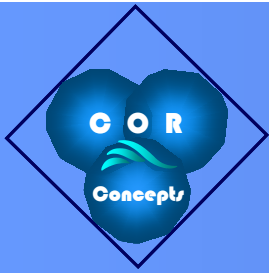
- In this day and age, avoid using sexist language such as: 'The user should add a signature by configuring his email program'. Apart from using he/she, you can also use the neutral gender: 'The user should add a signature by configuring the email program'.



E-mail etiquette

29. Don't reply to spam.

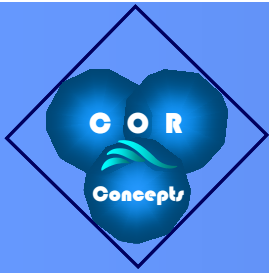
- By replying to spam or by unsubscribing, you are confirming that your email address is 'live'. Confirming this will only generate even more spam. Therefore, just hit the delete button or use email software to remove spam automatically.



E-mail etiquette

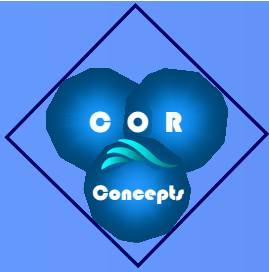
30. Use cc: field sparingly.

- Try not to use the cc: field unless the recipient in the cc: field knows why they are receiving a copy of the message. Using the cc: field can be confusing since the recipients might not know who is supposed to act on the message.
- When responding to a cc: message, only include the person in the cc: field if you have a particular reason for wanting this person to see your response.



Policies to consider

- Records management
- Electronic records management
- E-mail policy
- Internet usage policy
- ICT policy
- Usage monitoring policy
- Information security policy (MISS?)
- Employee policy
- Use of Organisational assets.



E-mail archiving

- The following slides are an example based on Open Text.
- This is used to highlight key components

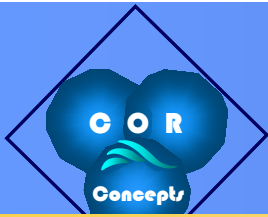


Why archive email?

Your mailbox has exceeded one or more size limits set by your administrator. Your mailbox size is 1035723 KB.

Mailbox size limits: You will receive a warning when your mailbox reaches 972800 KB. You may not be able to send or receive new mail until you reduce your mailbox size.

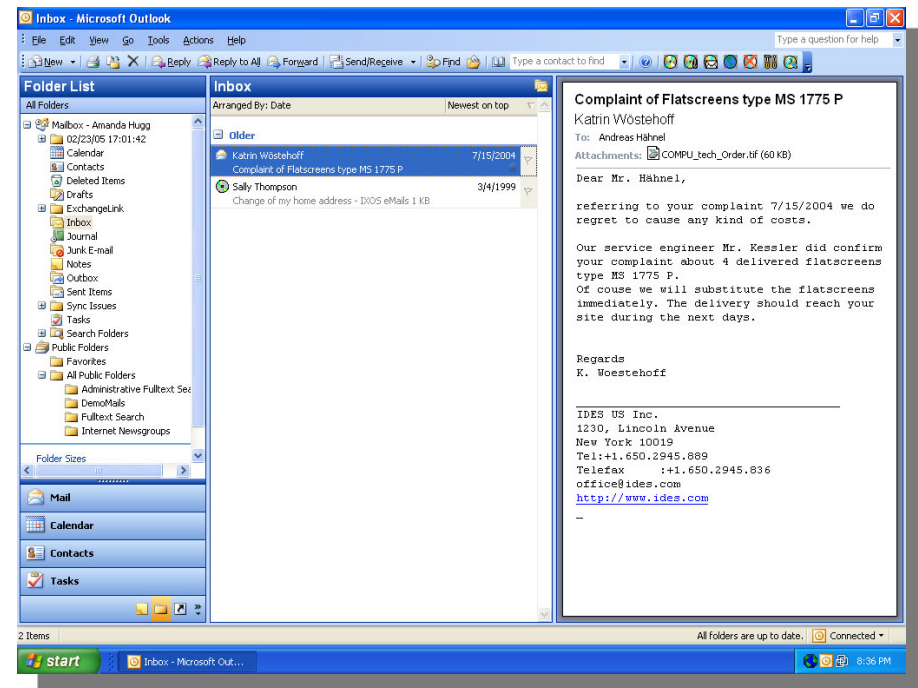
To make more space available, delete any items that you are no longer using or move them to your personal folder file (.pst), or select some items that you no longer need and permanently (SHIFT + DEL) delete them.

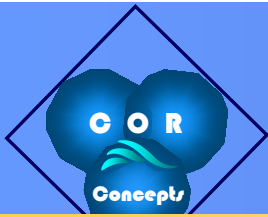


Typical functionality

Livelink ECM – Email Archiving for Microsoft® Exchange Minimize Operations Costs and Optimize System Performance

- Simplify email access
- Optimize email system performance
- Archive email interactively or automatically
- Unparalleled scalability for outstanding performance
- Minimize overhead with simplified administration
- Minimized discovery costs with optional advanced search capabilities
- Reduce support overhead with the elimination of PST files



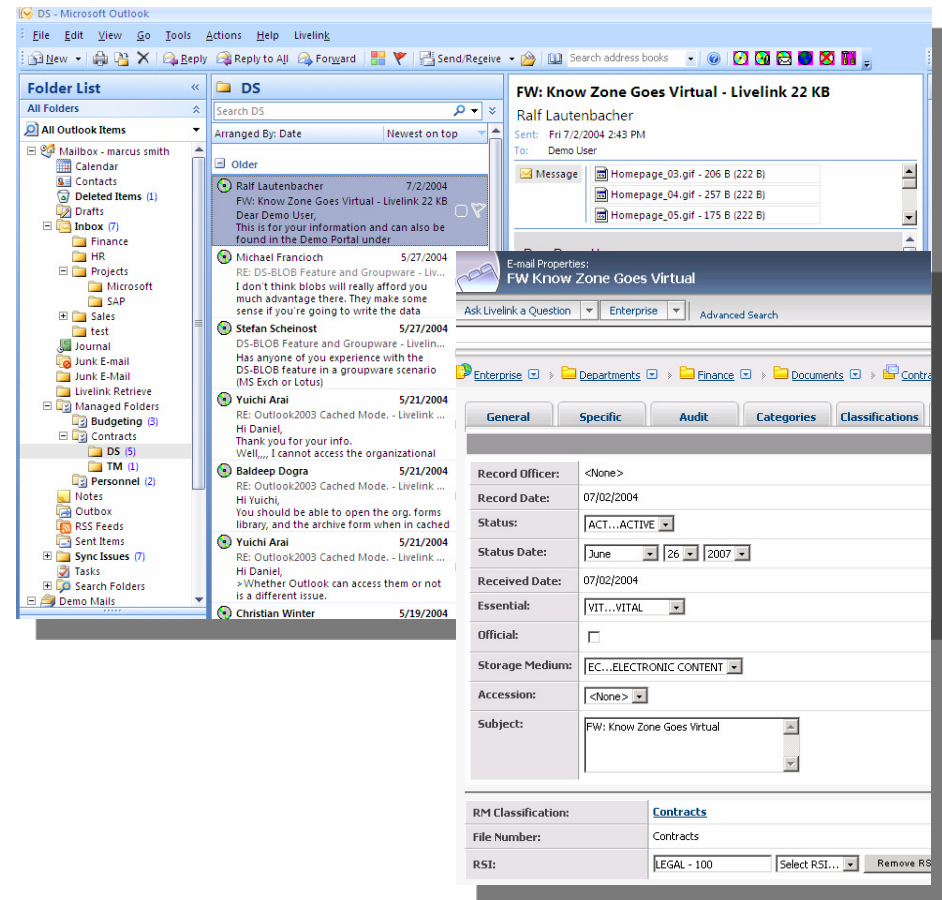


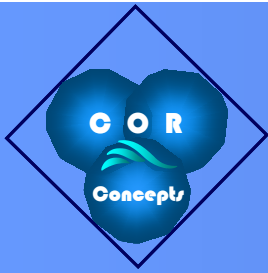
Typical functionality

Open Text Email Management for Microsoft® Exchange

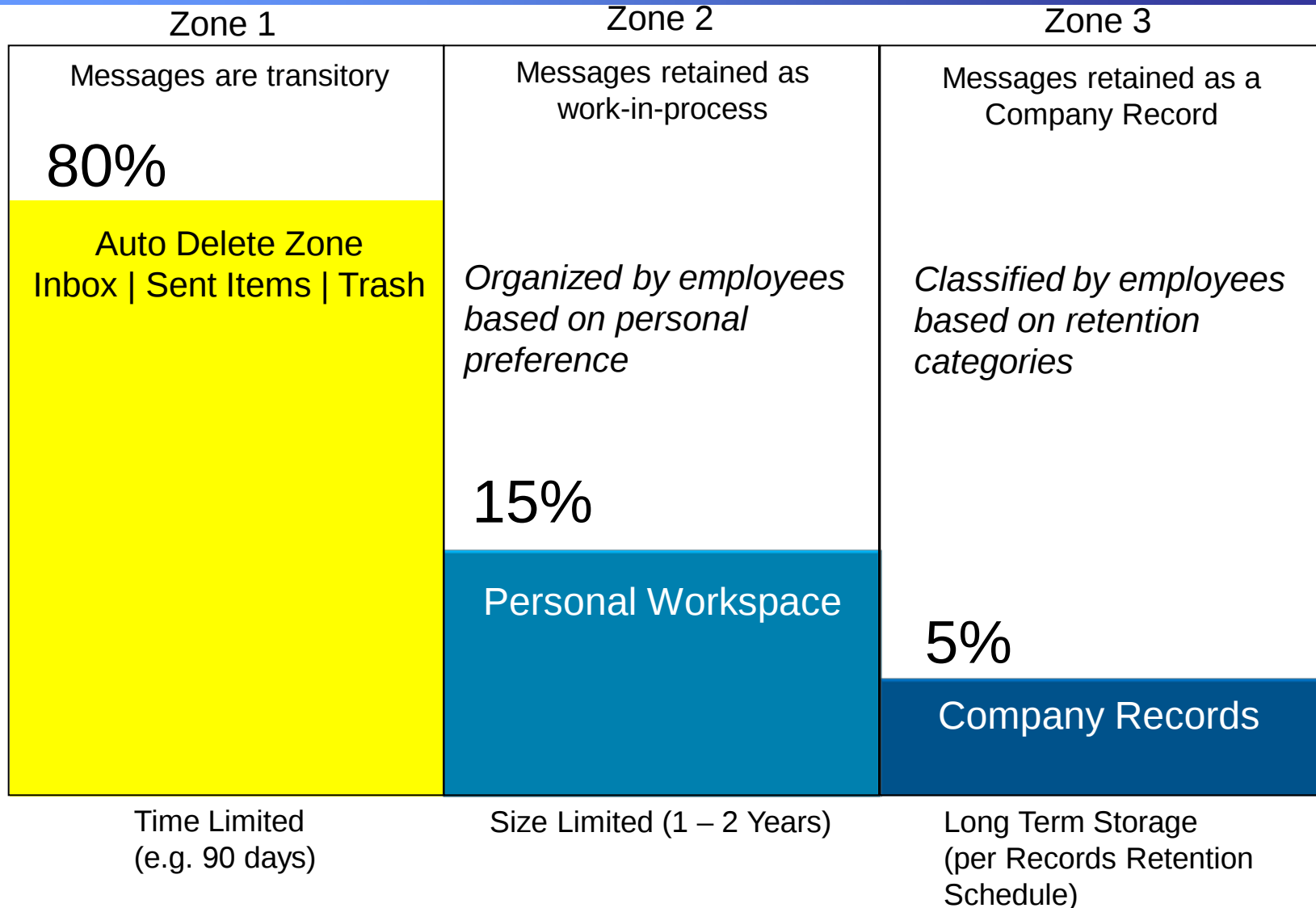
Manage email as a business record

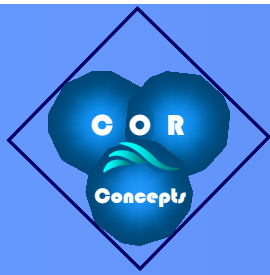
- Capture content into a centralized repository
- Assess and identify business record emails
- Easy and immediate access with advanced search capabilities
- Compliance and certification
(DoD 5015.2, PRO-UK, PIPEDA, VERS, SEC 17a-4, NASD 400...)
- Preservation, Rendition and Disposition
- Disaster Recovery





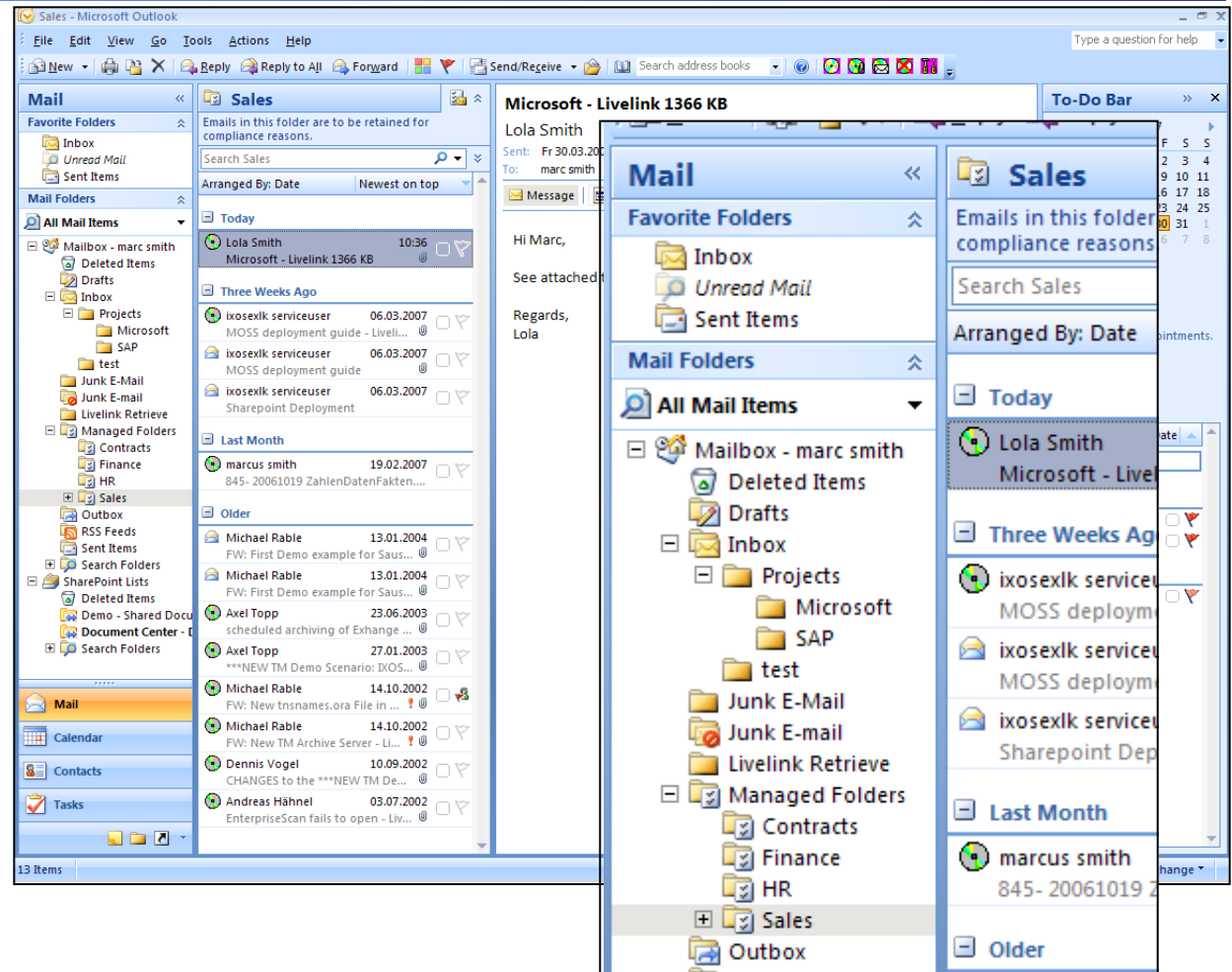
Multi- Zone Approach

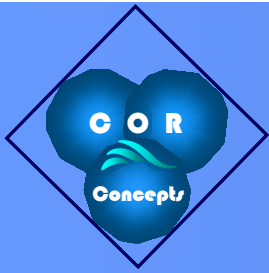




Email management today

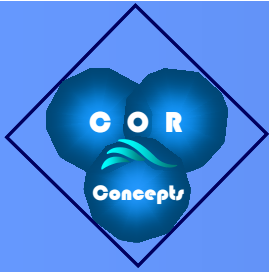
- Messages can be classified as business records
- “Records-enabled” folders exposed in mail client interface
- Drag-and-drop individual or multiple messages
- Retention by record classification
- Personal or business views





Other considerations

- Digital signatures
- Relationships with IT and other key stakeholders (Unions, HR, Legal etc)
- Templates and naming conventions
- Consistent file structures
 - E-mail
 - Paper
 - Electronic records



Other considerations

- “Archiving” strategy and systems
 - E-mail
 - Paper
 - Electronic records
 - Data



Questions?

Any questions?

