

# ISO27001 Certification

## ISO 27001 : NTT Europe Online Experiences and Commercial Benefits

15 February 2007  
Paris

Authors:  
Neil Wheelwright, CISO, CISSP-ISSMP  
Robert Steggles Director Marketing Europe  
:



# Contents

- Introduction - Who is NTT Europe Online?
- NTTEO's approach to ISO27001
- ISO27001 Deliverables
- Useful Pointers
- Questions

# Neil Wheelwright, CISSP-ISSMP

To 1987 Mainframe operating system and database support

Police project in London

Banking work in Amsterdam, Zurich, Manchester

1988-2001 Internal IT Audit, Unisys

Worldwide remit

2001-2003 Information Security Manager, Logicom

Achieved certification to BS7799:2002

Since 2003 European Information Security Manager, NTTEO

# NTT Europe Online

NTT Europe Online designs, deploys and manages critical internet infrastructure, managed security and application services for businesses globally

Our dealers are located throughout the UK. Locate your nearest dealer by entering your Postcode below.

Nissan has put together a selection of great offers for you. Visit our special offers page to see details. And once you've found

Your gateway to the Earth's wilder reaches. You'll meet the people who know these breathtaking but inhospitable landscapes and

Code	Libellé ou Mat. coté	Recherche rapide	OK
14:56	BOURVELLE	88.95	+5.89%
13:00	SOTEC SALON	23.53	+5.04%
	PUBLICIS GROUPE	29.10	-2.81%
	TRIGALVO	34.05	-7.22%
	EVRAUCIS GROUPE AGE	85.00	+2.94%

# NTT Europe Online: Part of the NTT Communications Family



- Operations in Europe, Asia, USA
- 500,000+ business customers
- Ranked #1 in telecom industry
- 24th in Fortune's Global 500 (2006)
- 397 NTT Group companies
- \$92 billion annual revenues
- Financially secure
- 200,000 + employees globally

# NTT Europe Online

## Operational offices:

UK	London
France	Paris
Germany	Regensburg & Frankfurt
Spain	Barcelona & Madrid

## Finance office:

Netherlands	Hoofddorp
-------------	-----------

## Data centres:

London, Paris, Frankfurt, Madrid

Outsourced staff

# NTTEO's Approach to Certification



Why Certify to ISO27001

Management Commitment

Scope & Objectives

Management Forums

Timeline

# Why Certify to ISO27001

- Company must decide WHY it wants ISO27001
  - **Business reasons preferred**
- For NTTEO
  - **Existing customer requested it**
  - **Tender documents were asking about it (especially Public Sector)**
  - **Customers now require it**
- Certification versus Compliance
  - **Anyone can say they comply**
  - **Certification is an external verification**
- If you don't know 'WHY' – don't bother!

# Management Commitment

- Senior Management COMMITMENT is fundamental
- Senior Management INVOLVEMENT is obligatory
- Your auditor will interview senior management and expect them to understand information security and ISO27001.....!
  
- Without management commitment, the project will not get adequate resource

# ISMS

- Information Security Management System
- NTTEO runs a single ISMS covering all countries
  - **Keeps everything simple**
  - **Allows central control**
  - **But – span of control issues**
- All policies Europe wide unless specified otherwise
- Includes all deliverables

# Scope

Choose your scope carefully

- **It will be on your certificate – i.e., in the public domain**
- **So there is an ‘image’ aspect**

Scope can be changed

- **No need to certify whole company in one go**
  - Recommend including HR & IT within initial scope as they support other departments
  - Business purpose of certification will identify which departments to start with
  - Try to keep to a manageable size
- **Scope can be increased without the 2 stage audits involved in initial certification**
- **Can align changes with 6 monthly surveillance audits**

# Objectives

Goes back to 'Why?'

Management must choose & approve measurable objectives

- **'Being more secure' does not seem to be acceptable!**
- **Commercial objectives**
- **Review regularly**

# Management Forums

- Created an Information Security Management Group at start of project
  - **Provides strategy, business input, policy approvals**
  - **Included project sponsor (VP Ops), Company lawyer, HR, IT, Country manager**
- Implemented in all countries to take local ownership of security including internal audits, incident logs, awareness training, etc
- Meet monthly
  - **Needed prior to certifications audits**
  - **Useful thereafter as 2 months can be too long.**
  - **Focuses management's mind!**
  - **Agenda gets longer – but meetings are getting shorter!**
  - **All chaired by European Information Security Manager (who also writes minutes – ensuring they say what they should!)**
- Auditor requires a separate 'Management Review'. In fact this is European ISMG plus a representative from owning company (NTTE)

# NTTEO Timelines

- Project started – November 2003
- First certification audit, UK - June 2004 – UK Ops, HR, IT (to BS7799:2002)
- Remainder of UK (Sales / Marketing / Finance) – December 2004
- France - September 2005
- Germany - February 2006
- Spain - June 2006
- Transition to ISO27001 - June 2006
- Name Change Verio to NTT Europe Online – October 2006
- Netherlands - December 2007

# ISO27001 Deliverables



Statement of Applicability

Risk Treatment Plan

Risk Register

Risk Assessment

# SoA – Statement of Applicability

Simple document, lists controls, selected or not - headline about how addressed

Experience suggests auditors prefer as many controls selected as possible.

## Need to justify exclusion

ISO27001:2005 Control Objective	Selected?			Countries differ?	Method Of Implementation / Reason For Exclusion
	Data Centres	NTTE (UK)	NTTEO		
<b>Section 4 - ISMS</b>			YES		As evidence to auditor.
<b>Section 5 - Management Responsibility</b>			YES		ISMGs – ToR – IS019. ISMS Objectives – IS038.
<b>Section 6 – Internal ISMS Audits</b>			YES		In place in all countries.
<b>Section 7 - Management Review of ISMS</b>			YES		Country & European ISMG Meetings ISMS Management Review meetings to be held every 6 months, ISMS Objectives Europe-wide
<b>Section 8 - ISMS Improvements</b>			YES		ISM Responsible. ISMG input & Reviews. Annual policy review. Internal Audits
<b>A.5 Security Policy</b>					
<b>A.5.1 Information security policy</b>					
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.					
A.5.1.1 Information security policy document An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.			YES		High level security policy authorised by senior management is displayed by the UK Regional Director's desk – IS001 - Approved by the European President and ISM. See also Information Security Principles - IS002
A.5.1.2 Review of the information security policy The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.			YES		The content of the high level policy is such that it should remain static. However, it is reviewed annually with all information security policies.
<b>A.6 Organisation of information security</b>					
<b>A.6.1 Internal organization</b>					
Objective: To manage information security within the organization.					
A.6.1.1 Management commitment to information security Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.			YES		Employment of CISSP qualified Information Security Manager (ISM). Management attends Information Security Management Groups (ISMG) established at European and country levels. See ISMG minutes & Terms of Reference – IS019. Resources allocated to internal audits.

# RTP – Risk Treatment Plan

Lists controls AND other risks

Used as working document - status of work, responsibilities assigned, etc., Colour coded for visibility

<u>Cntrl Ref.</u>	<u>Control Description</u>	<u>Applies to RA Refs.</u>	<u>Current Status UK, Fr, De, ES</u>	<u>Current Status NL</u>	<u>Notes</u>	<u>Resp.</u>	<u>Comments</u>	<u>Proof / Policy Name</u>
							<b>Restricted Circulation:</b>	<b>ISM, All ISMGs, LRQA Auditors</b>
							Version 7.0	19/01/2007
<b>A.5</b>	<b>Security policy</b>							
<b>A.5.1</b>	<b>Information security policy</b>							
A.5.1.1	Information security policy document	All	Y	Y		ISM	For BS7799 - In place For ISO27001 - Clauses added to align with new standard. Additionally, IS004 updated to refer to risk assessment process, risk management and control selection	IS001 - Information Security Policy IS004 - BS7799 / ISO27001 Policy
A.5.1.2	Review of the information security policy	All	Y	Y		ISM / ISMGs	In place - Annual Review - 1st performed Oct / Nov 2004. 2nd review Nov-05-March-06.	IS001 - Information Security Policy See policy index for details.
<b>A.6</b>	<b>Organization of information security</b>							
<b>A.6.1</b>	<b>Internal organization</b>							
A.6.1.1	Management commitment to information security		Y	Y		ISMG / ISM	Employment of a qualified ISM and regular meetings of the ISMG at a European and country level indicates management commitment. Original ToR 27/10/03	ISMG minutes
A.6.1.2	Information security coordination		Y	X		ISM / ISMGs	In place - ISMG, UKISMG, FISMG, GISMG, SISMG Original ToR 27/10/03 ISM has pan-European role. Local staff project manage certification and post-certification support. NL - ??????	See security forum minutes & ToR - IS019
A.6.1.3	Allocation of information security responsibilities	All	Y	X		ISM / ISMGs	In place - ISMG, UKISMG, FISMG, GISMG NL - ??????	IS002 - Information Security Principles & other policies as applicable

# Risk Register

Not a required deliverable – but....

Allows documentation of accepted risk,  
shows status of risks being worked on,  
shows you are aware of changes to  
environment, etc.

## Cross reference to Security forum minutes

Ref.	Type	Logged Date	Risk Description	Vulnerability	Supporting Documentation	Policy / BS7799 Control reference	Responsibility	Status	Expected completion
16	T	01/06/04 UK	Clear Screen is OK, but Clear Desk is a problem. Audit results showed that there is insufficient cupboard space to be able to force Clear Desk policy on employees. HR / Facilities Mgr has requested the budget.		Agreed to go ahead at ISMG 14 October 2004. Completion – declared for 1/12/04, enforced from 1/1/05. End of grace period notified 18/1	A.7.3.1 – Clear Desk and Clear Screen Policy	ISM / Country Manager	Closed 18/01/05	End 2004
17	P	14/10/04	Camera phones The standard Verio mobile telephone handset includes a camera. As this is now a standard feature, Verio has no choice but to accept the risk inherent with them. Staff education will take place in order to mitigate the risk as far as possible.	Staff could photograph parts of our DCs and distribute electronically- to 'friend or foe'.	Minutes of ISMG 14th October 2004	A.9.1.3 Securing offices, rooms & facilities	ISM / Country Manager	Accepted	Permanent

# Risk Assessment

Keep it simple!

Initial model was good for producing a risk measure at the start and where it would be with the standard implemented.

Further iterations – as required by the standard – were not easy.

Wrote own RA – ‘approved’ by auditor last month

Group assets together – try to (sensibly) minimise

Do not get too detailed (i.e., no RA per laptop / per filing cabinet / etc)

BS7799-3:2005 – good for background reading, not really that much practical use

# Useful Pointers



External Auditors

Challenges

Lessons

# External Auditors

Auditor relationship is important

- Choose your audit company carefully - not just on cost
- Each auditor will have his own 'concerns' or 'interests'
- Try to keep a single external auditor - even if it means paying travel costs!
- 'Don't be afraid to 'push back' / discuss / negotiate
- Be 'straight' with the auditor – build trust
  - **Does not mean showing him the weaknesses!**
- Auditor can be a good source of 'best practice' suggestions
- Understand their approach to physical signatures and hard-copy documents!

# Challenges

- Internal Audits
  - **Internal auditors should be formally trained**
  - **Keeping internal auditors working – tendency to go back to ‘day job’**
  - **Keep track of open findings**
  - **Wide coverage of risks and controls is important**
  - **Can accept Simple audits**
    - E.g., Checking AV definitions up to date
- Effectiveness
  - **Standard tends to cover the business, not just security**
  - **Keep it simple, try to ensure your auditor on your side!**
- Awareness
  - **People are problem!**
  - **Small companies cannot afford many of the packaged solutions**
  - **Simple can work – Posters / Videos / Newsletters**



## Lexique

Dans chaque édition du bulletin Infosec nous expliquerons l'un des termes utilisés par le BS7799.

**ISMG** – Non, ce n'est pas un sport auto pratiqué par le responsable sécurité, cela signifie Information Security Management Group et cela peut être traduit par Groupe de supervision de la sécurité de l'information

Il y en a deux types, l'ISMG européen et l'ISMG local.

L'ISMG européen fixe la direction, la stratégie et évalue les risques pour Verio Europe et valide les politiques. L'ISM Europe (Information Security Manager) est nommé par ce Groupe.

Les ISMGs locaux, sont composés de l'ISM, du Country Manager, du responsable financier et du chef de projet BS7799 local. Ils sont responsables de l'obtention de la certification pour leur bureau et encore plus important, ils font en sorte de garder la certification. Cela implique d'évaluer et réduire au minimum les risques en mettant en place des systèmes adaptés, en surveillant et en effectuant des contrôles.

Si vous avez des questions à poser sur la sécurité de l'information, contactez Neil, notre « European Information Security Manager » ou votre « ISMG » local.

Y a-t-il un acronyme qui vous pose problème ?

Si vous désirez de plus amples informations, si vous avez des commentaires ou des suggestions, contactez :

## Bienvenue

Voici la troisième édition de notre *newsletter* européenne sur la sécurité de l'information. Notre but, répondre à vos questions sur le BS7799 et vous éclairer sur les *policies*.

## Policies

Cette fois ci, nous allons nous intéresser à la *policy* sur la **Protection des informations confidentielles, IS013** dont le but est d'éviter la divulgation non autorisée ou par négligence d'informations sur la société. Quatre documents ont été réalisés : la *policy*, des *guidelines* (une liste de directives), des *practical interpretations* (instructions pratiques), et un résumé d'une page qui présente la *policy*. Vous trouverez tout cela, sur sharepoint à l'adresse suivante :

<https://eu-sharepoint.corp.verio.net/sites/quality/Policies/Forms/AllItems.aspx>

Cette *policy* définit les quatre niveaux de confidentialité utilisés par Verio. Chaque document (physique ou électronique) doit comporter un niveau de sécurité qui donne des informations sur la façon dont il peut être diffusé. Voici une description des quatre niveaux :

**Company Secret (Secret d'entreprise)** - Documents contenant des informations dont la divulgation non autorisée dans et hors de Verio pourrait nuire gravement aux intérêts de la société. Cela peut concerner les fusions, les acquisitions, les informations sur la concurrence, les accords avec des partenaires et des entreprises etc. Ce niveau est utilisé assez rarement.

**Restricted Circulation (Diffusion restreinte)** – Informations dont la divulgation non autorisée dans et hors de Verio causerait de considérables préjudices pour la société. Cela peut concerner des informations sur des négociations, sur le marketing, sur les clients ou des informations personnelles.

**Confidential (Confidentiel)** – Ce niveau couvre la majorité des documents dont la diffusion est libre au sein de Verio mais pas en dehors de la société. La divulgation de tels documents hors de Verio doit être justifiée et requiert l'aval de son propriétaire. C'est le niveau de sécurité « par défaut », il n'est pas obligatoire de la faire apparaître en toute lettre sur les documents.

**Public Information (Diffusion publique)** - Entrent dans cette catégorie les informations dont la diffusion auprès du public a été clairement autorisée et peut s'effectuer sans restriction. Leur diffusion s'effectue le plus couramment dans les brochures commerciales de l'entreprise ou sur son site Web.

Les Guidelines et les instructions pratiques expliquent la façon de protéger les informations pour chaque niveau de sécurité.

## Trucs et Astuces

Le mot de passe CORP – Depuis plusieurs mois déjà un effort a été réalisé pour centraliser les mots de passe. Désormais pour vous logger sur votre PC, mais aussi pour accéder à des applications telles que GMP, PRISM, GAIM/jabber un seul mot de passe est nécessaire : le mot de passe CORP.

Pour le changer : CTL + ALT + SUPP puis cliquez sur « modifier le mot de passe ».

## Evènements

BS7799 – France – Champagne ! Après l'audit du 29 septembre, la France a été recommandée pour la certification BS7799. (plus exactement, La certification BS7799 Verio a été étendue à la France).

## Liens

Le Site Web "IS & QA" rubrique "Information Security Guidelines library" contient cette newsletter, des infos pratiques et des annonces. N'hésitez pas à y jeter un œil à

<https://eu-sharepoint.corp.verio.net/sites/quality/default.aspx>

[Nwheelwright@verio.net](mailto:Nwheelwright@verio.net)  
[lcaudy@verio.net](mailto:lcaudy@verio.net)

Devon House, +44 207 767 3724  
Suresnes, +33 1 41 38 74 96

# Lessons

- Don't go straight to the controls
  - **Remember Sections 4 to 8 – The REQUIREMENTS**
  - **( ISMS / Management Responsibility / Internal ISMS Audits / Management Review of ISMS / ISMS Improvements )**
- Ensure management input & INVOLVEMENT
- Cross reference documents – including to control references
- The reason 'to be secure' may not work - be honest, it will be either regulatory or marketing reasons!
- Resources
- ISO9000 issues
  - **ISO27001 is aligned with ISO9001**
  - **ISO9001 requires several policies (corrective actions, etc)**
  - **These should be in place for ISO27001**

# Commercial Use of ISO27001 Certification



Why did NTT Europe Online certify to ISO27001?

How do we use the certification?

# NTT Europe Online

NTT Europe Online designs, deploys and manages critical internet infrastructure, managed security and application services for businesses globally

Our dealers are located throughout the UK. Locate your nearest dealer by entering your Postcode below.

Nissan has put together a selection of great offers for you. Visit our special offers page to see details. And once you've found

Your gateway to the Earth's wilder reaches. You'll meet the people who know these breathtaking but inhospitable landscapes and

# External Proof of Reliability and Security



Home Who we are How we work Case studies Products & services Partners Contact us

**What our customers say...**

**NTT Europe Online** was the obvious choice for hosting services. It is a large and stable company, has a flexible and pragmatic approach and an **excellent reputation for service quality**

Willy Goldschmidt  
Commercial Development Director, Xansa

- ▶ Are you looking for **Software as a Service Hosting?**
- ▶ Are you looking for **The Gartner Magic Quadrant?**
- ▶ Are you looking for **Information Security Management?**
- ▶ Are you looking for **Business Continuity?**

- Case studies**
- ▶ **Managed Hosting and Application Management - Nissan** - Nissan guarantees its growing European web presence with the help of NTT Europe Online.
  - ▶ **Online Share Trading and Banking - Boursorama** - Online share trading and banking provider Boursorama reaps the dividends of hosting with NTT Europe Online.

- Our products & services**
- ▶ **Managed hosting** - Reliable, available, secure and scalable managed hosting services from NTT Europe Online.
  - ▶ **Security Management** - Secure your online infrastructure and the continuity of your business with NTT Europe Online's managed security services.
  - ▶ **Application management** - Outsource the management of operating system, middleware and database solutions, as well

- Latest News**
- ▶ 20 Nov 2006: **SaaS Alliance with Microsoft** - NTT Europe Online and Microsoft announce alliance enabling ISVs to adopt Software as a Service business models
  - ▶ 10 Nov 2006: **UEFA Video Service** - Innovative online video service provides live UEFA Champions League football to fans globally
  - ▶ 20 Oct 2006: **NTT Europe Online** -



# Customer Facing Documentation



Sales Proposal for

**Customer Name or  
Project Name**

Logo position, delete  
if not required

Prepared by:	Name
Title:	Sales Proposal: Sample Customer 3
Version:	May 2005 v1.0
Distribution:	CONFIDENTIAL
Sales office region:	Region name

Copyright © 2006 NTT Europe Online



# Business Continuity

- Live Environment
- High Availability Configurations
- Global Load Balancing
- Disaster Recovery
- Pre-Production Environments
- Testing Environment
- Multiple Data Centres
- Business Continuity
- Reliability, Scalability, Security

NTT Europe Online has its own Business Continuity Plan to protect its business in the event of difficulties.

The BCP is tested in all countries every six months and independently audited by Lloyd's Register



# Security as Competitive Advantage

- Point Solutions (FW, AV,IPS etc)
- Unified Threat Management
- OS Hardening and Security Patch Management
- Backup Strategy
- Vulnerability Scanning
- Forensic Penetration Testing
- Secure Authentication Services
- ISO 27001 Certification

Necessary Evil  
 Cost Centre  
 Vulnerability  
 Internal Competence

Brand Enhancement  
 Reputation Management  
 Risk Reduction  
 Shareholder Value  
 Market Leading



### Xansa

Xansa is an outsourcing and technology company, offering business and technology consulting, IT implementation, IT outsourcing and business process outsourcing

#### REQUIREMENT:

Xansa were looking for a hosting partner to underpin a web services platform for three major Government departments:

- Directgov (Cabinet Office)
- Department of Health
- Department of Education and Skills (DfES)

#### SOLUTION:

- Shared services platform for government departments:
  - o Shared development resources
  - o Common functionality
  - o Allows re-use of components
  - o Reduces time to market and cost
- Multi-environment solution
- Disaster recovery site
- Secure Content Delivery
- Tailored SLA offering 99.8% solution availability



NTT Europe Online was the obvious choice for hosting services. It is a large and stable company, has a flexible and pragmatic approach and an excellent reputation for service quality.

Willy Goldschmidt, Commercial Development Director, Xansa

Thank you

[robert.steggles@ntt.eu](mailto:robert.steggles@ntt.eu)  
[neil.wheelwright@ntt.eu](mailto:neil.wheelwright@ntt.eu)

NTT Europe Online,  
22 Quai Gallieni  
92158 Suresnes