ARCAD for Compliance

SOLUTION WHITE PAPER

www.arcadsoftware.com

1. Executive Summary

As if IT staff didn’t have enough to worry about. They also have to ensure that they adhere to an abundant, confusing and ever changing array of industry and regional compliance requirements. An increasingly difficult task in today’s decentralized, multi-platform and mobile world with an ever faster software delivery mandate.

The good news is that many of the compliance requirements are being consolidated. Best practices are emerging which help ensure IT staff remain in compliance with all requirements, past present and hopefully future irrespective of industry sector or geographical region.

This paper is for anyone who is considering the impact of compliance requirements on IT staff who has an environment which includes IBM Power Systems IBM i.

This paper summarizes a sample of compliance requirements from around the world and the best practices emerging for IT staff. This paper also identifies how ARCAD tools aid the implementation of these emerging best practices.

Compliance is a hot issue for IT staff and for good reason. Data and applications have become a pervasive component of modern business and these have become a subject of new and diverse compliance requirements. Failure to comply could mean fines, penalties, loss of trust, even imprisonment.

‘Compliance is concerned with laws that a business must obey or risk legal sanctions up to and including prison for its officers’

– Gartner

The rapid evolution of technology is making the world smaller. This helps fuel company expansion and acquisitions. This in turn causes application environments to become more complex which increases the chances of ‘dropping the ball’ when it comes to compliance.

Pioneering governments have invented their own regional compliance requirements for specific industry sectors and these often influence other regions to adopt similar measures.

High profile companies are not immune to compliance scandals and when these events happen it puts pressure on governments and governing institutions to expand and strengthen existing requirements, invent new ones and stiffen penalties.

‘It takes 20 years to build a reputation and five minutes to ruin it! If you think about that, you`ll do things differently.’

- Warren Buffet

For IT staff, understanding compliance requirements can be difficult and frustrating. IT staff generally are not experts in law and lawyers who are involved in writing the requirements are not experts in IT. The language which described compliance requirements is therefore difficult to align with specific IT requirements.

This problem is compounded by the growing number and diversity of requirements which span different industry sectors and geographical regions. These requirements are constantly evolving. Where businesses operate internationally they will likely be subjected to different compliance requirements concurrently.

The good news is that governments and governing institutions are aware of the problem and are consolidating the requirements to make them easier to understand and implement.

The DevOps culture is breaking down the traditional silos of Development, QA and Operations. This is leading to a concern that a ‘wild west’ ecosystem will emerge where everyone has access to all production applications and sensitive data.

‘DevOps oriented approaches often lack foresight into compliance obligations’

- Gartner

The days of showing the auditor your physical paper audit trail are gone. Instead, IT staff need to find automated solutions. Automation is the key to avoiding the ‘wild west’ and simplifying adherence to compliance requirements with a *‘compliance by design*’ culture.

‘Compliance requirements may be complex, but having IT staff meet them doesn't have to be’

- Philippe Magne, ARCAD Software

2. Sample of Compliance Requirements from Around the World

Global

Abbreviation	Name	Requirement
Basel	Basel accords	Accord I - Minimum capital requirements for banks Accord II - Ensure that a bank has adequate capital for the risk the bank exposes itself to through its lending, investment and trading activities Accord III, Further strengthen bank capital requirements by increasing bank liquidity and decreasing bank leverage
COBIT	Control Objectives for Information and Related Technology	Framework created by ISACA for information technology (IT) management and IT governance
COSO	Committee of sponsoring organizations of the Treadway commission	Thought leadership to executive management and governance entities on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting
ISO 19779/27001	International standards organization	Family of standards for IT asset management (ITAM) address both the processes and technology for managing software assets and related IT assets
ITIL	IT Infrastructure library	Set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business
PCI DSS	Payment card industry data security standard	Information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB

North America

Abbreviation	Name	Requirement
CMMI	Capability maturity model integration	Often required for US government and defence contracts. Used to guide process improvement across projects, divisions or organizations, particularly especially in software development
GLBA	US - Graham Leach Bliley Act	Enhancement of competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, and other

		financial service providers, and for other purposes
HIPPA	US - Health insurance portability and accountability act	Title I, protects health insurance coverage for workers and their families when they change or lose their jobs Title II, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers
PIPEDA	Canada - Personal information protection and Electronic documents act	Governs how private sector organizations collect, use and disclose personal information in the course of commercial business
SOX	US - Sarbanes-Oxley Act	Federal law that sets new or expanded requirements for all U.S. public company boards, management and public accounting firms. There are also a number of provisions of the Act that also apply to privately held companies, for example the wilful destruction of evidence to impede a Federal investigation

Europe

Abbreviation	Name	Requirement
BDSG	Germany - Federal Data Protection Act	Laws which govern the exposure of personal data, which are manually processed or stored in IT systems
Directive 2006/24/EC	EU – Data retention directive 2006/24/EC of the European parliament and council	Security directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks
Directive 95/46/EC	EU – Data protection directive 95/46 of the European parliament and council	Protection of individuals with regard to the processing of personal data and on the free movement of such data
DPA-Swiss	Switzerland – Swiss federal data protection act	Applies to the processing of personal data by private persons and federal government agencies. Unlike the data protection legislation of many other countries, the DPA protects both personal data pertaining to natural persons and legal entities
DPA-UK	UK – Data Protection Act 1998	Laws which govern the protection of personal data of identifiable living people
Euro-SOX	EU – 8th European Union company law directive	EU law which aims to ensure that investors and other interested parties can fully rely on the

		accuracy of audited accounts.
GDPR	EU – General data protection regulation	Effective in 2018, GDPR will extend the scope of existing EU data protection laws to all foreign companies processing data of EU residents. It consolidates existing EU data protection laws which makes it easier for non-EU companies to comply. GDPR includes an audit regime with severe penalties for non- compliance
VDS	Germany - Telecoms Data Retention Act	Seeks to make law enforcement more effective in the face of increasingly pervasive information and communications technologies

Asia-Pacific

Abbreviation	Name	Requirement
APP	Australia – Australian privacy principles, schedule 1 of the Privacy Act 1988	Outline how most Australian and Norfolk Island government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses must handle, use and manage personal information
APRA	Australia – Australian prudential regulation authority	Regulates banks, general and life insurance companies, superannuation funds, credit unions, building societies and friendly societies to ensure that these institutions keep their financial promises; that is, that they will remain financially sound and able to meet their obligations to depositors, fund members and policy holders
CLERP 9	Australia – Corporate law economic program	The CLERP 9 changes were intended to improve investor confidence in relation to listed corporations and their financial reports
JPIPA	Japan – Japan personal information protection act	Protection of individuals with regard to the processing of personal data and on the free movement of such data. (Similar to Directive 95/46/EC)
J-SOX	Japan – Financial instruments and exchange act	The main statute codifying securities law and regulating securities companies in Japan
RTI	India – Right to information act	The right to information for citizens to secure access to information under the control of public authorities, in order to promote transparency and accountability

Latin America

Abbreviation	Name	Requirement
Azeredo	Brazil – Azeredo data protection act	Creates rights for those who have their data stored, and responsibilities for those who store, process or transmit such data
Bill 6891/02	Brazil – Draft bill for the protection of personal data	The draft bill applies to individuals and companies that process personal data via automated means, provided that the processing occurs in Brazil or personal data was collected in Brazil
Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Mexico - Federal law on the protection of personal data possessed by private persons	Protection of individuals with regard to the processing of personal data and on the free movement of such data. (Similar to Directive 95/46/EC)

2. Overlapping Compliance Requirements

It has become clear that the abundance of overlapping compliance requirements has made it difficult and expensive for businesses to comply. The good news is that governments and governing institutions are aware of this and are taking steps to consolidate the requirements.

One example of consolidation is the European Union general data protection regulation (GDPR) which from 2018 consolidates existing EU data protection requirements and makes it easier for EU and non-EU companies to comply. GDPR goals include the following:

One continent, one law - A single set of rules will make it simpler and less expensive for businesses to comply with requirements within the EU.

One-stop-shop - Businesses will only have to deal with a single supervisory authority.

EU rules on EU soil - Businesses based outside the EU must adhere to the same rules as all EU based businesses when offering services in the EU.

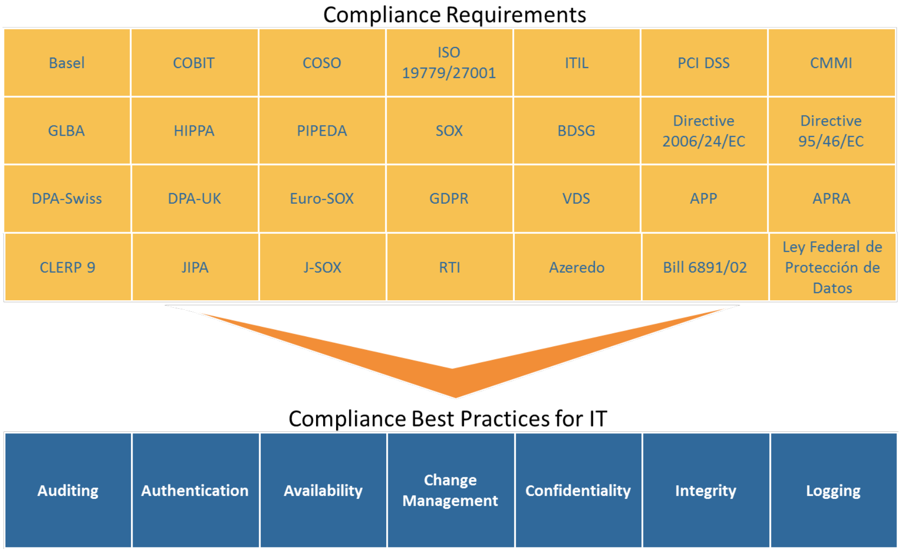
Risk-based approach - Rather than a one-size-fits-all requirement, smaller businesses will have lighter compliance requirements appropriate to the respective level of risk they represent.

Rules fit for innovation - Requirements will guarantee that data protection safeguards are built into products and services from the earliest stage of development (*Data protection by design*).

> ‘Due to the growth of regulations, organizations are increasingly adopting consolidated and harmonized sets of compliance controls. This approach ensures all necessary requirements can be met without duplication of effort’
>
> – Wikipedia

3. Compliance Best Practices for IT

Overlapping compliance requirements have resulted in the emergence of compliance best practices for IT. These consolidate compliance requirements into a single set of requirements which are easier for IT staff to follow. It doesn’t matter if we have to comply with SOX, HIPPA, GDPR or other because of the high level of overlap. The geography and industry sector may vary but the best practices remain the same.



Compliance Requirements

Basel	COBIT	COSO	ISO 19779/27001	ITIL	PCI DSS	CMMI
GLBA	HIPPA	PIPEDA	SOX	BDSG	Directive 2006/24/EC	Directive 95/46/EC
DPA-Swiss	DPA-UK	Euro-SOX	GDPR	VDS	APP	APRA
CLERP 9	JIPA	J-SOX	RTI	Azeredo	Bill 6891/02	Ley Federal de Protección de Datos

Compliance Best Practices for IT

Auditing	**Authentication**	**Availability**	**Change Management**	**Confidentiality**	**Integrity**	**Logging**

Fig 1 ~ Compliance requirements are being consolidated

Best Practice 1 Auditing

It must be possible to audit IT staff activities. It must also be possible to audit existing software applications for quality and impact of changes.

- 1.1 Duplicate and obsolete versions of source code and objects must be auditable
- 1.2 Assessing the impact of making changes must be auditable
- 1.3 Code quality must be auditable to uncover levels of technical debt(1)
- 1.4 Changes to source code and objects must be auditable
- 1.5 Changes to configuration data(2) must be auditable
- 1.6 Application testing must be auditable
- 1.7 Transfers to production must be auditable
- 1.8 Assessing the impact of third party application changes must be auditable

Best Practice 2 Authentication

Individual members of IT staff must be uniquely and reliably identified. Unauthorized access must be prevented. IT staff must not have more authority than they need. IT staff must have clear roles so that it is easy to expose abuse cases.

- 2.1 User profiles must enforce strong passwords. IT staff must not share user profiles. Inactivity must cause automatic log-off
- 2.2 Limit authority of IT staff only to libraries, objects and commands they need
- 2.3 IT staff must have clear roles

Best Practice 3 Availability

Application availability must be maximized. Most downtime is caused by application failures rather than equipment failure or disaster. Poor code quality and poor testing have been identified as the lead causes of application failures and security breaches.

- 3.1 Reduce application downtime by improved testing with realistic test data
- 3.2 Reduce application downtime by improved, repeatable test procedures
- 3.3 Reduce application downtime when promoting changes to production

(1) Technical debt ~ (also known as design debt or code debt) is a concept in programming that reflects the extra development work which arises when code that is easy to implement in the short run is used instead of applying the best overall solution. A high level of technical debt represents a ticking time bomb in terms of causing application downtime in the future due to software errors.

(2) Configuration data ~ this is data stored in software application configuration files which determines how the application will behave. (Also known as parameter data or metadata).

- 3.4 Reduce application downtime when applying third party vendor release upgrades and service packs
- 3.5 Reduce application downtime by better understanding all the impacts of changes
- 3.6 Proactively identify weak code to avoid downtime from happening

Best Practice 4 Change Management

Application changes must be carefully managed because they can introduce risks. Fraud generally comes from disgruntled employees. IT staff must be held accountable for changes made to software applications. Applications must be protected from accidental or malicious changes by IT staff.

- 4.1 Avoid accidental errors or malicious acts when making source code changes
- 4.2 Avoid accidental errors or malicious acts when modernizing applications
- 4.3 Avoid accidental errors or malicious acts when re-compiling changed objects
- 4.4 Avoid accidental errors or malicious acts when testing software changes
- 4.5 Avoid accidental errors or malicious acts when deploying changes to production
- 4.6 Avoid accidental errors or malicious acts when introducing third party software to production

Best Practice 5 Confidentiality

Confidential information cannot be exposed to unauthorized IT staff.

- 5.1 IT staff must apply the principles of least authority to sensitive data and avoid authority escalation
- 5.2 Mask (obfuscate) sensitive production data from developers, testers an operators

Best Practice 6 Integrity

Evidence must be provided to show that sensitive production data has not been accidentally or maliciously modified by IT staff.

- 6.1 Production data must not be modified by unauthorized IT staff
- 6.2 Configuration data must not be modified by unauthorized IT staff
- 6.3 IT staff are responsible for introducing third party changes to production

Best Practice 7 Logging

Any IT action which might need to be audited must be logged. The logs must resist tampering.

- 7.1 Log all changes to source code
- 7.2 Log all changes to configuration data
- 7.3 Log all changes to objects re-compilation
- 7.4 Log all application tests
- 7.5 Log all deliveries to production
- 7.6 Log all third party changes to production

4. IT Staff Must Take Compliance Seriously

Some IT myths about compliance:

- MYTH 1 - Compliance is something only senior management must worry about
- MYTH 2 - Compliance only applies to the business and not to IT staff
- MYTH 3 - Compliance is so confusing that it’s impossible to implement fully so why bother
- MYTH 4 - Compliance failures will have no consequences for IT staff

‘IT staff are centre stage
for compliance accountability’
- Philippe Magne, ARCAD Software

All modern business stores and processes data. Much of the stored data is about customers and suppliers and this is sensitive. Most compliance requirements relate to the protection of sensitive data and the safeguards around the changes to software which manipulate that data, this puts IT staff centre stage for compliance accountability.

IT staff are in a unique position of trust within most businesses and they cannot totally avoid exposure to sensitive data and the software which manipulates that data. Pretending that compliance doesn’t apply to IT staff is akin to telling a police officer that you were speeding because you were ignorant of the speed limit.

. ARCAD Tools Simplify Compliance for IT

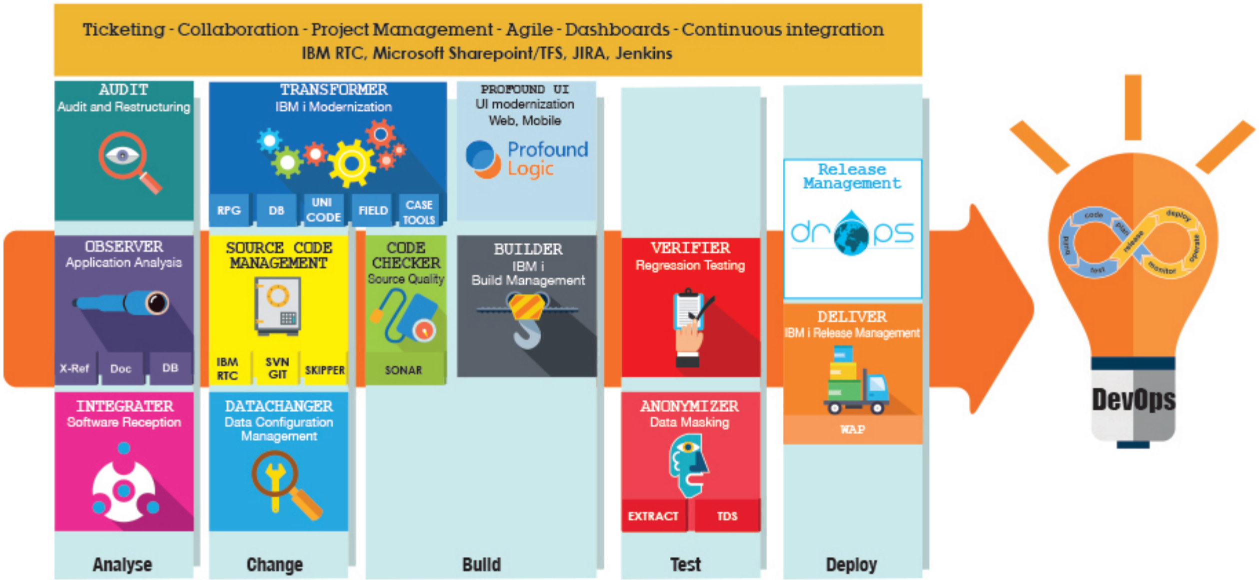


Fig 2: ARCAD tools simplify compliance through automation

ARCAD tools span the full scope of DevOps activities and have been built from the start to be *compliance ready*. ARCAD tools automate the compliance process by design. Automation is the key to simplifying compliance for IT staff. ARCAD tools have been designed to enable IT staff to go about their business unhindered and keep them compliant automatically.

'ARCAD tools have been designed to enable IT staff to go about their business unhindered and keep them compliant automatically'

- Philippe Magne, ARCAD Software

Below is a list of ARCAD tools and a description of the compliance best practices each tool automates:

All ARCAD Products

- Authentication 2.3 IT staff must have clear roles
- Confidentiality 5.1 IT staff must apply the principles of least authority to sensitive data and avoid authority escalation

ARCAD Anonymizer – IBM i data masking

- Availability 3.1 - Reduce application downtime by improve testing with realistic test data
- Confidentiality 5.2 - Mask (obfuscate) sensitive production data from developers, testers an operators

ARCAD Builder – IBM i build management

- Auditing 1.7 - Transfers to production must be auditable
- Change Management 4.3 - Avoid accidental errors or malicious acts when re-compiling changed objects
- Logging 7.3 - Log all object re-compilation

ARCAD Audit – IBM i audit and restructuring

- Auditing 1.1 - Duplicate and obsolete versions of source code and objects must be auditable

ARCAD Code Checker – IBM i source quality auditing

- Auditing 1.3 - Code quality must be auditable to uncover levels of technical debt
- Availability 3.6 - Proactively identify weak code to avoid downtime from happening

ARCAD Data Changer – IBM i data configuration management

- Auditing 1.5 - Changes to configuration data must be auditable
- Integrity 6.2 - Configuration data must not be modified by unauthorized users
- Logging 7.2 - Log all changes to configuration data

ARCAD Deliver – IBM i release management

- Availability 3.3 - Reduce application downtime when promoting changes to production
- Change management 4.5 - Avoid accidental errors or malicious acts when deploying changes to production
- Integrity 6.1 - Production data must not be modified by unauthorized IT staff
- Logging 7.5 - Log all deliveries to production

ARCAD Integrater – IBM i software reception management

- Auditing 1.8 - Third party application changes must be auditable
- Availability 3.4 - Reduce application downtime when applying third party vendor release upgrades and service packs
- Change management 4.6 - Avoid accidental errors or malicious acts when introducing third party software to production
- Integrity 6.3 – IT staff are responsible for introducing third party changes to production
- Logging 7.6 - Log all third party changes to production

ARCAD Observer – IBM i application analysis

- Auditing 1.2 - Assessing the impact of making changes must be auditable
- Availability 3.5 - Reduce application downtime by better understanding all the impacts of changes

ARCAD Skipper – IBM i source code management

- Auditing 1.4 - Changes to source code and objects must be auditable
- Change management 4.1 - Avoid accidental errors or malicious acts when making source code changes
- Logging 7.1 - Log all changes to source code

ARCAD Transformer – IBM i modernization

- Change management 4.2 - Avoid accidental errors or malicious acts when modernizing applications

ARCAD Verifier – IBM i regression testing

- Auditing 1.6 - Application testing must be auditable
- Availability 3.2 - Reduce application downtime by improved, repeatable test procedures
- Change management 4.4 - Avoid accidental errors or malicious acts when testing software changes
- Logging 7.4 - Log all application tests

ARCAD TDS – IBM i test data synchronization

- Availability 3.1 - Reduce application downtime by improved testing with realistic test data

ARCAD WAP – IBM i while active promotion

- Availability 3.3 - Reduce application downtime when promoting changes to production

DOT Anonymizer – Multi-platform data masking

- Availability 3.1 - Reduce application downtime by improved testing with realistic test data
- Change management 5.2 - Mask (obfuscate) sensitive production data from developers, testers an operators

DOT Verifier – Multi-platform regression testing

- Auditing 1.6 - Application testing must be auditable
- Availability 3.2 - Reduce application downtime by improved, repeatable test procedures
- Change management 4.4 - Avoid accidental errors or malicious acts when testing software changes
- Logging 7.4 - Log all application tests

DROPS – Multi-platform release management

- Availability 3.3 - Reduce application downtime when promoting changes to production

- Change management 4.5 - Avoid accidental errors or malicious acts when deploying changes to production
- Integrity 6.1 - Production data must not be modified by unauthorized IT staff
- Logging 7.5 - Log all deliveries to production

IBM i operating system security

- Authentication 2.1 - User profiles must enforce strong passwords. Users must not share user profiles. Inactivity must cause automatic log-off
- Authentication 2.2 - Limit authority of signed on users only to libraries, objects and commands which they need
- Confidentiality 5.1 – IT staff must apply the principles of least authority to sensitive data and avoid authority escalation

IBM i Rational Team Concert – Multi-platform source code management

- Auditing 1.4 - Changes to source code and objects must be auditable
- Change management 4.1 - Avoid accidental errors or malicious acts when making source code changes
- Logging 7.1 - Log all changes to source code

6. Conclusions

Abundant overlapping compliance requirements are being consolidated by governments and governing institutions.

IT compliance best practices are emerging which are easier for IT staff to implement.

Most compliance requirements relate to the protection of sensitive data and the safeguards around the changes to software which manipulates that data.

This puts IT staff centre stage for compliance accountability. All IT staff must take compliance seriously.

Compliance doesn't have to be complex, the key is automation. ARCAD tools span the full scope of IT activities and are built from the start to be compliance ready.

Implementing ARCAD tools will help automate compliance and go a long way towards making your business compliant no matter which regulations apply.

www.arcadsoftware.com

North America
ARCAD Software Inc.
1 Phoenix Mill Lane, Suite 203
Peterborough NH 03458
USA
1-800-676-4709 (toll free)
1-603-371-9074
1-603-924-7377 (fax)
sales-us@arcadsoftware.com

Asia
ARCAD Software Asia
Room 22, Smart-Space 3F
Unit 908-915, Level 9, Cyberport 3
100 Cyberport Road
Hong Kong
+852 3618 6118
sales-asia@arcadsotware.com

Europe (head office)
ARCAD Software
55, rue Adrastée – Parc Altaïs
F-74650 Chavanod/Annecy
France
+33 450 578 396
+33 450 575 279 (fax)
sales-eu@arcadsoftware.com

Sweden
ARCAD Software Nordic AB
Prostvägen 36
141 43 HUDDINGE

+46(0) 70-793 6570
sales-se@arcadsoftware.com

Germany
ARCAD Software Deutschland
GMBH
Richardstr. 84
22089 Hamburg
+49 40 357 09 10-2
+49 40 357 09 10-6 (fax)
sales@arcadsoftware.de