PERRY JOHNSON
REGISTRARS, INC.

STEPS TO
ISO/IEC 27001:2005
REGISTRATION

755 W. Big Beaver Rd., Suite 1340
Troy, Michigan U.S.A. 48084
1-800-800-7910 • (248) 358-3388
Fax: 248-358-0882 • www.pjr.com

Steps to ISO/IEC 27001 Registration

Perry Johnson Registrars, Inc.
755 W. Big Beaver Rd., Suite 1340
Troy, Michigan 48084 USA

Table of Contents

Foreword

In response to the exponential growth of global technology and rising threats to information security, the ISO/IEC JTC 1 produced **ISO/IEC 27001:2005** Information Technology – Security Techniques – Information Security Management Systems - Requirements; a standard which provides a model for establishing, implementing, operating, monitoring, reviewing and improving an Information Security Management System (ISMS).

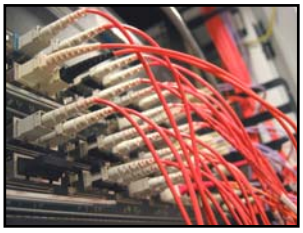
In the business world, it is important to safeguard information in order to minimize risks and operate effectively. As with all other information security standards, this standard also aids trading in a trusted environment. It affects companies where critical infrastructure protection is necessary. The standard defines the best practice controls that meet the information security requirements of an organization. It helps protect the confidentiality, integrity and availability of all kinds of information, including intellectual property.

ISO/IEC 27001:2005 was drafted to facilitate the selection of sufficient and appropriate security controls to protect information assets. The standard is a replacement for BS 7799 part 2: 2002, a long established standard first published in the 1990s. **ISO/IEC 27001:2005** has taken this standard into consideration making it easy to upgrade from BS 7799.

This booklet, **Steps to ISO/IEC 27001:2005 Registration**, was created by **Perry Johnson Registrars** to give companies a clear understanding of the complete process. We hope this booklet serves as an aid in helping your company become a member of the world's elite club for information security management.

Terry Boboige,
President - Perry Johnson Registrars

What is ISO/IEC 27001:2005?



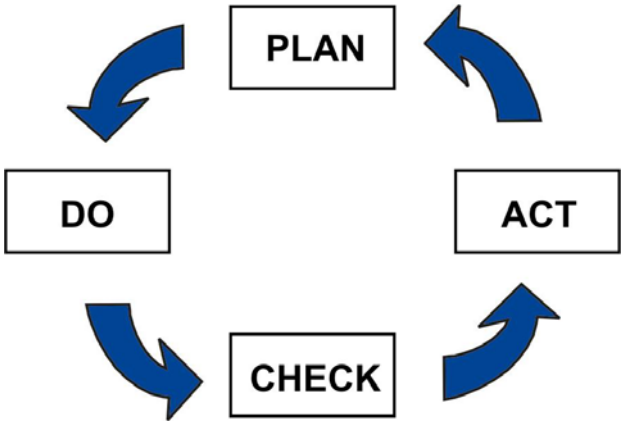
ISO/IEC 27001:2005 is the new international Information Security Management System (ISMS) standard that has replaced BS 7799-2:2002 since October 2005. The standard provides specification for an ISMS through a Six Stage Process. **ISO/IEC 27001:2005** serves to assess conformance by third parties and aligns with other management standards such as ISO 9001 and ISO 14001. The basic objective of the standard is to help establish and maintain an effective information security management system, using a continual improvement approach.

The content of **ISO/IEC 27001:2005** is similar to BS 7799-2:2002. It includes cross-reference to ISO 17799:2005 controls, use of the "Plan-Do-Check-Act" (PDCA) model, terms and definitions, among others.

The standard follows the "process approach", which is the application of a system of processes within an organization, together with the identification and interactions of these processes, and their management. This process approach, along with the PDCA model, enables the organization to function effectively by implementing risk prevention and security management.

- **PLAN:** Establish ISMS policy, objectives, processes and procedures relevant to the organization's Information Security needs.
- **DO:** Implement and operate policy, controls, processes & procedures of the ISMS.
- **CHECK:** Monitor and review the ISMS. Assess and measure performance against ISMS objectives and practical experience. Report results to management for review.

THE PDCA MODEL



- **ACT:** Maintain & improve the ISMS. Based on internal audits, management review and other relevant information, take corrective & preventive actions for continual improvement.

Approach to ISO/IEC 27001:2005

There are multiple ways to approach this standard. ISO and IEC suggest that you begin by identifying your organization's information security risks and needs. The right approach will be unique to each organization depending on the nature of these risks & needs. However, the following can be used as a general guideline.

- Obtain a copy of the standard. While this may seem obvious, many times people attempt to evaluate suitability without having studied the documents.
- Consider the merits of the standard, such as impact on confidence of customers and partners, improving the organization's security, etc.
- Decide to move forward with the standard – you can choose to comply with it, or better still, to obtain certification.
- Determine the scope of the exercise and plan the resources.
- Review existing documentation to assess the extent and quality of measures already in place and draw an inventory of significant information assets.
- Perform a "gap analysis" to identify the gaps between the existing security systems and the controls and processes outlined in the standard.
- Conduct a risk analysis and create a Risk Assessment document.
- Determine how the risks are to be managed. Assign and document responsibilities for managing them.
- Select controls to address the identified risks and develop a Statement of Applicability.
- Using the Statement of Applicability and other inputs, create Security policies.
- Create appropriate procedures.
- Initiate an awareness program to ensure employees and partners are familiar with the ISMS requirements of the organization. Introduce a method of compliance monitoring.
- Review your position. Consider certification – it requires external audits by an accredited body.

The Benefits of Registration

Registering to **ISO/IEC 27001:2005** brings to your company several benefits:

Access to Global Marketplace

- You will gain global recognition in both public and private sectors as an organization committed to information security. Your registration certificate, issued by an independent, third party registrar, will provide objective evidence of that commitment.

International Standards

- **ISO/IEC 27001:2005** is the most widely recognized standard that has been developed for managing information security. It establishes a common language on information security for all organizations around the world. In addition to helping you gain access to the global marketplace, **ISO/IEC 27001:2005** registration is a sure way to verify that your Information Security Management System (ISMS) is meeting international standards.

A Market Differentiator

- Information in its various forms is the most important asset to any organization and is essential to the continuity of its business. For most businesses, information security may be necessary to maintain competitive edge, cash flow, profitability, legal compliance and commercial image. But many businesses and most non-business organizations may hold information as their only asset. An absence of information security may threaten their integrity and existence.

- Users of this standard can demonstrate to their business partners and customers that they are fit and secure enough to do business, helping them translate their investment in information security into business-enabling opportunities.

International Recognition/A Publicity Vehicle

- When your company achieves **ISO/IEC 27001:2005** registration, you will be presented with a certificate of approval, bearing a registration mark. This mark can be used in advertising and promotional literature to show potential customers that your company is committed to quality. You will also receive a registration letter, which can be a powerful strategic tool.

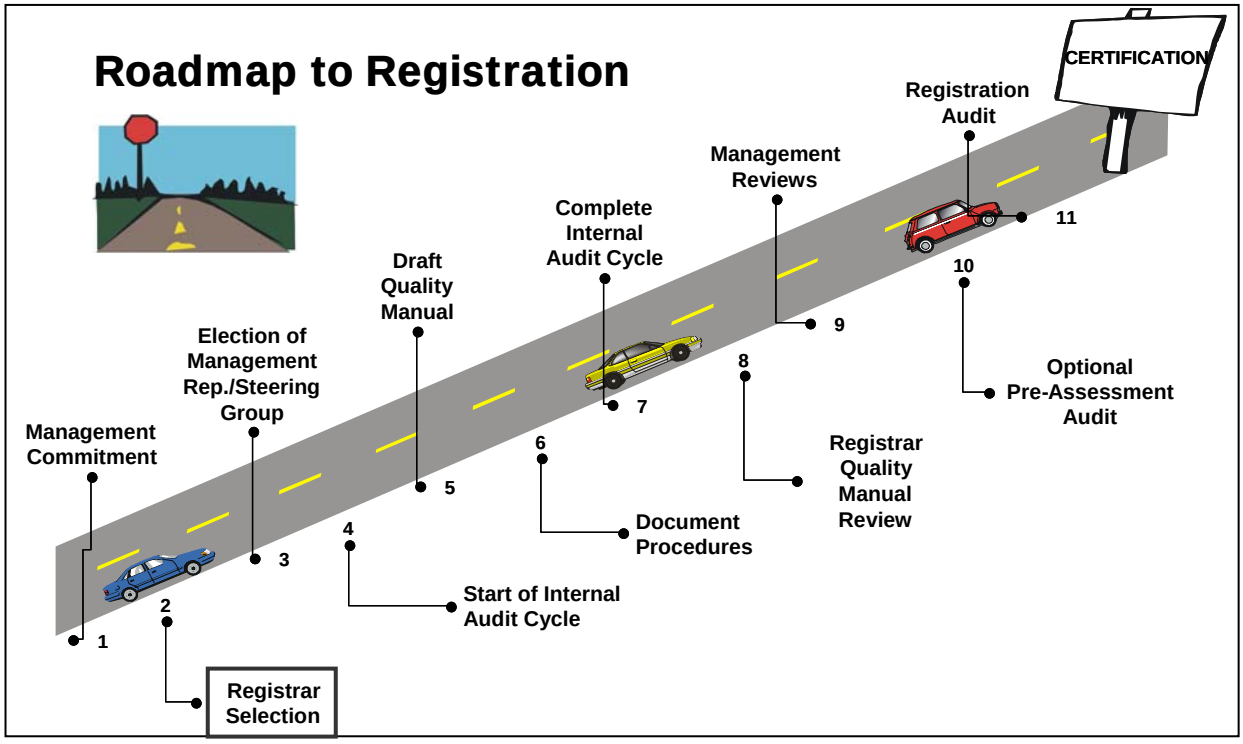
A Strong Competitive Edge

- As you can see, **ISO/IEC 27001:2005** can be a valuable tool. By becoming registered, you can look forward to an efficient information security system that safeguards accuracy of information and ensures that authorized users have access to information when necessary.

The Road to Registration

The Road to Registration requires an organization to establish clear targets for implementation and assessment. When your company is seeking registration, the following are the basic steps to consider:

- Management Commitment
- Choosing a Registrar
- Selection of a Management Representative and Team
- Start the Internal Audit Cycle
- Training & Consultancy Options
- Development and implementation of a documented management system to meet the requirements of the standard
- Complete the Internal Audit Cycle & Management Reviews
- Complete the Registration Process



Registration by an independent 3rd party such as **PJR**, offers objective evidence to the world that your organization has met the requirements of a rigorous standard and is committed to focusing on customer requirements and customer satisfaction.

Once you have completed the registration process and received your **ISO/IEC 27001:2005** registration certificate, zinc-etched plaque and letter, you will earn valuable recognition in the industry. In addition, **ISO/IEC 27001:2005** is an international standard, you will gain a greater footing in the international marketplace.

Choosing a Registrar

The global technology boom demands increased security measures to safeguard information. Threats such as computer assisted fraud; espionage and hacking are not uncommon for organizations and their information systems. Today's global business practices mandate organizations to seriously look in to the security concerns of their information systems.

A key ingredient of the **ISO/IEC 27001:2005** recipe for information security is third-party registration. A company cannot become registered until it hires an accredited registrar to carry out a complete and thorough audit of its information security management system (ISMS).

The registrar is responsible for gathering *objective/audit evidence* to determine whether your information system conforms to **ISO/IEC 27001:2005** requirements. The registrar ultimately decides whether or not to grant registration to a company.

Knowing this, you should study potential registrars' credentials carefully. To assist you in selecting a registrar best suited for your company's needs, examine the following key areas:

Key Questions to Consider

- Is the registrar qualified to grant registration to the information security management system (ISMS) you have implemented?
- Does the registrar have auditors qualified to conduct audits in your industry? In addition, are these auditors located in geographic areas close to your organization?
- Does the registrar meet the appropriate SIC, EA or NACE codes for your scope of business? Do they meet the background requirements for **ISO/IEC 27001:2005** auditors as well?
- Is the registrar willing to provide you with a complete description of its registration process? Find out if there are any policies, contract restrictions or **ISO/IEC 27001:2005** limitations that may affect you.
- Is the registrar's name recognized? Check to see if people have heard of the company. When you buy a car, the manufacturer's name plays a significant role. The same holds true for registrars.
- Is the company financially stable? Will the registrar still be in business during the period that your **ISO/IEC 27001:2005** registration certificate is valid?
- Is the company's registration mark recognized and accepted in the nations where you plan to do business?
- Is the registrar accredited? This is the most important question to ask because accreditation is the guarantee that the registrar is a credible organization, just as your **ISO/IEC 27001:2005** registration certificate is a guarantee to your prospective customers that your information security system meets the highest standards.

The Importance of Accreditation

There are hundreds of registration bodies around the world, but not all of them have received internationally recognized accreditation.

The credibility of a registration scheme rests upon the reliability of third-party auditing organizations – registrars.

In order for a registrar to have any validity, a registrar must be approved by a recognized accreditation body.

Accreditation

- Verifies that the registrar/ certification body is independent, impartial, competent and knowledgeable.
- Verifies that the registrar uses qualified and experienced staff.

Accreditation bodies serve as the watchdog of the registrar. These boards formally license or accredit registrars to perform audits for international quality and management standards. The accreditation body monitors the registrar through regular surveillance audits.

PJR is accredited by a number of national organizations: ANAB of the United States, RvA of the Netherlands, JAB of Japan, UKAS of Great Britain, INMETRO of Brazil, ACCREDIA of Italy, and ema of Mexico. These organizations have granted **PJR** accreditation to register clients to various standards*.

By seeking an accredited registrar such as **PJR**, you can be assured that your registration certificate will be recognized by customers all over the world.

** Accreditations vary by standard*

The Registration Process

Let us now examine the **ISO/IEC 27001:2005** Registration Process.

PJR's team works with your organization utilizing a well-defined registration process comprised of the following steps. Each step will be explained in detail on the following pages.

The Registration Process

- Request for Registration: Application & Proposal
- Documentation Review
- Pre-Assessment (optional)
- The Registration Audit (Stage 1 & Stage 2)
- Taking Corrective Action
- Registration Decision
- Certification & Publicizing Your Registration
- Maintaining Registration & Surveillance Audits

Request for Registration – Application and Proposal

It is usually a good idea to establish a relationship with your registrar in the early stages of implementing your information security management system. That way, you can familiarize yourself with its practices and establish a schedule for registration in advance, thereby avoiding possible delays.

As with most registrars, you will be asked to complete an application. Here are some of the standard questions the registrar, such as **PJR**, will ask:

- What is your desired time frame for registration?
- Describe your business and any applicable SIC/EA codes.
- What is your company's scope of operations?
- What is the size of your facility and the number of employees?
- What is the status of your existing information security management system?
- What is the state of your information security management system documentation?

The Client Profile/Questionnaire used by **PJR** will provide us with information about your organization and each of the sites to be audited.

Using this information and the IAF requirements, **PJR** will prepare a proposal and a time estimate for completion of the registration audit.

If the proposal is acceptable, the registration agreement (contract) will be signed, and your relationship with **Perry Johnson Registrars** will be formalized.

Documentation Review

Once you are ready to begin the registration process, **PJR** will request a controlled copy of your ISMS manual or equivalent document. Most registrars will recommend that you submit your quality manual at least four to six weeks before your scheduled audit so that if any nonconformities are uncovered, you will have ample time to make corrections without delaying the process.

PJR will review your ISMS manual to determine whether it meets all requirements of the **ISO/IEC 27001:2005** information security management system model. In general, the more records and files you provide to the auditors, the greater the scope of the documentation review.

After your manual has been reviewed, **PJR** will submit a report to your company. If your documentation fails to meet all the criteria stipulated in the **ISO/IEC 27001:2005** standard, the nonconformities will be identified in the report, and you will need to take corrective action.

Before or during the document review process, your company may decide to hire the services of an outside consultant to help with your information security management system. Alternatively, you may want to send key personnel to a public seminar to learn what needs to be included in the quality manual.

A Documented Quality System:

- Defines the authorities and responsibilities of personnel.
- Clearly communicates the objectives of the system, the company's policies, procedures and work instructions.
- Documentation should include a "quality policy" that describes your company's overall pursuit of quality objectives, and a "quality manual"
- Documentation should include "quality plans" – documents that explain how quality will be managed for individual projects, contracts, or products.
- Documentation should also include "quality records" providing evidence that your system is in conformance to specified requirements.
- Promotes continual improvement, since the system is monitored regularly and changes can be incorporated easily.
- Ensures consistent performance.

Whether you choose to bring in a consultant or to send employees to a seminar is entirely up to you and what you feel your company needs. However, if you decide that you would like to seek the advice of someone specializing in the field of **ISO/IEC 27001:2005**, do not turn to the registrar. Registrars are not allowed to provide consulting services, as this would be a direct conflict of interest.

Once **PJR** has determined that your documented information security management system is satisfactory, final arrangements will be made for the audit at your facility. **PJR** will appoint a qualified audit team to carry out a full audit of your information security management system. The team will consist of a Lead Auditor, who is responsible for coordinating audit activities, and in some cases, one or more additional auditors, depending on your facility's size. At least one of the team members will be experienced in the industry.

The **PJR** Lead Auditor will work with your **ISO/IEC 27001:2005** Management Representative to devise a schedule for the on-site visit. Prior to the day of the audit, the **PJR** Lead Auditor will send you an audit plan, confirming the daily schedule of events and any accommodation requests.

It is the audit team's job to verify whether your information security management system is meeting all the requirements of **ISO/IEC 27001:2005**. The team determines this by collecting *objective/audit evidence* from a variety of people and sources regarding the effectiveness of your information security management system.

Pre-Assessment (optional)

Sometimes, prior to initiating the registration audit, the company seeking registration may request to have a pre-assessment, or "dry run," of its information security management system.

This gives the registrar an opportunity to identify in advance, any weaknesses that may exist in your information security management system.

Should you select this option, **PJR** will send an audit team to your facility to conduct the pre-assessment. This team of certified auditors, will study your facility, information security management system, records and other documentation, alerting you to any concerns that may interfere with a successful registration audit.

Pre-Assessment Perks

- Helps to determine a company's preparedness for a full assessment; i.e., registration audit.
- Can pinpoint major deficiencies in your quality system, giving your company sufficient lead time to correct any problems before the registration audit.
- Aids the registrar in planning for the final audit by determining the number of auditors needed, the length of time required to complete the audit, etc.
- May lead to overall cost savings.
- Gain a working understanding of the registrar's audit team practices.
- Increase the probability for a successful registration audit.

The main advantage of a pre-assessment is that it allows you to correct any potential problems before the registration audit begins. But you should remember that a pre-assessment is not required for **ISO/IEC 27001:2005** registration. It is strictly optional, depending upon your own needs.

The extent of the pre-assessment is also up to you. You may decide that you want a full pre-assessment performed on every aspect of your company's operations, or, to save on costs, you may decide that all you need is a sampling of your information security management system. It is your decision.

While a pre-assessment is optional, it is usually a good idea. The length of time allotted for a pre-assessment is discretionary; however, **PJR** typically recommends that this activity be equal to 60 percent of the total time required for the registration audit. In the long run, it can save you time and money by revealing nonconformities that, if corrected before the registration audit, can save you the expense of follow-up actions.

The Registration Audit

There are two stages to the Registration Audit as follows:

- **Stage 1 Audit**: Is performed to verify information regarding the scope, processes & location(s) of your organization, and related regulatory aspects & compliance. One very important activity performed by auditor(s) during the Stage 1 is a site tour, which provides a focus for planning the Stage 2 audit.

- **Stage 2 Audit**: Is performed to evaluate conformity, implementation & effectiveness of your organization's ISMS to **ISO/IEC 27001:2005**.

The timeframe between Stage 1 and Stage 2 can vary, but typically, it should not exceed 90 days.

Stage 1 Audit

The objectives of **Stage 1 Audit** include:

- Evaluation of the organization's location & site-specific conditions.
- Discussions with key personnel to determine preparedness for Stage 2.
- Review of the existing information security management system and the organization's understanding of the requirements of **ISO/IEC 27001:2005**. In particular, the identification of significant hazards and risks, processes, operations, and objectives of the ISMS.
- Review allocation of resources for the Stage 2 Audit activities, such as the need for Technical Experts and number and competencies of audit team members.
- Evaluation of the planning, execution and results of the organization's internal audit and management review functions and whether the level of implementation of the ISMS substantiates that the organization is ready for Stage 2.
- Understand the scope of the ISMS- employee count, shift pattern, remote functions etc.
- Any nonconformities identified at Stage 1 must be addressed and accepted/verified by the Audit Team Leader before Stage 2 can commence.

Stage 2 Audit

The objective of the **Stage 2 Audit** is to verify whether:

- The documented system is consistent with **ISO/IEC 27001:2005** standard.
- The organization's activities are consistent with the documented system.
- The ISMS is effective, and the company is meeting its objectives and goals.
- All information security hazards and risks have been identified, evaluated, and controlled.

- Improvement objectives support the ISMS Policy.
- All employees are aware of their roles and responsibilities in support of the ISMS.
- The process for identification of regulatory requirements continues to be effective and if the organization monitors these requirements.

During the **Stage 2 Audit**, a team of **ISO/IEC 27001:2005** qualified auditors will evaluate your information security management system. The team conducts a thorough review of your system to verify whether it meets all the requirements set forth in the standard and all applicable customer specific requirements.

The Opening Meeting

On the first day of your scheduled audit, an opening meeting will be held with upper management. Under the direction of the Lead Auditor, the audit team will present an audit process overview, giving you a clear understanding of what can be expected in the days to follow.

The team will review your audit scope and objectives. They will confirm times, schedules and resources with you, and they will go over the procedures for identifying and reporting nonconformities.

At this time, you will be expected to introduce your guide – the person you have selected to accompany the team on its audit of your facility.

The Registration Audit Consists of:

- An Opening Meeting
- A detailed examination of your quality management system
- A Closing Meeting
- Recommendation

Audit Observation, Interviews, Objective/Audit Evidence

Following the opening meeting, the audit team will walk through the various areas of your facility to observe activities. Team members may conduct one-on-one interviews with employees, they may ask to inspect documents and records, and they may examine equipment and products.

Throughout the audit, audit team members will seek *objective/audit evidence*, such as statements, documented procedures and written policies, to support their observations. The team will look for answers to the following questions:

- Is the documented system consistent with the standards? (Do you *describe* what you do?)
- Are activities consistent with the documented system? (Do you *do* what you say you do?)
- Is the information security management system effective, and is the company meeting its objectives and goals?

The **PJR** Auditors will bring to your attention any nonconformity as soon as possible after it is discovered. At the conclusion of the audit, the auditor will formally document all nonconformities on a nonconformity report.

The Closing Meeting

After the audit team has completed its on-site facility evaluation, a closing meeting will be held. The same people who sat in on the opening meeting usually attend this session.

At the closing meeting, the Lead Auditor will summarize the audit results. The Lead Auditor will explain in detail, any nonconformities that were found, and will provide you with a preliminary audit report. The Lead Auditor will also provide a recommendation as to whether your company should be granted registration.

Soon after the audit, you will receive a final audit report. In this report, the audit findings will be reiterated in detail. If any outstanding nonconformities were identified, the registrar should allow you a reasonable period of time, given the nature of the nonconformity, to take corrective action.

Taking Corrective Action

If the audit team indicates that corrective action is required, it is nothing to be alarmed about.

If a nonconformity is identified as minor – a problem that can be easily corrected – you will be asked to locate and fix the cause. The registrar requires the root cause, corrective action & objective evidence of its effective implementation in writing. This is followed by verification at the next surveillance audit, to make sure that the corrective action remains effectively implemented.

If a nonconformity is identified as major – the corrective action process is more involved. A major nonconformity is a deficiency or breakdown in your quality management system that prevents your company from reaching its objectives and goals.

When a major nonconformity is identified, it usually means that you have to make a significant change to either your quality management system or to a procedure. You must investigate the root cause and take corrective action to eliminate the nonconformity. You do not want to apply a Band-Aid to the problem – you want to find the root cause and prevent it from recurring.

After you have corrected the major nonconformity, **PJR** may require a follow-up audit limited to the relevant area, to confirm that the problem has been resolved. The Lead Auditor cannot recommend registration until the objective evidence of corrective action implementation of all nonconformities have been verified.

Registration Decision

After the Lead Auditor has closed out all nonconformities, your registration documents are forwarded to **PJR**'s Executive Committee – the registrar's independent decision-making body. The Executive Committee will review your application and the Lead Auditor's recommendation, and decide whether to grant registration to your company.

If the **PJR** Executive Committee determines that you have met all **ISO/IEC 27001:2005** registration requirements, you will be notified immediately.

Possible Audit Outcomes

- *Approval* – a company has met all the requirements for the applicable standard. All corrective actions have been closed out.
- *Disapproval* – either a company has not properly implemented its ISO quality system, or documentation is inadequate. The registrar must perform a comprehensive re-evaluation before granting registration.

A registration certificate and letter will be prepared. The registration certificate will bear the seals of the applicable accreditation bodies of the registrar, as well as the registrar's own logo. The registration letter will be on **PJR**'s letterhead.

PJR will also communicate your company's name and your registration status, to a variety of resources, such as the McGraw Hill Information Services of Organizations and *www.whosregistered.com* (managed by the Quality Systems Digest).

Publicizing Your Registration

You can display your registration mark in advertising, promotional literature and stationery to show customers that your company is committed to quality. **PJR** can provide you with camera-ready artwork, together with the procedure covering the reproduction and use of the Registration Certificate and logos. Registration marks cannot be used on products or in such a way that the product is implied to be **ISO/IEC 27001:2005** certified.

PJR Registration Plaque

PJR will provide your company with a free registration plaque. This three-color, zinc-etched plaque sets forth in embossed lettering your company name, the standard(s) to which your company is registered, the certificate number, the accreditation body seals, the issue date and expiration date. This plaque can be proudly displayed to let the world know that your certified management system meets the most rigorous international standards.

PJR Press Release Service

PJR's staff of seasoned writers can write a customized profile of your company, announcing your organization's attainment of registration status. Whether you are in need of a short press release or a detailed article describing your company's journey to registration, we offer this program to our clients free of charge.

PJR Flag & Banner Program

In addition to being able to announce your registration status in your marketing material, your company can purchase a flag and/or banner for publicity purposes.

The leadership of Chukyo Coca-Cola (now part of Coca-Cola Central Japan Co., Ltd) one of Japan's largest bottlers, is proud to accept congratulations for their achievement of both ISO 9000 and ISO 14001 Certifications.

Awards Ceremony

This is an excellent vehicle to publicize your company and gain full advantage of your newly achieved status as a registered firm. **PJR** can arrange to have your certificate, plaque and flag presented to top management at a special Awards Ceremony and picture-taking session. The Awards Ceremony is included at no extra charge.

Publication in Internationally Recognized Database Directories

PJR communicates your registration status to a variety of resources, such as the McGraw Hill Information Services of Organizations, *www.whosregistered.com* (managed by the Quality Systems Digest), as well as in any other organizations that may require notification regarding certification to this specific standard.

Maintaining Registration

Once you have attained **ISO/IEC 27001:2005** registration, you will be scheduled for periodic surveillance audits. Audits must be conducted under the provisions of ISO/IEC 17021 (ISO/IEC Guide 62), which sets out general guidelines for registrars. The surveillance audits, which are audits based on a sampling of your information security management system, are invaluable, because you learn how to continue meeting the industry-specific demands, as well as the **ISO/IEC 27001:2005** elements. Registered clients can choose from two different surveillance schedules as follows:

Semi-Annual Surveillance Audits

Most PJR clients choose Semi-Annual Surveillance Audits. If you choose this option, the audit visits in the first two years will be more frequent, but typically shorter. The advantage to this method is that your system remains under ongoing maintenance. With shorter intervals between audit visits, your system has less of a chance to break down. In this way there is far less chance of auditors finding any major nonconformities, which can be time-consuming and expensive to correct. At the end of three years, PJR will conduct a full reassessment of all **ISO/IEC 27001:2005** requirements.

Annual Surveillance Audits

PJR offers the annual surveillance plan as an alternative to semi-annual surveillance. For annual surveillance, the auditing guidelines require a minimum of one audit visit per year. Each surveillance audit will cover a sampling of your facility's information security management system & customer specific requirements. At the end of three years, PJR will conduct a full reassessment of all **ISO/IEC 27001:2005** requirements.

Recertification Audit

A recertification audit is to be performed at the end of 3 years, to prevent expiry of your certificate. If the recertification audit does not take place within this timeframe, your certificate will no longer be valid and you will have to go through the entire registration process again to get certified.

A Word About Reassessment Requirements

The International Accreditation Forum (IAF) has established rules mandating reassessment to verify continuing effectiveness of an organization's information security management system. The rules apply regardless of whether the organization has elected an annual or semi-annual surveillance schedule.

If the organization has elected the continuous (semi-annual) method of surveillance, **PJR** will conduct the reassessment at the fifth and sixth visits. For organizations on an annual program, the reassessment is conducted at the third visit. **PJR** schedules reassessments to conclude approximately 90 days prior to the Registration Certificate expiration date to permit closure of any findings, with no lapse in certification. The amount of time established for reassessment by the rules are equal to 2/3 of the time mandated for an initial audit of the organization, determined as of the time it is to be reassessed. Reassessment time may vary from the mandated 2/3 figure based on "significant factors that uniquely apply to the organization."

Disputes & Appeals

If you believe your company has been unfairly denied registration, or you wish to dispute an audit nonconformity, you can file a dispute. If the results of the dispute are unsatisfactory to your organization, you may file an appeal. All registrars are required to have a board of appeals with an impartial panel. This board is independent of the registrar and will listen to your arguments and re-evaluate your application.

Integrated Management Systems

Many companies have implemented individual management systems based on quality, health and safety, and the environment. The standards for certification of these systems are very compatible. Some companies operate their separate systems in combination or parallel, while others take the approach of integrating everything into a single system.

By integrating responsibilities and centralizing control, a company may reduce duplication of required processes and records. Thus, you could achieve a reduction in everything from top management time to internal audits to forms. The harmonization of standards can potentially lead to economies of scale and thus, fewer man-days.

Systems that fit together as part of an Integrated System are based on international standards, such as:

Quality Management

ISO 9001 – a family of standards developed to provide the framework around which a quality management system is based.

Environmental Management

ISO 14001 – a standard that addresses process for controlling and improving a company's environmental performance.

Occupational Health & Safety

OHSAS 18001 – an assessment specification for Occupational Health and Safety Management Systems.

The range of standards that may be incorporated into the integrated management system may vary in regions or industry sectors. Please contact **PJR** for full details.

Organizations with multiple formal management systems can benefit significantly by merging all their systems into one "business management" system, where the quality (QMS), environmental (EMS), occupational health & safety (OH&SMS), and any sector specific management systems are harmonized, and work in conjunction with the business planning, HR, finance, procurement, administration, operations, audit, management review and other systems.

There are several advantages for having an Integrated Management System (IMS) in an organization:

- Helps gain competitive advantage by increasing the organization's market share through cost savings and improved efficiency.

- Used as a stepping stone to realize a more effective system with improved operational performance.

Organizations that are certified to ISO 9001 can fine-tune their documentation to be integrated with ISO 14001 and OHSAS 18001, thus resulting in less documentation required as the standards are compatible.

PJR offers such services for integrated management system audits, which can result in significant savings in costs while increasing the effectiveness of your overall management system.

Organizations that are certified to ISO 9001 can fine-tune their documentation to be integrated with ISO 14001 and OHSAS 18001, thus resulting in less documentation required as the standards are compatible.

PJR offers such services for integrated management system audits, which can result in significant savings in costs while increasing the effectiveness of your overall management system.

How Much Does Registration Cost?

When you enter the market for a registrar, you will find a wide range of pricing for registration services, depending on various factors.

Each company and plant has its own unique characteristics, and these come into play in estimating costs. But in general, there are three key elements that make up the cost of registration.

1. Daily rate
2. Overhead expenses
3. Travel and accommodations

Cost Estimates Should Include:

- Fees for document review
- Fees for optional pre-assessment
- Fees for registration audit
- Miscellaneous fees associated with registration (travel, accommodations, etc.)
- Fees for surveillance

Generally, most registrars will charge a daily rate. This part is straightforward. But when it comes to overhead costs and travel expenses, things can get somewhat clouded. Some registrars will quote a daily rate, and then add on extra charges for office preparation or other services. This creates confusion and presents an inaccurate picture of the total cost.

You must also consider travel expenses. Travel costs are generally added on top of the registration fee. Therefore, you will want to find out if the registrar intends to fly auditors in from out of town, or if the company has auditors located nearby.

Bottom Line: Ask the registrar to give you a quote on all fees expected to be incurred, so you can get an accurate total cost estimate. Be thorough and demand a full accounting up front.

How Long Does It Take to Become Registered?

Just as cost estimates vary, there is no set timeline for completing a registration audit. The number of required audit days varies, depending on several factors.

The number of days required to complete a registration audit depends upon:

- Size of company
- Number of employees
- Complexity of operations

Generally, the length of time required to complete a registration audit is determined by company size, the number of employees and the complexity of the company's operations.

The IAF (International Accreditation Forum, Inc.) has issued a detailed set of guidelines that sets forth minimum audit days for **ISO/IEC 27001:2005**, based on an organization's size, scope and organizational structure. These guidelines list the minimum days required for a valid registration audit. In evaluating a prospective registrar's proposed audit schedule, always ask if it follows IAF guidelines.

For the most part, it takes a company a minimum of one year to prepare for the registration audit. The registration process itself – from the evaluation of your documentation to the issuance of a certificate and letter – takes approximately two months to complete, assuming there are no major problems with the information security management system.

Why Do You Need Registration?

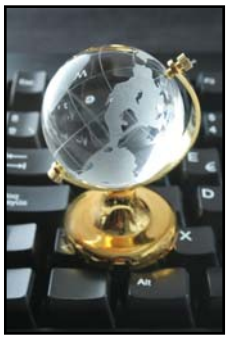
Gaining registration to **ISO/IEC 27001:2005** through **Perry Johnson Registrars** will help your organization flourish. Whether you are looking to operate internationally or to expand locally to accommodate new business, **ISO/IEC 27001:2005** will help you demonstrate to customers that you have a commitment to quality. It is often a requirement in the industry that you have implemented an information security management system and comply with the requirements of **ISO/IEC 27001:2005**.

The regular assessment process will ensure you continually monitor, improve and comply with your processes.

Registration can improve overall performance, remove uncertainty and widen market opportunities.

At **PJR** we have a structured route to registering to **ISO/IEC 27001:2005**. The **PJR** Road to Registration is designed to make your experience as enjoyable as possible, with minimal disruption to your business practices.

Conclusion



Becoming registered to the **ISO/IEC 27001:2005** is not difficult to achieve, so long as you pay close attention to the standard and adhere to its requirements.

Once you have completed the registration process and received your **ISO/IEC 27001:2005** registration certificate and letter, you will earn valuable recognition in your business sector. And because **ISO/IEC 27001:2005** is an international standard, you will gain a greater footing in the international marketplace.

In this age of high technology and state-of-the-art manufacturing, customers all over the world are demanding security in their business transactions. There is increased awareness regarding security issues. The trend in America and nations abroad is pointing to information security management system registration. According to the International Organization for Standardization, ISO management standards (including ISO 9000 and ISO 14000) have been implemented by more than 760,000 organizations in 158 countries. In North America alone, the total number of ISO 9000 registrations reached over 60,000 by the end of 2006.*

As global acceptance of the ISO quality and management standards continues to mount, industry experts say the move toward registration will continue to skyrocket. If you want to be a part of this growing trend, **ISO/IEC 27001:2005** registration is the only way to go.

*Source: QSU Publishing Company

About PJR

Perry Johnson Registrars, Inc. **(PJR)** is a full-service registrar that has been accredited by the multiple international accreditation bodies.

PJR is also recognized by the International Automotive Task Force (IATF) through the International Automotive Oversight Bureau (IAOB) for: ISO/TS 16949:2002.

In addition, **PJR** provides third-party services for ISO 9001:2008, ISO 14001:2004, OHSAS 18001, RC-14001, Responsible Care®, ISO 22000:2005, TL 9000, ISO 27001:2005, ISO 13485:2003, and other quality and other management standards.

The scope of **PJR**'s registration scheme and auditor base is broad enough to cover audits in virtually every SIC, EA, and NACE code. **PJR**'s auditors have conducted numerous audits in a wide variety of industries.

PJR Offers Multiple Accreditations:

- **ANAB** – ANSI-ASQ National Accreditation Board
- **UKAS** – United Kingdom Accreditation Service
- **RvA** – Dutch Accreditation Council/Raad voor Accreditatie
- **JAB** – The Japan Accreditation Board for Conformity Assessment
- **ACCREDIA** – Italian Accreditation Service
- **INMETRO** – National Institute of Metrology, Standardization and Industrial Quality of Brazil
- **ema** – entidad mexicana de acreditacion a.c.

Our experts are qualified through academia and professional certifications such as IRCA and RABQSA; industry affiliations such as ASQC, SME, SAE; hands-on teaching and training experience, and varied industry exposure. They average 15 to 20 years of experience in the quality arena and many posses training experience in the quality industry, having taught many of our competitors' auditors.

About the PJR Audit Staff

- Auditors are certified by the IRCA and RABQSA.
- 15 to 20 years experience.
- Many **PJR** Lead Auditors are also experienced classroom instructors, meaning they are detail-oriented and motivated to keep their knowledge level up to par.

PJR's auditors must have a minimum amount of industry experience in addition to meeting the above requirements. This experience is typically gained by working in engineering, design, manufacturing, quality or process control for a major manufacturer, supplier, auxiliary equipment supplier and/or an appropriate governmental agency.

If the auditor lacks the minimum amount of industry background, he or she must take an industry competency course through the registrar.

PJR also has a far-reaching Lead Auditor base in the United States with auditors located within 50 miles of every major city – offering significant savings in travel costs for our clients.

PJR Philosophy

Implementing a quality, environmental, or sector specific management system requires a lot of work, and no organization can get there overnight. In fact, it takes most companies 6 to 18 months to achieve registration.

At **PJR**, we believe the key ingredient to attaining registration is the sincere desire and commitment to succeed. There is no such thing as failure… only giving up.

We recognize that the registration process is a substantial undertaking for most companies, and are committed to being as flexible as necessary to ease the process. We will work within your scheduling needs, by offering a wide variety of auditors and scheduling options, while always maintaining a consistent auditing approach.

PJR Philosophy

- The sincere desire and commitment to succeed will lead to a successful registration.
- **PJR** strives to establish an open and satisfying partnership with each client.
- Clients are kept abreast of all key decisions. There are no surprises.

At **Perry Johnson Registrars**, we want our clients to feel as comfortable about the registration process as possible. That is why every effort is made to keep our clients' Management Representative informed about the entire audit planning process. If you have a full understanding of the registration audit process, there should be no surprises. Registration is a long-term process. You need to feel comfortable and secure with your registrar of choice.

Our entire team at **PJR** from sales, scheduling, operations, auditing, and customer services is dedicated to meeting your needs and strives to provide you with the highest level of service, to help you achieve success in the global marketplace.

How PJR Builds Trust

At **PJR**, we realize the relationship that exists between your organization and your registrar. There should be a good rapport and comfort level between you and your registrar.

In our efforts to make the registration process gratifying, we believe in involving our clients in all pertinent decisions. In fact, we even let our clients play a large role in selecting the audit team. We, at **PJR**, have no problem in letting clients review the resumes of our audit staff and make recommendations; our clients have the final approval on audit team composition.

Furthermore, our goal is to provide the highest quality of service. We strive to answer all questions within a 24-hour turn-around time, and we never arrive at a facility unannounced. Our clients are always informed of the date or dates on which surveillance audits are to be carried out.

PJR Advantages

- No application fee
- No travel mark-up
- No auditor transit-day billing
- NO HIDDEN COSTS
- **PJR** clients have a voice in auditor selection
- Full-time auditors are on staff to answer questions
- FREE Registration Plaque
- FREE press release service
- Awards Ceremony Option

The **PJR** advantage begins with the high level of professionalism and experience that **PJR** auditors provide. Add to that our multiple accreditation status, no application fees, no overtime charges, no travel mark-up… and you have a wealth of advantages difficult to find elsewhere. We offer a full-service registration package that we believe is a value second to none.

A Heritage of Quality

Perry L. Johnson, founder of **PJR** and Perry Johnson, Inc. (PJI), is an internationally recognized ISO/QS-9000 and ISO 14000 educator. He is the author of several publications including - *ISO 9000: The Year 2000 and Beyond, Third Edition*, published by McGraw-Hill in 2000; *ISO 9000: Meeting the New International Standards*, the best-selling U.S. book in the ISO 9000 field, published by McGraw-Hill in 1993; *ISO 9000: Meeting the International Standards, Second Edition*, published by McGraw-Hill in 1996; *The ISO/QS-9000 Yearbook: 1998*, published by McGraw-Hill in 1998; *ISO 14000 Road Map to Registration*, published by McGraw-Hill in 1997; *ISO 14000: The Business Manager's Complete Guide to Environmental Management*; published by John Wiley & Sons in 1997; *Keeping Score: Strategies and Tactics for Winning the Quality War*, published by HarperCollins in 1989; and numerous other workbooks and teaching aids.

Business Experience and Affiliations

PJR maintains memberships/affiliations to several professional organizations related to the quality and environmental industries. Our President and other top Executives within **PJR** attend annual meetings and serve on technical committees within these Bodies:

- American Society of Quality (ASQ)
- Independent Association of Accredited Registrars (IAAR)
- International Accreditation Forum (IAF)
- Association of British Certification Bodies (ABCB)
- American Aerospace Quality Group (AAQG)
- International Aerospace Quality Group (IAQG)
- Pacific Accreditation Conference (PAC)
- RAB/QSA Special Task Force regarding ISO 17024
- Asia Pacific Laboratory Accreditation Cooperation (APLAC)
- International Laboratory Accreditation Cooperation (ILAC)
- Canadian Medical Device Conformity Assessment Scheme (CMDCAS) Forum

PJR Home Page

More information about **PJR** can found on the **PJR** Home Page, located on the World Wide Web at http://www.pjr.com. Our Home Page includes:

- Background information on **PJR**
- Important news for customers
- A biography of Perry L. Johnson
- Frequently Asked Questions
- **PJR** Advantages
- Accreditation Scopes
- **PJR** Office Directory
- Client Listing and Testimonials
- Important facts about ISO 9001, ISO 14001, OHSAS 18001, ISO/TS 16949, ISO 22000, ISO 27001, ISO 13485, TL 9000, and other standards.
- Access to Root Cause/Systemic Corrective Action Interactive Module

PJR CLIENTS

Reputation of Strength

A **reminder**: This is only a partial list of **PJR** clients. Even though **PJR** has registered some of the largest companies in the world, **PJR** is still sensitive to the needs of small- to medium-sized businesses.

A partial list of Perry Johnson Registrars' clients:

Abel Construction Company, Inc.
Arnold Air Force Base
Autoliv Japan, Ltd.
BASF Catalysts, LLC
Bell Helicopter Textron
Brazilian Canadian Coffee Co., Ltd.
California Eastern Laboratories
California EPA/Integrated Waste Management Board
California National Guard
Cargill de Mexico
Carlisle Tire & Wheel
Chrysler de Mexico
Coca-Cola Central Japan Co.
Crane Army Ammunition Activity
Dassault Falcon Jet Corporation
Dept. of Energy – National Nuclear Security Y12
East Coast Fire Protection, Inc.
Eaton Corporation – Truck Components Operations
Electrolux Home Products
Elopak Incorporated
Epson de Juarez, Mexico
Ervin Amasteel
Farmers Co-Op Society
FlexSol Packaging Corp.
Fruehauf Co., Ltd (Japan)
GAC MidAmerica, Inc.
GE Fanuc Embedded Systems
Great Lakes Credit Union
Häagen-Dazs Japan, Inc.
Hasbro North America - ELM
Horizon Lines of Alaska, LLC
Husqvarna Outdoor Products
Ingersoll-Rand
ITOCHU Chemicals
Kansas Army National Guard RSMS
Kansas Army National Guard CSMS
Kikkoman Foods
Komatsu Forklift, USA
Koyo Machinery, Inc.
L-3 Communications/Titan Corp.
Label-Aid Systems
Lacks Enterprises
Maine Military Authority
MarChem/Dash MultiCorp
Mead-Johnson de Mexico
Metalcraft of Mayville
Mississippi Army National Guard RSMS
Missouri Army National Guard AVCRAD
Mitsubishi Motors
Mitsubishi Power Systems, Inc.
Mooney Airplane Company, Inc.
Murakami Manufacturing USA
Naval Undersea Warfare Center
Nissan Mexicana S.A. de CV
Ohio Army National Guard CSMS
OMNI Source Corp.
Oregon Army National Guard OSMS
Panther II Transportation
Parker Hannifan Corp.
Pennsylvania Army National Guard CSMS
Pentel of America, Ltd.
Phillips Service Industries Inc.
Poulan/Weedeaters Division of Electrolux
Power & Telephone Supply Company
Red River Army Depot
Remington Hybrid Seed Company
Siemans Manufacturing
Sierra Army Depot
Solvay Chemicals
Technicote, Inc.
Texas Army National Guard RSMS
The California Environmental Protection Agency
Toto USA
Toyal America
TW Metals, Inc.
Tyco Fire & Security/Simplex Grinnell
U.S. Army Contracting Agency Unisource
United States Brass & CopperCo.
Valeo
Wagner Spray Tech Corporation
Zenith Cable Products, Mexico

PJR Client Testimonials

"When I was given the task of consolidating 3 registrations, 3 registrars into 1, **PJR** was by far the most responsive and easiest to work with. This is the reason I chose **PJR** and I have been very pleased with our partnership. The auditor assigned to my account is great to work with. He is knowledgeable, and a pleasure to work with. I hope to continue the partnership with **PJR** as we extend our registration to our other facilities in North America."

- Patricia B. Hill, Solvay Chemicals, Inc.

"The Auditor does a good job with our accounts. We are very pleased with our auditor."

- Randall Toth, Unifirst

"Everyone we come in contact with at **PJR** are good to work with"

- Terry Lierman, Mitsubishi Motors, North America

"As always, it's been a pleasant, informative and constructive audit. We look forward to working with **PJR** again…"

- Lisa Wendling, Decatur Machine Services, Inc.

"The professionalism and experience of the Lead Auditor is appreciated and has been helpful in identifying areas that we can improve on, above and beyond the basic requirements of the standard"

- Robert Collier, Jr., Mooney Airplane Company, Inc.

"**PJR** did a First Class Job"

- Drago Santrach, Owens Corning Automotive

"Process for obtaining and maintaining certification is simple and trouble free."

- David Landis, Datamax Corporation (a subsidiary of Dover Corporation)

"**PJR** has been very professional in all areas of business. I will continue to use **PJR** as my company registrar."

- Joseph Sarlo, G&S Rubber Manufacturing

"Surveillance audit went great. The auditors **PJR** sent were excellent. The most positive and educational audit that we have been through."

- Greg Finch, Corrigan Manufacturing

"The **PJR** auditors were very polished and professional. DTI is quite happy with their performance and feel they give the kind of customer support and satisfaction we look for. Their thoroughness, as well as experience, provided DTI with a confident feeling that will continue to improve on the already solid QMS system in place. We look forward to our working relationship with **PJR** and their team."

- Benjamin Yoder, Damping Technologies, Inc.

"Our ISO Management/Quality Team is very satisfied with our relationship to **PJR** and the level of service we have received and continue to receive."*- Quincey Nixon, Hart Howerton Architects*

"Our experience with **PJR** remains very positive. We have considered the relationship to have added value to our business and we look forward to continuing the relationship."
- Gary P. Brennan, Hasbro North America - ELM

"The audit team that was sent was extraordinary. Their experience in the industry and knowledge of AS9100 requirements was exceptional…this was the best audit team I have ever worked with."
- David McCoy, Celltron, Inc.

"We continue to receive excellent service with the **PJR** team. The personnel that we deal with are professional and understand what "Customer Service" means. We appreciate your service and assistance at our site. We anticipate working with your firm for an extended period of time."
- Ronald E. Mullinax, Army National Guard Readiness Sustainment Maintenance Site

"The **PJR** auditors conducted themselves in a highly professional manner… we would be honored to have them back next year." *- Thomas W. Kilpatrick, HTP-Meds, LLC Hi-Tech Profiles, Inc.*

"Very satisfied with the services of **PJR**." *- Danny Gesell, B&F Fabricating, Inc.*

"**PJR** is a pleasure to work with. Auditors are knowledgeable and professional. Sales and Scheduling were very accommodating with changes and adjustments."
- James LeRoy, Workhorse Aviation Manufacturing, LLC.

"Very cooperative. Professional organization." *- Bill Rustic, Wolverine Pattern & Machine*

"My experience with everyone contacted at **PJR** is always pleasant and professional." *- Terri Sommers, Michigan Metals, Inc. (formerly Strip Steel, Inc.)*

"All of the auditors that I have worked with are very professional and knowledgeable in their field." *- Bill Hackmack, Howe Machine & Tool Corp.*

"I would recommend **PJR** to anyone seeking certification!"
- Kenneth A. Cogdell, United Machine Works, Inc.

"Auditors are a pleasure to work with and provided good feedback to the auditees."
- Bryon Holton, Bell Helicopter, a Textron Company

"The **PJR** Auditor was very professional and understands the standards better than any other auditor I have encountered in the last 10 years."
- Randy Green, Ultrapure & Industrial Services, a division of Driessen Culligan

"The auditors were knowledgeable and professional, I would welcome them back on our subsequent audits." *- Dick Davis, Oneida Molded Plastics*

"Our auditor is a pleasure to work with. He presents a very comfortable atmosphere while performing a thorough audit. I look forward to working with him in the future."

- Holland L. Dresser, VDC Display Systems, a division of Video Display Corporation

"We have been very satisfied with **PJR**, exceptionally the auditors we have had. Customer Service has been wonderful."

- Paul Becker, Economy Products

"Excellent company. Good preparation for client prior to audit and certification. Good follow-up afterwards."

- Frank Unger, North American Color, Inc.

"Very satisfied with **PJR**. Auditor was very professional, well informed, and conducted an impartial, value-added audit of our Environmental System."

- Donald L. Searle, Ervin Industries, Inc. (Amasteel Division)

"I would like to take this opportunity to express our appreciation for the timely manner our AS9100 audit request was handled on such short notice. Thanks to our audit coordinator for a job well done."

- Art Pecaut, Daca Machine & Tool

"I am happy to say the people at **PJR** I have met and have talked to have been very professional. They respond very quickly to our questions and concerns. We are extremely happy that we chose a registrar that has excellent employees working for them and their customers."

- Jackie Perry, AAA Plating Industries

"Our auditor arrived promptly on schedule and conducted the audit in a professional manner. Thanks **PJR**!"

- James Kolasinski, BVA Oil, Inc.

"We have been working with **PJR** for over 10 years, and it has been a great experience."

- Kerry Lang, Fritz Products, Inc. (Huron Valley Steel)

"Our audit team was excellent. They were very good at explaining their stand on the issues brought up. It was a learning experience on our part. Also, whenever I called **PJR**, I got quick results and if they needed to check on something they always got back to me in a timely manner."

- Husqvarna Turf Care Division of Husqvarna Professional Outdoor Products, Inc.

"The auditors were very professional and I appreciate their help with improving my quality system."

- Dennis Jolley, MarathonNorco Aerospace, Inc.

"I always use **PJR** as an example of excellent customer service."

- Don Doll, Avion/AvTask

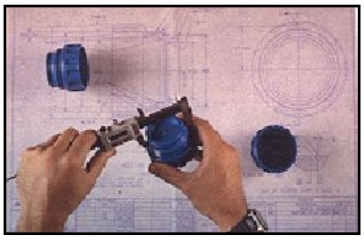
"**PJR** auditor was very professional and easy to work with. I look forward to working with him in the near future."

- V. Raj Narayanan, C-Cat, Inc.

"We are always treated with courtesy and respect from the auditors and staff at **PJR**."
- Dave Giampa, P.V. Engineering & Mfg., Inc.

"We have worked with **PJR** for the last 9 years and have found **PJR** to be competitive in price, and great in customer service." *- Jim Strawbridge, Top Die Casting Co., Inc.*

"It is a pleasure to do business with **PJR**."
- Cliff Craft & Gina Tatusko, ValveTech, Inc.



"Auditor did a great job explaining the scope of the audit as well as execution of the same. Very impressed with **PJR** professionalism. The auditor is an outstanding representative of **PJR**."
- Stacey Freels, Florida Circuit

"Our lead auditor was very thorough and professional throughout the audit."
- Glenn Myers, Robert Shaw Industrial Products

"Overall we are very satisfied with **PJR**. Our auditor is fair and is knowledgeable. A total all around good experience." *- Tony Mullikin, Superion, Inc.*

"We are happy with the service **PJR** has given us. Thanks!"
- JoAnn Kurek, Kurek Tool, Inc. (KTI)

"Very professional audit." *- Georgia Kovco, Nova Services/Summit Unlimited, Inc.*

"**PJR** has been a very helpful organization to be associated with regards to our ISO audits. The people are friendly, organized, and knowledgeable."
- Scott Herman, Performance Pattern

"We are satisfied with **PJR** staff help during our audits. We appreciate the time the auditor provides in explaining changes which were unclear or unknown." *- Catherine Almanzo, Powervar, Inc.*

"I am impressed with all of the **PJR** employees that I have had contact with in the past several months, especially our **PJR** Lead Auditor." *- David Zedaker, CT Industries, Inc.*

"If I were to go to work for another company, **PJR** would be my (the) registrar I'd go to for registration." *- Jay Lawrence, Insight, Inc.*

"Our audits are a very positive experience and Perry Johnson has done a great job for us."
- Judy DiStefano, Filtration Systems, a division of Mechanical Mfg. Corporation

"We are very satisfied with **PJR**." *- Jason Conover, Avion Manufacturing Company*

"Each person that I have spoken with on the phone has been exceptionally nice. With those I encountered through e-mails, they have been most helpful and always willing to take the time to help." *- Bea Anderson, Tilson Machine, Inc.*

"**PJR** has been very accommodating, even when we switched the audit date. The pre-assessment audit and the registration audit were both very value added, allowing an extra set of eyes to look at our system and point out our weaknesses and strengths. Altogether a great experience."

- Summer Lutton, Systima Technologies, Inc.

"This is the second facility that I have taken part in ISO certification. Both facilities have used PJR and everything has been great." *- Bob Srnovrsnik, Quantum Coatings*

"Our company has been very pleased with your process. The **PJR** auditor is very informative in explaining a non-compliance issue as well as positive aspects of our processes." *- Priscilla Paclik, Comsys Vendor Management Services (VMS)*

"I have never had any issues with **PJR**. Everyone I talk with is always helpful, knowledgeable, and professional." *- Katherine Goeser, IntegriGuard, LLC.*

"We are pleased with all aspects of Perry Johnson Registrars. Thank you."

- Kenneth Moore, Dern Moore Machine Co., Inc.

"**PJR** is very easy to work with and we are satisfied with services provided."

- Paul Oberlander, Tru Corporation

"Prompt, accurate timely service." *- Ricky Cox, Roll Forming Corporation*

"Thanks to **PJR** our organization has benefited from our quality system, and continuous improvement along with the focus on customer satisfaction, as we have at no other time in our company's history. As with any other thing that seems to benefit your company once Top Management realizes the benefits, it becomes a top priority that cannot be ignored. So again, I would like to say thank you **PJR**."

- Johnny M. Rhoades, Spartan Carbide, Inc.

"Thank you for your services."

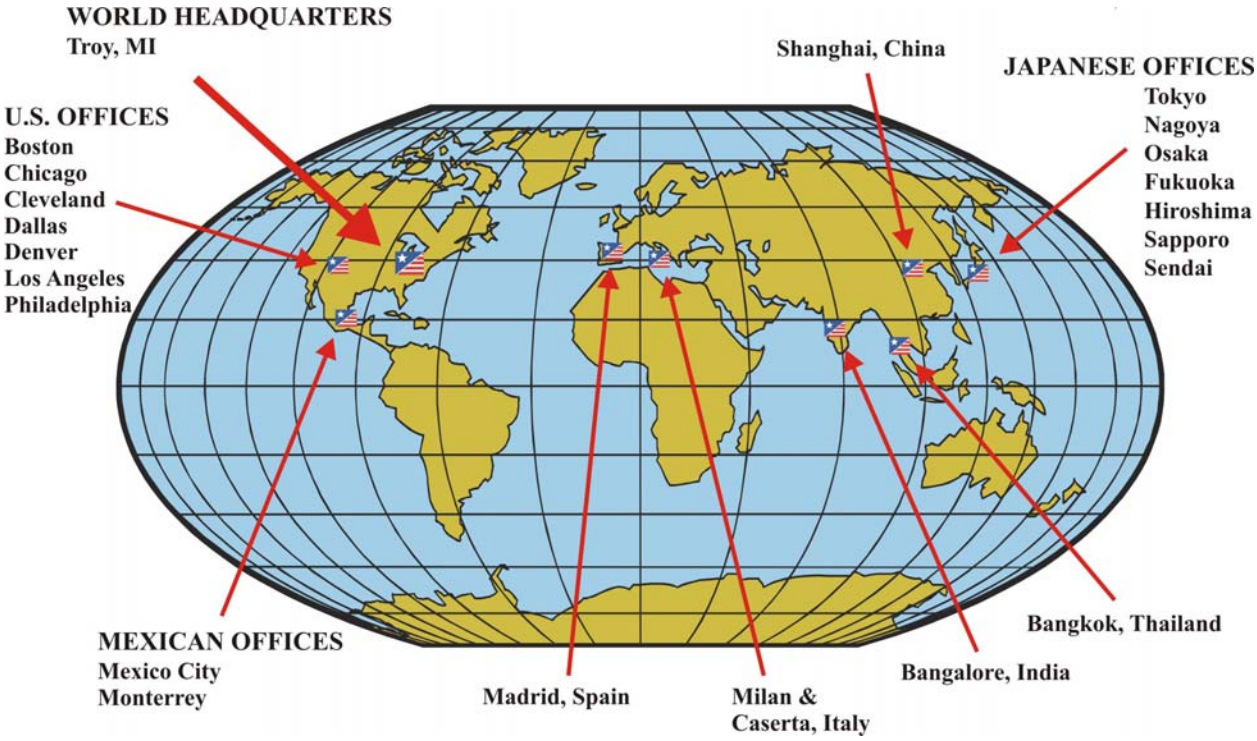
- Steve, Borcik, Kropp Forge Division of Park-Ohio Forged and Machined Products

Contact PJR

PJR is headquartered in Troy, Michigan with branch offices located in Boston, Chicago, Cleveland, Dallas, Denver, Ft. Myers, Philadelphia, Los Angeles and Valencia, CA.

Abroad we have offices in Mexico City and Monterrey, Mexico; Tokyo, Nagoya, Osaka, Fukuoka, Hiroshima, Sapporo and Sendai, Japan; Shanghai, China; Bangkok, Thailand; Bangalore, India; Milan and Caserta, Italy; and Madrid, Spain.

PJR's GLOBAL PRESENCE



For more information on PJR's registration services:

Call: 1-800-800-7910
(If your company is located outside the United States, please call: 1-248-358-3388)

Fax: 1-248-358-0882

You may also write to:
Perry Johnson Registrars, 755 W. Big Beaver Rd., Suite 1340, Troy, Michigan 48084 USA

Access our website at: www.pjr.com

E-mail: pjr@pjr.com

Appendix A: Correspondence between ISO 9001:2008, ISO 14001:2004, and ISO/IEC 27001:2005

ISO/IEC 27001:2005		ISO 9001:2008		ISO 14001:2004	
0	**Introduction**	**0**	**Introduction**		**Introduction**
0.1	General	0.1	General		
0.2	Process Approach	0.2	Process Approach		
		0.3	Relationship with ISO 9004		
0.3	Compatibility with other management systems	0.4	Compatibility with other management systems		
1	**Scope**	**1**	**Scope**	**1**	**Scope**
1.1	General	1.1	General		
1.2	Application	1.2	Application		
2	**Normative references**	**2**	**Normative references**	**2**	**Normative references**
3	**Terms and definitions**	**3**	**Terms and definitions**	**3**	**Terms and definitions**
4	**Information security management system**	**4**	**Quality management system**	**4**	**EMS requirements**
4.1	General requirements	4.1	General requirements	4.1	General requirements
4.2	Establishing and managing the ISMS				
4.2.1	Establish the ISMS				
4.2.2	Implement and operate the ISMS			4.4	Implementation and operation
4.2.3	Monitor and review the ISMS	8.2.3	Monitoring and measurement of processes	4.5.1	Monitoring and measurement
		8.2.4	Monitoring and measurement of product		
4.2.4	Maintain and improve the ISMS				
4.3	Documentation requirements	4.2	Documentation requirements		
4.3.1	General	4.2.1	General		
		4.2.2	Quality Manual		
4.3.2	Control of documents	4.2.3	Control of documents	4.4.5	Documentation control
4.3.3	Control of records	4.2.4	Control of records	4.5.4	Control of records
5	**Management Responsibility**	**5**	**Management Responsibility**		
5.1	Management commitment	5.1	Management commitment		
		5.2	Customer focus		
		5.3	Quality policy	4.2	Environmental policy
		5.4	Planning	4.3	Planning
		5.5	Responsibility, authority and communication		
5.2	Resource management	6	Resource management		
5.2.1	Provision of resources	6.1	Provision of resources		
		6.2	Human Resources		
5.2.2	Training, awareness and competence	6.2.2	Competence, awareness and training	4.4.2	Competence, training, and awareness
		6.3	Infrastructure		
		6.4	Work environment		
6	**Internal ISMS audits**	**8.2.2**	**Internal audit**	**4.5.5**	**Internal audit**
7	**Management review of ISMS**	**5.6**	**Management review**	**4.6**	**Management review**
7.1	General	5.6.1	General		
7.2	Review input	5.6.2	Review input		
7.3	Review output	5.6.3	Review output		
8	**ISMS improvement**	**8.5**	**Improvement**		
8.1	Continual improvement	8.5.1	Continual improvement		
8.2	Corrective action	8.5.3	Corrective actions	4.5.3	Non-conformity, corrective action and preventive action
8.3	Preventive action	8.5.3	Preventive actions		
Annex A	Control objectives and controls			Annex A	Guidance on the use of this International Standard
Annex B	OECD principles and this International Standard				
Annex C	Correspondence between ISO 9001:2008, ISO 14001:2004 and this international standard	Annex A	Correspondence between ISO 9001:2008 and ISO 14001:1996	Annex B	Correspondence between ISO 14001:2004 and ISO 9001:2008