Industry and government regulations and intense competitive pressures are driving the need for greater control of information throughout its life cycle—to protect confidentiality, personal privacy, and long-term integrity of critical business data.

Today, the need for data protection and security goes well beyond the realm of access privileges and firewalls. Organizations of all sizes, in public and private sectors, must not only protect information from unauthorized access and intrusion but also manage how documents, presentations, spreadsheets, and e-mails are handled in the normal course of daily business. Imagine the potentially damaging business risk should a company-confidential financial statement be inadvertently e-mailed to an analyst with the same name as your CFO, should patient records be exposed, or should a manager accidentally leave behind a printed copy of a performance review in a public space.

The optimum way to ensure the proper use and audit tracking of company-sensitive information in today’s networked world is to programmatically define a robust use policy, encrypt the information, and let the policy travel with the data to enforce the use rights of the information anywhere it travels. There must be a level of continual control over who receives access to sensitive information as well as a control mechanism easily understood by end users.

This area of technology is called enterprise rights management, or information rights management (IRM), and is specifically focused on protecting digital information like documents and e-mail. For IRM to effectively do its job, it must be generally available in the network infrastructure, integrate easily into existing applications, and transparently manage policies for documents or other data—all based upon who is accessing information, what computer they are using at the time, and other considerations relevant to enforcing corporate data-handling policies.

HP provides effective IRM solutions to prevent mishandling of information and documents in Microsoft® environments. Our IRM solutions enhance our customers’ existing security strategy, protecting information through persistent usage policies. Drawing upon our extensive security experience and strong collaboration with Microsoft, HP designs and deploys an IRM strategy and infrastructure that:

• Protects sensitive digital information from unauthorized use, both online and offline, whether inside or outside a firewall
• Enforces policies that indicate which people, machines, or applications it will or will not trust for specific actions on the content
• Simplifies administration and enforcement of privacy policies and regulatory requirements and ensures appropriate privacy policies are in effect and enforced by the infrastructure

From initial needs assessment and planning to solution design, implementation, and support, HP delivers the IRM services and industry-standard technologies you need to define, enact, and enforce a corporate-wide solution for protecting digital information throughout its life cycle.

Delivering a comprehensive, policy-driven solution
HP works with your organization to ensure that appropriate corporate governance policies, standards, and rules are in place. We leverage industry-standard security technologies from HP, Microsoft, and other...
leading security organizations to design and implement a complete IRM solution that supports your business requirements. Our solutions span the full range of IRM services by providing:

- Risk assessments and strategy, policy planning, and enforcement
- Trustworthy infrastructure design and implementation
- Document Information Systems
- Data classification and information life cycle management (ILM)
- Software integration, implementation, and testing
- IRM protected web and business-enabling application deployment and management

Protecting information wherever it is distributed

Built on powerful, flexible, and secure HP platforms, our IRM solutions leverage industry-leading security software to enforce corporate policies governing digital information in Microsoft environments, including:

Microsoft Rights Management Services (RMS): Designed for Microsoft Windows® Server 2003 and Microsoft Office 2003 environments, RMS combines developer tools and proven security technologies—including encryption, certificates, and authentication—to safeguard information at the document level. RMS enables you to create rules for Microsoft Office 2003 documents, applying persistent usage policies that remain with the documents wherever they are distributed inside or outside your company. For example, documents can be marked “cannot forward” or “cannot print.” Anyone receiving such documents will be unable to forward or print them.

HP ProtectTools E-mail Release Manager (ERM): ERM works in conjunction with RMS, enforcing a centrally controlled and managed security policy by applying labels to each e-mail message and its attachments. Built-in intelligence evaluates these labels and the destination of the message to determine what rules (if any) apply before the message can be released. Such rules could include imposing specific RMS templates, or direct security measures like digital signing or encryption, which can be transparent to the user. ERM can be configured to apply a double layer of defense—at the desktop and at the mail server—for maximum protection. By automating policy enforcement, ERM simplifies implementation of security rules and ensures that those rules are carried out without dependence on human factors.

HP is also working with other third-party vendors to extend the functionality of RMS in areas beyond Microsoft Office documents, adding functionality to mobile devices and enabling better interorganizational sharing of protected data.

In addition, HP adds ILM strategies and technologies to this software mix, enabling rights management for archived information. This innovative approach ensures that corporate governance policies are maintained long after a document is actively used and continue to be enforced should that document be retrieved at any time in the future.

Maximizing results with a proven services methodology

An IRM solution is only as effective as the policies on which it is based. HP uses a best practices-guided methodology in delivering our IRM solutions, ensuring that appropriate policies are established and that the IRM solution is optimized to enforce those policies. Our methodology includes:

- Assessment: Through consulting engagements and workshops, HP provides a “best fit” assessment of governance and infrastructure requirements to evaluate the readiness of the customer’s IT environment for an IRM/ERM implementation, including an assessment of the policies, practices, and procedures in place as well as a determination as to whether the technical prerequisites for an RMS implementation have been met.
- Design: HP consultants can determine your precise business requirements and design a trustworthy infrastructure with the most appropriate combination of security software and hardware to meet those requirements.
- Pilot: HP can provide a limited implementation to evaluate and refine the IRM/ERM solution design to maximize its effectiveness prior to full rollout. The pilot validates the features of the IRM technology; defines the standards used; demonstrates ease of use, deployability, and manageability within the customer environment; and determines the ability for IRM to meet the requirements and working practices of the customer.
- Implementation: HP provides complete implementation and integration services to enable IRM across your enterprise.
- Support: HP provides comprehensive training and support to help you get the most out of your current investments and to enhance security as your needs evolve.

With HP, you have an experienced, trusted partner to address the full scope of your security requirements and protect your Microsoft environment, wherever documents and files are distributed throughout the information life cycle.

For more information on HP information rights management solutions featuring Microsoft RMS and HP ERM, contact your HP representative or visit www.hp.com/solutions/microsoft/irm.

© Copyright 2005 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein. Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.