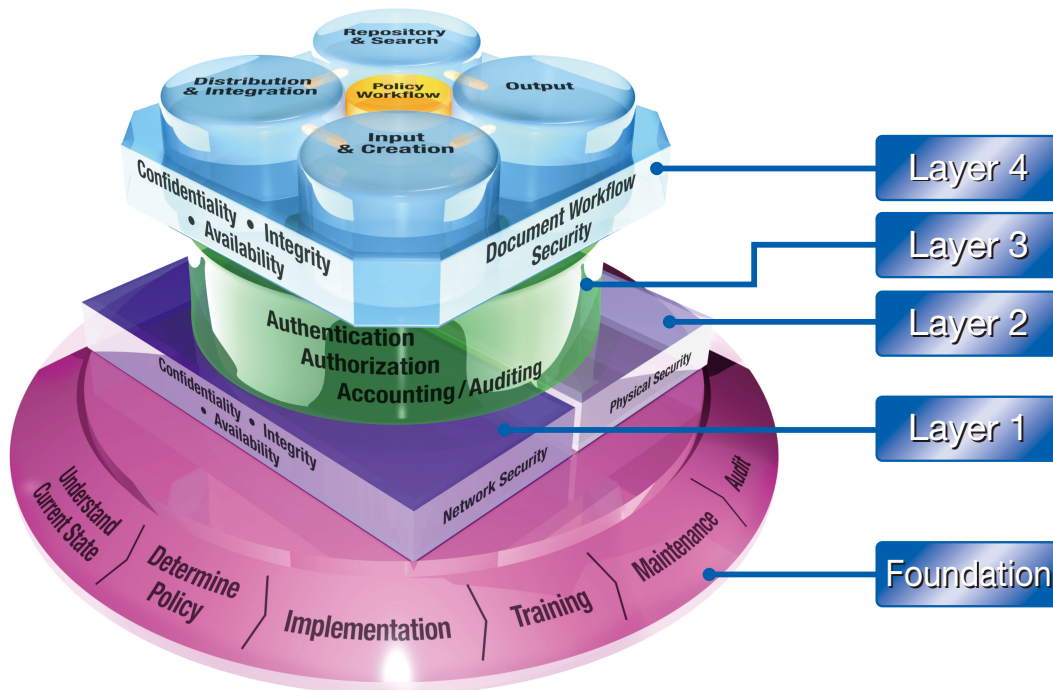


## Multilayered Framework Concept Enabling Comprehensive Security

When digital devices are connected to a network, there should be assurance that system resources and data are protected from disruptive forces inside and outside the organization. This assurance enables IT managers to embrace products that would otherwise pose a security risk, while providing employees with high-performance equipment that streamlines the work flow, protects vital business interests, and ensures peace of mind.

### Document Security Framework



### The Framework Concept

The Document Security Framework concept is derived from Ricoh's extensive research on our customers' document-related business processes, and reflects respect for the considerable IT investments that have been made. Central to this framework is Ricoh's commitment at each layer, starting with the Physical Security and Network Security Layers (Layers 1 and 2).

These Physical Security and Network Security countermeasures are some of the basic methods used to maintain the Confidentiality, Integrity, and Availability of documents and data.

Once the basic security measures are implemented, stages in the document workflow

must be protected as well. This includes Input & Creation, Output, Repository & Search, and Distribution & Integration (Layer 4). Providing the foundation for this is Layer 3, comprised of Authentication, Authorization, and Accounting/Auditing countermeasures. This AAA Security Layer safeguards the document workflow.

Once the AAA Security Layer is implemented, the document workflow can include correct and safe processes governing information Input & Creation, Output, Repository & Search, and Distribution & Integration. It is then possible to establish proper Document Workflow Security (Layer 4). This can include MFP integration with backend Document Management Systems (DMSs) that provide organizations with the power to control information assets and meet

stringent compliance requirements.

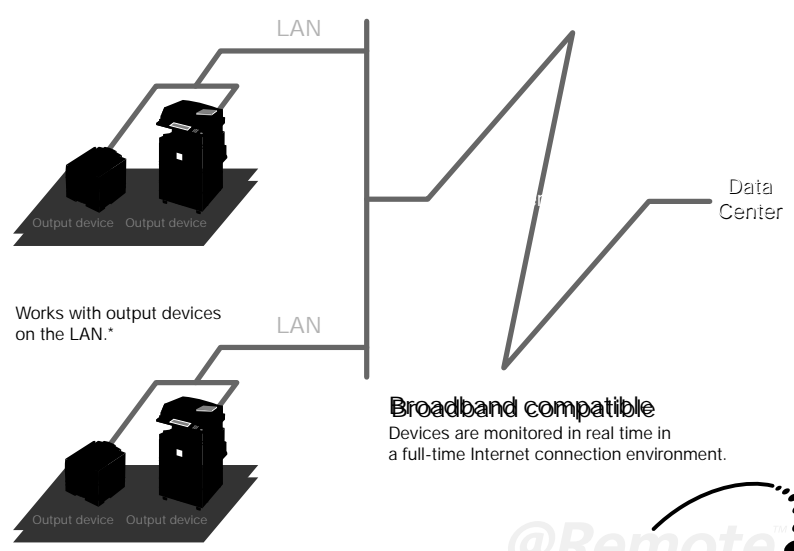
After deploying countermeasures, processes should be reviewed according to the Deming Plan-Do-Check-Act (PDCA) cycle. For example, in the planning stage, it's important to understand the current state of security and define any new policies. To ensure proper use and maintenance of countermeasures, employees must also understand the policies. Furthermore, auditing should be conducted from time to time, in order to check if the security procedures are successful, or if modifications are necessary (Foundation).







@Remote enables greater operating



\*Multi-purpose digital devices and laser printers compatible with @Remote.

