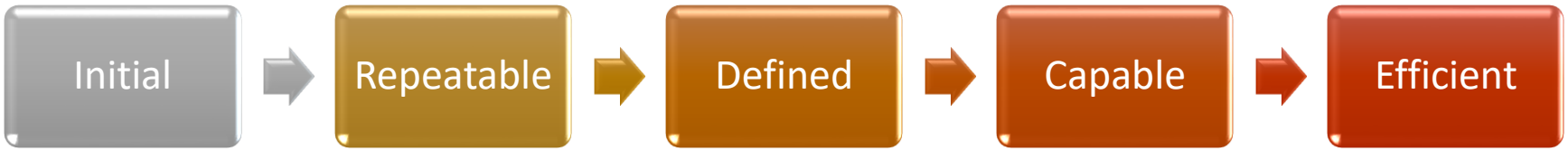
IT Security Risk Assessment Executive Summary

Dean Dorton Allen Ford, PLLC (Dean Dorton), performed an independent information security risk assessment of Jefferson County Public Schools (JCPS). The purpose of the assessment was to identify security risks to JCPS systems and information and assess the current activities in place to mitigate risks identified.

Dean Dorton used a framework prescribed by International Organization for Standardization (ISO) which is considered a best practice in the industry.

An effective risk management process, identifies potential problems before they occur so that risk-handling can be implemented to mitigate adverse impacts on achieving objectives. The risk assessment has identified areas where JCPS can improve its practices to further manage the risks inherent in the information technology environment. The speed in which JCPS can move the processes from the initial stage to optimizing is dependent on the resources available, both human and financial capital. However, some areas simply require creating documentation of what is already being performed.

The Office of Technology (OT) has evaluated the results of the risk assessment and have put together a plan to strengthen the security posture of the organization. This will include educating employees in their role to help ensure a strong security environment, purchasing and utilizing tools to help manage the ever changing security environment, evaluating the responsibilities of staff to ensure critical functions are properly monitored and working with our partners and vendors to ensure expectations are clearly communicated and understood. In addition, while OT is the overall process owner, many of the activities will require input and buy in from others throughout JCPS. Specifically in the area of determining the risk tolerance and budgetary consideration.



The starting point for use of a new or undocumented repeat process. The controls are performed on an ad hoc basis, sometimes they are not performed. There is general agreement within the organization that identified actions should be performed. The practices are not adopted, tracked, and reported on.	The base requirements for the control area are planned, implemented, and repeatable.	Processes used are more mature: documented, approved, and implemented organization-wide.	Processes are measured and verified (e.g., auditable).	Defined, standard processes are regularly reviewed and updated. Improvements reflect an understanding of, and response to, a vulnerability's impact.

IT Security Risk Assessment Executive Summary

Risk Reference	IT Activity Category	AssessedMaturity Level
ISO 27005:2011	Risk Management	Initial
ISO 5	Information Security Policies	Initial
ISO 6	Organization of Information Security	Initial
ISO 7	Human Resources Security	Repeatable
ISO 8	Asset Management	Repeatable
ISO 9	Access Control	Initial
ISO 10	Cryptography	Initial
ISO 11	Physical & Environmental Security	Defined
ISO 12	Operations Security	Repeatable
ISO 13	Communications Security	Repeatable
ISO 14	System Acquisition, Development and Maintenance	Initial
ISO 15	Supplier Relationships	Initial
ISO 16	Information Security Incident Management	Repeatable
ISO 17	Information Security Aspects of Business Continuity Management	Initial
ISO 18	Compliance	Repeatable

IT Security Risk Assessment Executive Summary

Plan of Action for the Top 10 Items

Risk Reference	Activity	Estimated Timeline
ISO 6	Working on Organizational Structure that will allow us to focus Cyber Security Functions	Starting July 1, 2019
ISO 6	We will engage with local authorities and attend local events to enhance our involvement in Cyber Security threats throughout the year	Starting July 1, 2019
ISO 8 & 9 & 11	In process of a Proof of Concept evaluating of an Inventory Asset Management (ITAM) solution	Starting July 1, 2019
ISO 9	We have placed controls on students allowed to only send and receive email within the U.S.	Completed
ISO 12	We will pursue Proof of Concept with IT Service Manager (ITSM) for Change Management	Q4 FY2019 – Q1 FY2020
ISO 12	We will implement a Vulnerability Management Program-SANS Framework with processes, tools and people structured to perform that work throughout the year	Start July 1, 2019, estimated program in place by 9/2019
ISO 12	We will be pursuing Proof of Concept of Microsoft A5 licensing (highest available Security Suite) and Log Analytics	June 30, 2019
ISO 13	We have submitted a budget request to upgrade the Network Wireless for the Entire District that will increase our Wireless Security for start of Implementation in 2019	Start of Implementation in 2019, estimated completion Q1 FY 2022
ISO 15	We have created a Data Governance committee and have created workflow documents for approval of software and collection with 3rd party software and collection of Data Sharing documents. Recommendation and Diagram are ready to be presented to members of the Cabinet	Recommendation and Flow Diagram are ready to be presented to members of the Cabinet
ISO 17	Currently working with KDE to establish a Business Continuity Site	In progress anticipated completion 12/2019