Business Continuity Maturity Matrix

A maturity model is one of the most valuable tools available for planning and sustaining a new Business Continuity program. Like the Business Continuity Planning (BCP) program itself, this maturity model should be customized around the unique goals, priorities and competencies of your organization. The model included below is the model developed by Intellinet's Business Solutions Group. It can, and should, be customized to meet the needs of your organization.

Business Continuity Planning Maturity Matrix

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
1. Mission Essential Functions	The *Mission Essential Functions* have not been discussed or documented.	General awareness of the *Mission Essential Functions* but not fully understood or endorsed. A determination of needed resources has	*Mission Essential Functions* defined and understood by most. Resources to support essential functions have been informally identified. Functions reflect a	*Mission Essential Functions* are defined, understood and agreed to by all. They have been created with staff input, and reflect a operational focus	*Mission Essential Functions* are defined, understood and promoted by all. They were developed with input from the organization and are consistent with the		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
2. Management Structure	No incident management structure ha been defined. Incident management is handled "ad-hoc".	Basic emergency roles are established. Most staff have been trained.	Emergency roles are established, routinely updated. The emergency management structure generally follows the ICS. All command and control staff has been trained.	Emergency roles are established, routinely updated and communicated to all applicable people within the organization. The emergency management structure follows the ICS. All command and control have been trained and tested and a requalification schedule is in place.	Emergency roles are established, routinely updated and communicated to all applicable people within the organization. The emergency management structure ensures adequate span of control. Orders of succession are identified and documented. The emergency management structure follows the ICS. All command and control have been trained and tested and a requalification schedule is in place.		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
3. Facilities	No hazard assessment has been conducted. No protective devices are available.	General understanding of vulnerabilities exists. Basic protection is installed or can be installed for some hazards. No backup utilities are in-place.	General understanding of vulnerabilities exists. Protection devices are installed or capable of being installed, for several of the identified hazards. Backup utilities are in place to sustain facility operation.	A comprehensive facility vulnerability assessment has been conducted and reviewed by management. The facility has protection devices installed, or capable of being installed, for all identified hazards. Backup utilities are in place to sustain facility operation. Administrative and physical security practices are fully established.	A comprehensive facility vulnerability assessment has been conducted and reviewed by management. The facility meets all current applicable building codes. The facility has protection devices installed, or capable of being installed, for all identified hazards. Utilities entering the facility are protected and secure. Backup utilities are in place to sustain facility operation. Administrative and physical security practices are fully established.		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
4. Communications	No communications plan exists. Impact of the loss of communications has not been assessed. Call lists are informal. Internal and external communications are mainly handled via landline and cellular phone.	Communications plan is informal and undocumented. An alternate communications mechanism is in place but has limited capability. Call lists for key employees are established. Internal and external communications are mainly handled via landline and cellular phone.	Communications plan is established and communicated to most within the organization. Call lists for key employees are established. Multiple modes of internal and external communications are established.	Communications plan is established, routinely updated and communicated to most within the organization. Call lists for key employees are established and current. Multiple modes of internal and external communications are established and alternate systems are actively enabled upon failure.	Communications plan is established, routinely updated and communicated to all applicable people within the organization. Call lists for key employees, vendors and customers are established, current and readily available. Multiple modes of internal and external communications are established and alternate systems are actively enabled upon failure. All communication systems are tested routinely		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
5. Personnel	Only basic contact information is kept for most company personnel. No drills or exercises are conducted. Emergency roles and responsibilities are not defined.	Only basic contact information is kept for most company personnel. No drills or exercises are conducted. Personnel are generally aware of their emergency roles and responsibilities.	Basic contact information is kept for most company personnel. Personnel routinely participate in drills and exercises. Personnel are aware of their emergency roles and responsibilities. A passive employee accountability system is utilized in case of evacuation or emergency.	Accurate and up-to-date contact information is kept for most company personnel. Personnel are encouraged to have personal disaster plans. Company provides some emergency supplies for responders. Personnel routinely participate in drills and exercises. Personnel are aware of their emergency roles and responsibilities and are cross-trained in other roles. A passive employee accountability system is utilized in case of evacuation or emergency.	Accurate and up-to-date contact information is kept for all company personnel. Personnel have personal disaster plans on file. Company provides emergency supplies and child care provisions for responders. Personnel routinely participate in drills and exercises. Personnel are fully aware of their emergency roles and responsibilities and are cross-trained in other roles. An active employee accountability system is utilized in case of evacuation or emergency.		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
6. Vendors	Only basic business contact information is kept for vendors. No contracts are in-place for post-disaster services.	Only basic business contact information is kept for vendors. Some plans have been made for increased inventory. Contracts and agreements are in place for a few post-disaster services.	Some contact information is kept for key vendors. Increased inventory and/or modified shipment plans have been considered for when disaster threatens. Contracts and agreements are in place for post-disaster services.	Accurate and up-to-date contact information is kept for key vendors. Alternate vendors have been identified in the event the primary vendors are unavailable. Increased inventory and/or modified shipment plans have been considered for when disaster threatens. Contracts and agreements are in place for post-disaster services.	Accurate and up-to-date contact information is kept for all vendors. Vendors' business continuity plans have been reviewed and are kept on-file. Alternate vendors have been identified in the event the primary vendors are unavailable. Increased inventory and/or modified shipment plans are in place for when disaster threatens. Contracts and agreements are in place for post-disaster services.		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
7. Customers	No alternate capabilities are pre-established to handle customer interface. No customer communications plan is in place to ensure customers know what to expect and how contact will be maintained.	No alternate capabilities are pre-established to handle customer interface. The company has an informal customer communications plan to ensure customers know what to expect and how contact will be maintained.	Alternate capabilities are in place to handle customer interface. The company has an informal customer communications plan to ensure customers know what to expect and how contact will be maintained.	Key customers are identified and accurate and up-to-date contact information is maintained. Alternate capabilities are in place to handle customer interface. The company has an informal customer communications plan to ensure customers know what to expect and how contact will be maintained.	Key customers are identified and accurate and up-to-date contact information is maintained. Changes in products and services for customers have been identified and incorporated into emergency plans. Alternate capabilities are in place to handle customer interface. The company has a customer communications plan to ensure customers know what to expect and how contact will be maintained.		

intellinet Business Continuity Planning Maturity Matrix

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
8. Vulnerability Assessment	No Vulnerability Assessment has been conducted. Current vulnerabilities are not consistently understood	A Vulnerability Assessment has been done but is outdated. Not completed for the entire organization.	Vulnerability Assessment complete, and current, but not fully communicated. Awareness is on an informal basis.	Vulnerability Assessment complete and communicated. A general understanding of vulnerabilities and their impact on Mission Essential Functions exists. There also exists a general idea of the potential business	A comprehensive vulnerability assessment has been conducted and reviewed by management. The vulnerabilities have been cross-referenced with Mission Essential Functions and potential business interruptions are identified.		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
9. Mitigation	No protective devices are installed or capable of being installed.	The facility has some protection devices installed, or capable of being installed, for some of the identified hazards.	A general sense of mitigation opportunities exist but aren't based on vulnerability assessment or cost /benefit analysis. A desire to strengthen the facility exists.	Mitigation opportunities have been identified based on vulnerability assessment and a cost /benefit analysis has been done but specific funding has not been identified.	The facility meets all current applicable building codes. The facility has protection devices installed, or capable of being installed, for all identified hazards. The organization has a prioritized list of mitigation projects that it intends to complete as part of its strategic plan.		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
10. IT / Information Management	No mission critical information sources have been identified. No software and hardware assets are identified and tracked. No essential hardware and software configurations have been documented. Data backups have been established only for onsite systems. No recovery team has been identified. The organization has no change management procedures.	Few mission critical information sources have been identified. Few software and hardware assets are identified and tracked. Few essential hardware and software configurations have been documented. Manual data backups have been established for both onsite and offsite storage. Recovery team is identified ad-hoc. Few inter-office networks have been established with adequate redundancy to prevent isolation. The organization has informal change management procedures.	Some mission critical information sources have been identified. Some software and hardware assets are identified and tracked. Some essential hardware and software configurations have been documented. Manual data backups have been established for both onsite and offsite storage. Routine testing of backup capability is performed. A recovery team has been identified and trained. Some inter-office networks have been established with adequate redundancy to prevent isolation. The organization has developed and implemented change management procedures.	Most mission critical information sources have been identified. Most software and hardware assets are identified and tracked. Most essential hardware and software configurations have been documented. Automated data backups have been established for both onsite and offsite storage. Routine testing of backup capability is performed. A recovery team, with alternates, has been identified and trained. Some inter-office networks have been established with adequate redundancy to prevent isolation. The organization has developed and implemented comprehensive change management, testing and release procedures.	All mission critical information sources have been identified. All software and hardware assets are identified and tracked. All essential hardware and software configurations have been documented. Automated data backups have been established for both onsite and offsite storage. RTO's and RPO's have been established and systems have ben designed accordingly. Routine testing of backup capability is performed. A recovery team, with alternates, has been identified and trained. All inter-office networks have been established with adequate redundancy to prevent isolation. The organization has developed and implemented comprehensive change management, testing and release procedures.		

intellinet Business Continuity Planning Maturity Matrix

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
11. Information Security	There are no policies and procedures to secure the business. Management does not consider investing in systems necessary for the overall security of their information systems. In addition, the organization does not assess the business impact of its vulnerabilities and it does not understand the risks involved due to these vulnerabilities.	The organization is conscious about the threats that their information systems face. The organization is characterized by being chaotic, inconsistent and ad hoc in response to attacks. There is recognition of the business risks due to vulnerabilities but have no defined policies or procedures to protect the organization. In addition, the organization has little in the way of practical implementation in security systems. Most control will be reactive and not planned. There overall focus is on the business activities of the organization and little attention is focused on securing the information systems. The goals may change in response to attacks by implementing some kind of protection but it will not be continuous or systematic.	The organization wants to protect its investment and ensure continuity. Application and network security is implemented but changes are not centrally managed and ad hoc security requests are common. The organization trusts the interaction between the user and the systems. Security awareness programs are being considered for key resources only. IT security procedures are informally defined and some risk assessments take place. In addition, responsibilities for IT security have been assigned but enforcement is inconsistent. Some intrusion and detection testing is also being performed. The goals at this level are usually centered on the business activities of the organization and the protection of core systems. The organization will consider the security of a system after the system's implementation. There is a general perception that information systems are protected and an unawareness of the threats and vulnerabilities.	There is a central management of all security related issues and policies. Users are trusted but their interactions with the systems are viewed as vulnerability. No ad hoc changes and central configuration models, from which all configurations are derived, are implemented. Security policies and procedures are in place together with adequate delivery mechanisms to aid awareness and compliance. Access controls are mandatory and are closely monitored. Security measures are introduced on a cost/benefit basis and ownership concept is in place. Since the actions of users are the starting point for many attacks, there is a desire to inculcate a "culture of security" in users. Communication between the security team and the users takes place to keep the users informed of possible threats. Culturally, users don't fully understate security concerns and the security team views users as a threat. There is a general perception that many security mechanisms are merely overhead that gets in the way of their real work. Goals are usually centered on the business activities, the users, and monitoring security threats and all related patches are tested and implemented. The organization is conscious of their security needs and they invest in systems that protect the organization.	IT has control over the security needs of the organization, monitoring the systems, being aware of threats and benchmarking by comparing the organization itself to other similar organizations and to international standards. In addition, a comprehensive security function has been established that is both cost effective and efficient which delivers high quality implementation. This comprehensive plan has formal policies and procedures in place to prevent, detect, and correct any security related issues. Corporate governance is aligned with the security needs of an organization. Corporate governance has policies for internal auditing and is independent and objective focused on improving the security of the organization. The result of any audit activity is published and actions are implemented. Security is managed by identifying the security concerns. Security incidents are tracked in a systematic way. The organization has proper policies for security in a formal sense and business plans have items for security. The use of specific technologies throughout the organization is in a uniform manner and the implementation was driven out of a business plan. Security architecture is a full consideration to the organization. While the business architecture considers all external factors in an organization, the security architecture considers all users in the implementation. Policies are created to meet the needs of the users but information in or out of the organization is captured. A system for providing traceability through the organization is in place. Users are also involved in architectural analysis		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
12. Finances	The company has no cash reserves for the recovery period. Some important financial records may be secured but are not pre-identified. No provisions have been made for the acquisition and storage of additional inventory needed for the recovery period. The organization has no budgeting for preparedness activities. There are no specific budget items for mitigation activities. No processes are in place for emergency purchases	The cost of sustaining some business functions for a 3-day recovery period has been set aside. Some important company financial records have been secured. No provisions have been made for the acquisition and storage of additional inventory needed for the recovery period. The organization has no budgeting for preparedness activities. There are no specific budget items for mitigation activities. Only informal processes are in place for emergency purchases.	The cost of sustaining business for a 3-day recovery period has been set aside. Important company financial records have been secured. Provisions have been made for the acquisition and storage of some additional inventory if needed for the recovery period. The organization has sporadic budgeting for preparedness activities. There are no specific budget items for mitigation activities. Only informal processes are in place for emergency purchases.	The cost of sustaining essential business functions for a 5-day recovery period has been set aside. Payroll and employee expenses have been established as a cash reserve. Important company financial records have been secured. Alternate financial institutions are accessible to the company outside the impacted area. The organization has specific budgeting for preparedness activities. There are some specific budget items for mitigation activities. Processes are in place for emergency purchases.	The cost of sustaining essential business functions for at least 7-day recovery period has been set aside. Payroll and employee expenses have been established as a cash reserve. A system/procedure for tracking and paying disaster & preparedness expenses has been created. Important company financial records have been secured. Provisions have been made for access to multiple financial institutions outside the impacted area. The organization has specific budgeting for preparedness activities. Specific budget items exist for all mitigation activities. Processes are in place for emergency purchases.		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
13. Insurance	The business has some insurance but no business interruption coverage. Policy currency is unknown. Insurance documents are difficult to find if needed.	The business has some insurance but no business interruption coverage. All insurance policies are current. Insurance documents are difficult to find if needed.	Adequate levels of insurance coverage, including business interruption, have been acquired based on management assumptions. All insurance policies are current. Insurance documents are	Adequate levels of insurance coverage, including business interruption, have been acquired based on a basic vulnerability assessment. All insurance policies are current. Insurance	Adequate levels of insurance coverage, including business interruption, have been acquired based on a comprehensive vulnerability assessment. All insurance policies are current. Insurance documents		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
14. Plan Content / Maintenance	The organization has no emergency plan.	The organization has a written emergency management plan. Some of the basic emergency planning elements are addressed in the plan but have not been promulgated. The plan is seldom reviewed. No training is provided on the plan. Safety equipment and other critical elements of the plan are rarely available and not maintained as part of a maintenance process.	The organization has a written emergency management plan that is reviewed and revised after major business changes. The plan addresses most components of a comprehensive emergency management plan. The plan identifies some essential functions. Training is sometimes provided. Safety equipment and other critical elements of the plan are available but not maintained as part of a maintenance process.	The organization has a written, comprehensive emergency management plan that is reviewed and revised at least annually, with all revisions being approved and tracked. The plan addresses all (#) standard components of a comprehensive emergency management plan. Training is routinely provided. Safety equipment and other critical elements of the plan are available but not maintained as part of a maintenance process.	The organization has a written, comprehensive emergency management plan that is reviewed and revised at least annually, with all revisions being approved and tracked. The plan is driven from the comprehensive vulnerability assessment. The plan addresses all (#) standard components of a comprehensive emergency management plan. The plan identifies both essential and non-essential functions to clarify what segments of the business will continue to function post-event. Training is routinely provided and plan revisions are communicated throughout the organization. Safety equipment and other critical elements of the plan are fully maintained.		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
15. Physical Security	The facility has no intrusion detection system. The facility has no access control system. Employees are not issued identification cards. There are no specific procedures for receiving and checking in mail, packages and shipments. Vehicular traffic is not controlled.	The facility has an intrusion detection system but it may or may not be monitored. The facility has an access control system for the main building. Employees are all issued identification cards. Procedures for receiving and checking in mail, packages and shipments are informal. Vehicular traffic is not controlled.	The facility has an intrusion detection system. The intrusion detection system is monitored. The facility has an access control system for the main building. Employees are all issued identification distinguishing their access level. Procedures for receiving and checking in mail, packages and shipments are informal. Vehicular traffic is not controlled.	The facility has an intrusion detection system providing basic building perimeter protection. The intrusion detection system is monitored. The facility has an access control system for the main building and all other secure locations inside. Employees and visitors are all issued identification distinguishing their access level. Procedures for receiving and checking in mail, packages and shipments are informal. Vehicular traffic is not controlled.	The facility has an intrusion detection system providing complete perimeter protection. The intrusion detection system is monitored and split into functional zones. The facility has an access control system for the main building and all other secure locations inside. Employees, customers, vendors and visitors are all issued identification distinguishing their access level. Procedures have been established for receiving and checking in mail, packages and shipments. Vehicular traffic is kept a safe distance from the building(s).		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
16. Re-Entry	The organization has no written re-entry plan. PPE is not provided for re-entry personnel. Personnel have not been trained on re-entry duties.	The organization has no written re-entry plan. PPE is provided for re-entry personnel. Personnel have not been trained on re-entry duties.	The organization has a written re-entry plan that is reviewed after major business changes. PPE is provided for re-entry personnel. Personnel have not been trained on re-entry duties.	The organization has a written, comprehensive re-entry plan that is reviewed and revised at least annually. PPE is provided for all re-entry personnel. Personnel have been trained on re-entry duties.	The organization has a written, comprehensive re-entry plan that is reviewed and revised at least annually. PPE is provided for all re-entry personnel. Re-entry acceptance criteria has been established and documented. Personnel have been trained on re-entry duties.		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
17. Threat Monitoring	No threat monitoring takes place within the organization. No formal process is in place for analyzing threat information. Threat information is not communicated to decision makers. Communication of threat information to employees does not exist. No communication of threat information goes to customers and vendors.	Threat monitoring is handled by personnel receiving broadcast news reports via tv and radio. No formal process is in place for analyzing threat information. Threat information is communicated to decision makers as necessary. Communication of threat information to employees is best effort. No communication of threat information goes to customers and	Procedures are in place for manual continuous threat monitoring. No formal process is in place for analyzing threat information. Threat information is communicated to decision makers as necessary. Communication of threat information to employees, customers and vendors is best-effort.	Procedures are in place for manual continuous threat monitoring. A formal process is in place for analyzing threat information. Threat information is communicated to decision makers as necessary. A process is in place to communicate threat information to employees, customers and vendors.	Procedures are in place for active continuous threat monitoring. A formal process is in place for analyzing threat information. Threat information is effectively communicated to decision makers. A process is in place to communicate threat information to employees, customers and vendors.		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
18. Alternate Sites	No plans exist to transfer essential operations to an alternate facility if needed.	An alternate facility is available if needed. The alternate location has some of the necessary infrastructure in place to sustain emergency operations for a short period of time. Roles and responsibilities for personnel at the alternate location are based on normal roles.	A plan exists to transfer essential operations to an alternate facility if needed. The alternate location has some of the necessary infrastructure in place to sustain emergency operations for a short period of time. Roles and responsibilities for personnel at the alternate location are based on normal roles. Contact numbers for the alternate facility are published when the facility is activated.	A plan exists to transfer essential operations to an alternate facility if needed. The alternate location has some of the necessary infrastructure in place to sustain emergency operations for a short period of time. Roles and responsibilities for personnel at the alternate location have been clearly defined. Contact numbers for the alternate facility have been published. A plan exists to transfer essential operations from an alternate facility back to the primary location(s).	A plan exists to transfer essential operations to an alternate facility if needed. The alternate location has the necessary infrastructure in place to sustain emergency operations. Roles and responsibilities for personnel at the alternate location have been clearly defined and communicated. Contact numbers for the alternate facility have been published. A plan exists to transfer essential operations from an alternate facility back to the primary location(s).		

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
19. Training & Exercises	No training is conducted for emergency responders. The organization has no drill and exercise program.	High-level emergency responders are trained initially for their specific roles. No requalification schedule is in place. The organization has an exercise program incorporating one or two types of drills and scenarios. Exercise participation is not tracked to ensure proficiency. Post-exercise critiques are not conducted.	High-level emergency responders are trained for their specific roles. Re-training is conducted when personnel change normal roles. The organization has an exercise program incorporating various types of drills and scenarios. Exercise participation is not tracked to ensure proficiency. Post-exercise critiques are conducted but the results are rarely acted upon.	All emergency responders are trained for their specific roles. A requalification schedule is in place to ensure emergency responders are re-trained periodically. Emergency preparedness and emergency response is part of new employee orientation. The organization has an exercise program incorporating various types of drills and scenarios. Key employee exercise participation is tracked to ensure proficiency. Post-exercise critiques are conducted and the results are discussed by the management team but may not be incorporated.	All emergency responders are trained and tested for their specific roles. A requalification schedule is in place to ensure emergency responders are re-trained at least annually. Emergency preparedness and emergency response is part of new employee orientation. The organization has an exercise program incorporating various types of drills and scenarios. Employee exercise participation is tracked to ensure proficiency. Post-exercise critiques are conducted and the results are incorporated into a corrective action plan.		

intellinet Business Continuity Planning Maturity Matrix

	UNFOCUSED	AWARE	CAPABLE	MATURE	WORLD-CLASS	Curr	Goal
20. Resource Management	The organization has no formal system for describing, inventorying or tracking resources. The emergency plan does not identify any of the resources needed to perform essential functions. No agreements /contracts have been made for handling emergency resource requests. No vendors have been identified for emergency repairs and replacements.	The organization has a basic system for inventorying resources. The emergency plan does not identify any of the resources needed to perform essential functions. Some informal agreements have been made for handling emergency resource requests.	The organization has a basic system for describing, inventorying and tracking resources. The emergency plan identifies some of the resources needed to perform essential functions. Some agreements/contracts are available for handling emergency resource requests. Increased inventory and/or modified shipment plans are handled ad-hoc when disaster threatens.	The organization has a comprehensive system for describing, inventorying and tracking resources. The emergency plan identifies some of the resources needed to perform essential functions. Some agreements/contracts are available for handling emergency resource requests. Some vendors have been identified for emergency repairs and replacements. Increased inventory and/or modified shipment plans are in place for when disaster threatens.	The organization has a comprehensive system for describing, inventorying and tracking resources. The emergency plan identifies the resources needed to perform essential functions. Agreements/contracts are available for handling emergency resource requests. Vendors have been identified for emergency repairs and replacements. Increased inventory and/or modified shipment plans are in place for when disaster threatens.		